Lenovo XClarity Administrator
Guide d'utilisation

Version 4.0.0

Première édition (Février 2023)

Table des matières

Tableaux

Récapitulatif des modifications

Les éditions ultérieures du logiciel de gestion Lenovo XClarity Administrator prennent en charge un nouveau matériel, des améliorations logicielles, ainsi que des correctifs.

Pour plus d'informations sur les correctifs, consultez le fichier historique des modifications (*.chg) qui est fourni dans le module de mise à jour.

Cette version prend en charge les améliorations ci-après dans le logiciel de gestion.

Pour plus d'informations sur les améliorations dans d'autres éditions, voir Nouveautés dans la documentation en ligne de XClarity Administrator.

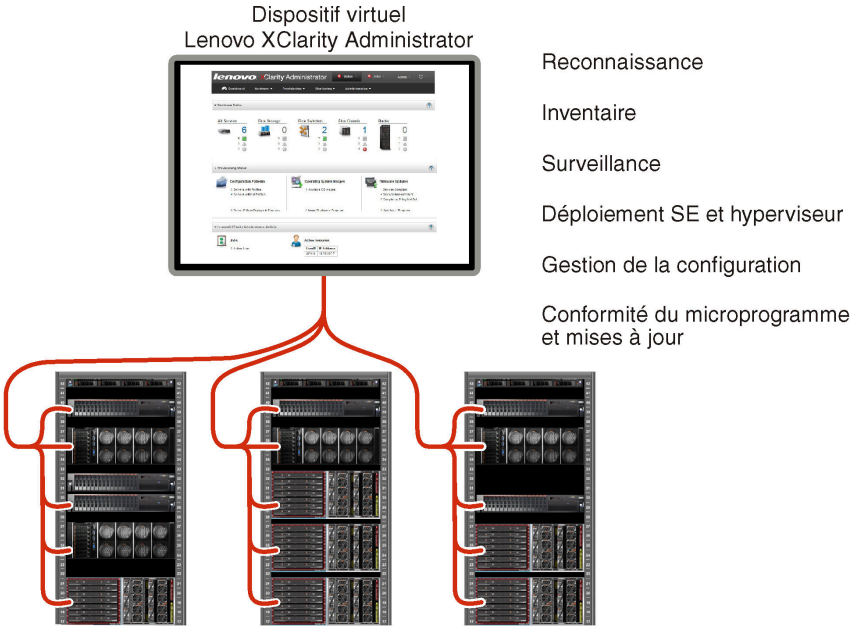
Fonction	Description
Administration	Vous pouvez envoyer les informations de DNS et FQDN (nom de domaine pleinement qualifié) du serveur de gestion XClarity Administrator aux serveurs gérés avec IMM2, XCC et XCC2 pour que les serveurs gérés trouvent le serveur de gestion à l'aide de ces informations (voir Configuration de l'accès réseau).
Surveillance	Vous pouvez afficher des données d'inventaire supplémentaires pour les composants de mémoire persistante (PMEM) (voir Affichage des détails d'un serveur géré). Vous pouvez afficher des données d'inventaire supplémentaires pour les dispositifs de stockage (voir Affichage des détails d'un serveur géré).
Gestion des appareils	Vous pouvez afficher et configurer le mode de sécurité pour des serveurs spécifiques distincts de XClarity Administrator (Configuration des paramètres de sécurité pour un serveur géré et Configuration des paramètres cryptographiques sur le serveur de gestion). Les adresses IP secondaires sont prises en charge pour le contrôleur de gestion de la carte mère sur les serveurs ThinkSystem applicables (voir Affichage des détails d'un serveur géré).
Mises à jour du microprogramme	Vous pouvez mettre à jour le microprogramme sur les bandothèques IBM TS4300 (voir Mise à jour du microprogramme sur les appareils gérés).
Déploiement du système d'exploitation	Vous pouvez déployer les systèmes d'exploitation suivants sur des serveurs gérés (voir Systèmes d'exploitation pris en charge). • Microsoft Windows Client 10 21H2, 10 22H2 et 11 22H2 • RedHat Enterprise Linux 9.x • Ubuntu Server 22.04.x

Chapitre 1. Présentation de Lenovo XClarity Administrator

Lenovo XClarity Administrator est une solution centralisée de gestion des ressources qui simplifie la gestion de l'infrastructure, accroît la rapidité des réponses, et améliore la disponibilité des systèmes et des solutions de serveur Lenovo®. Elle fonctionne comme un dispositif virtuel qui automatise les fonctionnalités de reconnaissance, d'inventaire, de suivi, de surveillance et de distribution pour le serveur, le réseau et le matériel de stockage dans un environnement sécurisé.

En savoir plus :

- XClarity Administrator : gestion du matériel comme des logiciels
- XClarity Administrator : Présentation



XClarity Administrator fournit une interface centrale destinée à l'exécution des fonctions ci-après pour tous les appareils gérés.

Gestion du matériel

XClarity Administrator permet une gestion sans agent du matériel. Elle peut reconnaître automatiquement les appareils gérables, notamment le serveur, le réseau et le matériel de stockage. Les données d'inventaire sont collectées pour les appareils gérés, afin d'offrir une vue d'ensemble de l'inventaire matériel géré et de son état.

Il existe diverses tâches de gestion pour chaque appareil pris en charge, notamment l'affichage de l'état et des propriétés, la configuration du système et des paramètres réseau, le lancement des interfaces de gestion, la mise sous tension et hors tension, ainsi que le contrôle à distance. Pour plus d'informations sur la gestion des appareils, voir Gestion des châssis, Gestion des serveurs, Gestion des commutateurs.

Conseil : Le serveur, le réseau et le matériel de stockage qui peuvent être gérés par XClarity Administrator sont appelés *dispositifs*. Le matériel qui est géré par XClarity Administrator est appelé *appareils gérés*.

Vous pouvez utiliser la vue Armoire dans XClarity Administrator pour regrouper vos appareils gérés pour refléter la configuration de l'armoire physique dans votre centre de données. Pour plus d'informations sur les armoires, voir Gestion des armoires.

En savoir plus :

- XClarity Administrator : Reconnaissance
- XClarity Administrator : Inventaire
- XClarity Administrator : Contrôle à distance

Surveillance du matériel

XClarity Administrator fournit une vue centralisée de l'ensemble des événements et alertes qui sont générés à partir des appareils gérés. Un événement ou une alerte est transmis à XClarity Administrator et s'affiche dans le journal des événements ou des alertes. Un récapitulatif de l'ensemble des événements et des alertes est visible dans le tableau de bord et la barre d'état. Les événements et les alertes d'un appareil spécifique sont disponibles dans la page de détails Alertes et Événements de cet appareil.

Pour plus d'informations sur la surveillance du matériel, voir Utilisation des événements, Utilisation des alertes.

En savoir plus : XClarity Administrator : Surveillance

Gestion de la configuration

Vous pouvez rapidement appliquer et pré-appliquer les accès de vos serveurs à l'aide d'une configuration cohérente. Les paramètres de configuration (tels que le stockage local, les cartes d'E-S, les paramètres d'amorçage, le microprogramme, les ports, ainsi que les paramètres de contrôleur de gestion et UEFI) sont enregistrés sous la forme d'un modèle de serveur qui peut être appliqué à un ou plusieurs serveurs gérés. Lorsque les modèles de serveur sont mis à jour, les modifications sont automatiquement déployées sur les serveurs concernés.

Les modèles de serveur intègrent également une prise en charge de la virtualisation des adresses d'E-S. Vous pouvez donc virtualiser les connexions Flex System Fabric ou réaffecter des serveurs sans interruption dans la matrice.

Pour plus d'informations sur la configuration des serveurs, voir Configuration des serveurs à l'aide de modèles de configuration.

En savoir plus :

- XClarity Administrator : du serveur au cluster
- XClarity Administrator : modèles de configuration

Conformité du microprogramme et mises à jour

La gestion du microprogramme est simplifiée grâce à l'affectation de stratégies de conformité du microprogramme aux appareils gérés. Lorsque vous créez et affectez une stratégie de conformité aux appareils gérés, XClarity Administrator surveille les modifications de l'inventaire pour ces appareils et marque tous ceux qui ne sont pas conformes.

Lorsqu'un appareil n'est pas conforme, vous pouvez utiliser XClarity Administrator pour appliquer et activer les mises à jour du microprogramme pour tous les dispositifs de cet appareil dans un référentiel de mises à jour du microprogramme que vous gérez.

Remarque : Pour actualiser le référentiel et télécharger les mises à jour du microprogramme, une connexion Internet est nécessaire. Si XClarity Administrator ne dispose d'aucune connexion à Internet, vous pouvez importer manuellement les mises à jour du microprogramme dans le référentiel.

Pour plus d'informations sur la mise à jour du microprogramme, voir Mise à jour du microprogramme sur les appareils gérés.

En savoir plus :

- XClarity Administrator : du serveur au cluster
- XClarity Administrator : mises à jour de microprogramme
- XClarity Administrator : Distribution des mises à jour de sécurité du microprogramme

Déploiement du système d'exploitation

Vous pouvez utiliser XClarity Administrator pour gérer un référentiel des images du système d'exploitation et déployer ces images simultanément sur jusqu'à 28 serveurs gérés.

Pour plus d'informations sur le déploiement de systèmes d'exploitation, voir Installation de systèmes d'exploitation sur des serveurs nus.

En savoir plus :

- XClarity Administrator : du serveur au cluster
- XClarity Administrator : déploiement du système d'exploitation

Gestion des utilisateurs

XClarity Administrator fournit un serveur d'authentification centralisé pour créer et gérer les comptes utilisateur et pour gérer et authentifier les données d'identification des utilisateurs. Le serveur d'authentification est créé automatiquement lorsque vous démarrez le serveur de gestion pour la première fois. Les comptes utilisateur que vous créez pour XClarity Administrator peuvent aussi être utilisés pour la connexion aux châssis et serveurs gérés en mode d'authentification gérée. Pour plus d'informations sur les utilisateurs, voir Gestion des comptes utilisateur.

XClarity Administrator prend en charge trois types de serveurs d'authentification :

- **Serveur d'authentification local**. Par défaut, XClarity Administrator est configuré pour utiliser le serveur d'authentification local qui se trouve sur le nœud de gestion.
- **Serveur LDAP externe**. Actuellement, seuls Microsoft Active Directory est pris en charge. Ce serveur doit se trouver sur un serveur Microsoft Windows externe connecté au réseau de gestion.Lorsqu'un serveur LDAP externe est utilisé, le serveur d'authentification local est désactivé.
- **fournisseur d'identité SAML 2.0 externe**. Actuellement, seul Microsoft Active Directory Federation Services (AD FS) est pris en charge. Outre la saisie d'un nom d'utilisateur et d'un mot de passe, l'authentification multifacteur peut être configurée pour offrir une sécurité accrue en exigeant un code PIN, la lecture d'une carte à puce et un certificat client.

Pour plus d'informations sur les types d'authentification, voir Gestion du serveur d'authentification.

Lorsque vous créez un compte utilisateur, vous affectez un groupe de rôles prédéfinis ou personnalisé au compte utilisateur pour contrôler le niveau d'accès accordé à cet utilisateur. Pour plus d'informations sur les groupes de rôles, voir Création d'un groupe du rôle personnalisé.

XClarity Administrator inclut un journal d'audit qui fournit un enregistrement historique des actions utilisateur, comme la connexion, la création d'utilisateurs ou la modification de mots de passe utilisateur. Pour plus d'informations sur le journal d'audit, voir Utilisation des événements.

Authentification d'appareil

XClarity Administrator utilise les méthodes suivantes pour authentifier les châssis et les serveurs gérés.

- **Authentification gérée**. Lorsque l'authentification gérée est activée, les comptes utilisateur que vous créez dans XClarity Administrator sont utilisés pour authentifier les châssis et les serveurs gérés.

  Pour plus d'informations sur les utilisateurs, voir Gestion des comptes utilisateur.

- **Authentification locale**. Lorsque l'authentification gérée est désactivée, les données d'identification qui sont définies dans XClarity Administrator sont utilisées pour authentifier les serveurs gérés. Les données d'identification stockées doivent correspondre à un compte utilisateur actif sur l'appareil ou dans Active Directory.

  Pour plus d'informations sur les données d'identification stockées, voir Gestion de données d'identification stockées.

Sécurité

Si votre environnement doit respecter les normes NIST SP 800-131A, XClarity Administrator peut vous aider à obtenir un environnement intégralement conforme.

XClarity Administrator prend en charge les certificats SSL auto-signés (qui sont émis par une autorité de certification interne) et les certificats SSL externes (qui sont émis par une autorité de certification privée ou commerciale).

Les pare-feux sur le châssis et les serveurs peuvent être configurés pour l'acceptation des demandes entrantes en provenance uniquement de XClarity Administrator.

Pour plus d'informations sur la sécurité, voir Implémentation d'un environnement sécurisé.

Service et support

XClarity Administrator peut être configuré pour la collecte et l'envoi automatique de fichiers de diagnostic à votre prestataire de services préféré, lorsque certains événements réparables se produisent dans XClarity Administrator et sur les appareils gérés. Vous pouvez choisir d'envoyer les fichiers de diagnostic à Lenovo Support à l'aide de l'Appel vers Lenovo ou à un autre prestataire de services via SFTP. Vous pouvez également collecter les fichiers de diagnostic manuellement, ouvrir un enregistrement de problème, et envoyer les fichiers de diagnostic au Lenovo Centre de support.

En savoir plus : XClarity Administrator : Service et support

Automatisation des tâches à l'aide de scripts

XClarity Administrator peut être intégré dans des plateformes externes de gestion et d'automatisation de niveau plus élevé, à l'aide d'API REST. Grâce aux API REST, XClarity Administrator s'intègre facilement à votre infrastructure de gestion existante.

Le kit d'outils PowerShell fournit une bibliothèque de cmdlets permettant d'automatiser la distribution et la gestion des ressources à partir d'une session Microsoft PowerShell. Le kit d'outils Python fournit une bibliothèque Python de commandes et d'API permettant d'automatiser la distribution et la gestion des ressources à partir d'un environnement OpenStack, tel qu'Ansible ou Puppet. Ces deux kits d'outils fournissent une interface avec des API REST XClarity Administrator pour automatiser des fonctions telles que :

- Connexion à XClarity Administrator
- Gestion et désactivation de la gestion de châssis, serveurs, dispositifs de stockage et commutateurs pour la partie supérieure de l'armoire (dispositifs)
- Collecte et affichage des données d'inventaire pour des appareils et des composants
- Déploiement d'une image du système d'exploitation sur un ou plusieurs serveurs
- Configuration de serveurs à l'aide de modèles de configuration
- Application des mises à jour du microprogramme à des appareils

Intégration à d'autres logiciels gérés

Les modules XClarity Administrator intègrent XClarity Administrator avec des logiciels de gestion tiers en vue d'assurer les fonctions de détection, surveillance, configuration et gestion afin de réduire le coût et la complexité les tâches d'administration du système courantes pour les appareils pris en charge.

Pour plus d'informations sur XClarity Administrator, consultez les documents suivants :
- Lenovo XClarity Integrator pour Microsoft System Center
- Lenovo XClarity Integrator pour VMware vCenter

Pour connaître les autres points à prendre en considération, voir Considérations relatives à la gestion dans la documentation en ligne de XClarity Administrator.

En savoir plus :
-  Présentation de Lenovo XClarity Integrator pour Microsoft System Center
-  Lenovo XClarity Integrator pour VMware vCenter

Documentation

La documentation XClarity Administrator est régulièrement mise à jour en ligne en anglais. Consultez Documentation en ligne XClarity Administrator pour connaître les informations et les procédures plus récentes.

La documentation en ligne est disponible dans les langues suivantes :
- Allemand (de)
- Anglais (en)
- Espagnol (es)
- Français (fr)
- Italien (it)
- Japonais (ja)
- Coréen (ko)
- Portugais (Brésil) (pt_BR)
- Russe (ru)
- Thaï (th)
- Chinois simplifié (zh_CN)
- Chinois traditionnel (zh_TW)

Vous pouvez modifier la langue de la documentation en ligne de plusieurs manières :

- Modifiez le paramètre de langue dans votre navigateur Web
- Ajoutez `?lang=`*<language_code>* à la fin de l'URL, par exemple, pour afficher la documentation en ligne en chinois simplifié :
  `http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/aug_product_page.html`**?lang=zh_CN**

Connexion à XClarity Administrator

Connexion à l'interface Web de Lenovo XClarity Administrator à l'aide d'un navigateur Web pris en charge.

Avant de commencer

Vérifiez que vous utilisez l'un des navigateurs Web pris en charge suivants :
- Chrome™ 48.0 ou supérieur (55.0 ou supérieur pour Console distante)
- Firefox® ESR 38.6.0 ou version ultérieure
- Microsoft® Internet Explorer® 11
- Microsoft Edge
- Safari® 9.0.2 ou supérieur (IOS7 ou supérieur et OS X)

Remarque : Le lancement des interfaces de contrôleur de gestion à partir de XClarity Administrator à l'aide du navigateur Web Safari n'est pas pris en charge.

Assurez-vous que vous vous connectez à l'interface Web de XClarity Administrator à partir d'un système disposant d'une connectivité réseau au nœud de gestion XClarity Administrator.

Procédure

Pour vous connecter à l'interface Web de XClarity Administrator, procédez comme suit.

Etape 1. Faites pointer votre navigateur sur l'adresse IP de XClarity Administrator.

Conseil : L'accès à l'interface Web s'effectue via une connexion sécurisée. Assurez-vous d'utiliser **https**.

- **Pour les conteneurs**. Utilisez l'adresse IPv4 spécifiée pour la variable ${ADDRESS} afin d'accéder à XClarity Administrator à l'aide de l'URL suivante :
  `https://<IPv4_address>/ui/login.html`

  Par exemple :
  `https://192.0.2.10/ui/login.html`

- **Pour les dispositifs virtuels**. L'adresse IP que vous utilisez dépend de l'installation de votre environnement.

  Si vous disposez de réseaux Eth0 et Eth1 sur des sous-réseaux distincts et si DHCP est utilisé sur les deux sous-réseaux, utilisez l'adresse IP d'*Eth1* lors de l'accès à l'interface Web pour la configuration initiale. Lorsque XClarity Administrator démarre pour la première fois, Eth0 et Eth1 obtiennent une adresse IP affectée par DHCP et la passerelle affectée par DHCP pour *Eth1* est définie comme passerelle XClarity Administrator par défaut.

  Utilisation d'une adresse IPv4 statique

  Si vous spécifiez une adresse IPv4 dans eth0_config, utilisez cette adresse IPv4 pour accéder à XClarity Administrator en utilisant l'URL suivante :
  `https://<IPv4_address>/ui/login.html`

  Par exemple :
  `https://192.0.2.10/ui/login.html`

  Utilisation d'un serveur DHCP configuré dans le même domaine de diffusion que XClarity Administrator

  Si un serveur DHCP est configuré dans le même domaine de diffusion queXClarity Administrator , utilisez l'adresse IPv4 qui s'affiche dans la console de machine virtuelle XClarity Administrator pour accéder à XClarity Administrator à l'aide de l'URL suivante :
  `https://<IPv4_address>/ui/login.html`

  Par exemple :
  `https://192.0.2.10/ui/login.html`

  Utilisation d'un serveur DHCP configuré dans un domaine de diffusion différent de XClarity Administrator

  Si un serveur DHCP n'est *pas* configuré dans le même domaine de diffusion, utilisez l'adresse IPv6 locale de liaison (LLA) affichée pour eEth0 (le réseau de gestion) dans la console de machine virtuelle XClarity Administrator pour accéder à XClarity Administrator, par exemple :

```
----------------------------------------
Lenovo XClarity Administrator  Version x.x.x
----------------------------------------

eth0   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.10  netmask 255.255.255.0  broadcast 192.0.2.55
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64   scopeid 0x20<link>
         ether 00:15:5d:0c:d1:92    txqueuelen 1000 (Ethernet)
         RX errors 0  dropped 0  overruns 0  frame 0

eth1   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.20  netmask 255.255.255.0  broadcast 192.0.2.130
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64  scopeid 0x20<link>
```

```
================================================================================
================================================================================

You have 150 seconds to change IP settings. Enter one of the following:
  1. To set a static IP address for Lenovo XClarity virtual appliance eth0 port
  2. To use a DHCP address for Lenovo XClarity virtual appliance eth0 port
  x. To continue without changing IP settings
  … …
```

Conseil : L'adresse IPv6 locale de liaison est dérivée de l'adresse MAC de l'interface.

Attention : Si vous configurez XClarity Administrator à distance, vous devez disposer d'une connectivité au même réseau de couche 2. Il doit être joint à l'aide d'une adresse non-routée jusqu'à ce que la configuration initiale soit terminée. Par conséquent, envisagez d'accéder à XClarity Administrator à partir d'une autre machine virtuelle disposant d'une connectivité à XClarity Administrator. Par exemple, vous pouvez accéder à XClarity Administrator à partir d'une autre machine virtuelle sur l'hôte sur lequel XClarity Administrator est installé.

– **Firefox :**

  Pour accéder à l'interface Web de XClarity Administrator à partir d'un navigateur Firefox, connectez-vous à l'aide de l'URL suivante. Notez que les crochets sont obligatoires lors de la saisie d'adresses IPv6.

  `https://[<IPv6_LLA>/ui/login.html]`

  Par exemple, en vous aidant de l'exemple précédent affiché pour Eth0, entrez l'URL suivante dans votre navigateur Web :

  `https://[fe80:21a:64ff:fe12:3456]/ui/login.html`

– **Internet Explorer :**

  Pour accéder à l'interface Web de XClarity Administrator à partir d'un navigateur Internet Explorer, connectez-vous à l'aide de l'URL suivante. Notez que les crochets sont obligatoires lors de la saisie d'adresses IPv6.

  `https://[<IPv6_LLA>%25<zone_index>]/ui/login.html`

  où *<zone_index>* est l'identificateur de l'adaptateur Ethernet connecté au réseau de gestion à partir de l'ordinateur sur lequel vous avez lancé le navigateur Web. Si vous utilisez un navigateur sous Windows, utilisez la commande `ipconfig` pour rechercher l'index de zone, qui affiché après le signe de pourcentage (%) dans la zone **Adresse IPv6 locale de liaison** de l'adaptateur. Dans l'exemple suivant, l'index de zone est « 30 ».

  ```
  PS C :> ipconfig
  Configuration IP Windows

  Adaptateur Ethernet vEthernet (teamVirtualSwitch) :

     Suffixe DNS spécifique à la connexion  . :
     Adresse IPv6 Link-local . . . . . : 2001:db8:56ff:fe80:bea3%30
     Adresse IPv4 autoconfiguration. . : 192.0.2.30
    Passerelle par défaut . . . . . :
  ```

  Si vous utilisez un navigateur sous Linux, utilisez la commande `ifconfig` pour rechercher l'index de zone. Vous pouvez également utiliser le nom de l'adaptateur (généralement Eth0) comme index de zone.

  Par exemple, en vous aidant des exemples affichés pour Eth0 et l'index de zone, entrez l'URL suivante dans votre navigateur Web :

  `https://[2001:db8:56ff:fe80:bea3%2530]/ui/login.html`

La page de connexion initiale de XClarity Administrator s'affiche :

Etape 2. Sélectionnez la langue souhaitée dans la liste déroulante **Langue**.

Remarque : Il est possible que les paramètres de configuration et les valeurs fournies par les appareils gérés soient disponibles uniquement en anglais.

Etape 3. Entrez un ID utilisateur et un mot de passe valides, puis cliquez sur **Se connecter**.

Lors de votre première connexion avec un compte utilisateur, vous êtes invité à modifier le mot de passe. Les mots de passe doivent satisfaire les critères suivants :

- (1) Doit contenir au moins un caractère alphabétique et ne peut pas avoir plus de deux caractères séquentiels, notamment des séquences de caractères alphabétiques, des chiffres et des touches de clavier QWERTY (par exemple, les séquences « abc », « 123 » et « asd » ne sont pas autorisées).
- (2) Doit contenir au moins un nombre (0 à 9).
- (3) Doit contenir au moins *deux* des caractères suivants :
  - Des caractères alphabétiques en majuscule (A – Z)
  - Des caractères alphabétiques en minuscule (a – z)
  - Des caractères spéciaux ; @ _ ! ’ $ & +
- (4) Ne doit pas répéter ou inverser le nom d’utilisateur.
- (5) Ne doit pas contenir plus de deux caractères consécutifs (par exemple, les séquences « aaa », « 111 » et « ... » ne sont pas autorisées).

Après avoir terminé

La page du tableau de bord de XClarity Administrator s'affiche :

Remarque : Si le système d'exploitation hôte est arrêté inopinément, vous pouvez recevoir une erreur d'authentification lorsque vous tentez de vous connecter à XClarity Administrator. Pour résoudre ce problème, restaurez XClarity Administrator à partir de la dernière sauvegarde pour accéder au serveur de gestion (voir Sauvegarde de Lenovo XClarity Administrator).

Vous pouvez effectuer les actions suivantes à partir du menu d'action utilisateur (ADMIN_USER) dans la barre de titre XClarity Administrator.

- Vous trouverez des informations concernant l'utilisation de XClarity Administrator dans le système d'aide incorporé en cliquant sur **Aide**.

  La documentation XClarity Administrator est régulièrement mise à jour en ligne en anglais. Consultez Documentation en ligne XClarity Administrator pour connaître les informations et les procédures plus récentes.
- Vous pouvez consulter la licence XClarity Administrator en cliquant sur **Licence**.
- Pour des informations sur la version de XClarity Administrator, cliquez sur **À propos de**.
- Vous pouvez modifier la langue de l'interface utilisateur en cliquant sur **Modifier la langue**.
- Pour vous déconnecter de la session en cours, cliquez sur **Déconnexion**.
- Vous pouvez soumettre des idées et des commentaires sur XClarity Administrator en cliquant sur **Envoyer des idées** ou **Envoyer l'avis**.
- Vous pouvez poser des questions et trouver des réponses sur le Site Web du forum de communauté Lenovo XClarity en cliquant sur **Visiter le forum**.

Astuces et techniques de l'interface utilisateur

Tenez compte de ces astuces et techniques lorsque vous utilisez l'interface utilisateur de Lenovo XClarity Administrator.

Affichage de plus ou moins de données par page

Vous pouvez modifier le nombre de lignes affichées par page à l'aide des liens situés dans le coin inférieur droit du tableau. Vous pouvez afficher **10**, **25**, **50** rangées ou **Toutes**

Recherche de données dans de grandes listes

La plupart des champs peuvent contenir jusqu'à 128 caractères.

Il existe plusieurs manières d'afficher un sous-ensemble d'une grande liste grâce à des critères spécifiques.

- Vous pouvez trier les lignes du tableau en cliquant sur les en-têtes de colonne.

  La modification de l'ordre de tri d'une colonne d'un tableau demeure au fil des sessions utilisateur.
- Vous pouvez utiliser les icônes **Filtrer par** et la liste déroulante **Afficher** disponible sur certaines pages pour afficher un sous-ensemble de données selon les critères sélectionnés.
- Vous pouvez affiner davantage le sous-ensemble en entrant un texte (par exemple, un nom ou une adresse IP) dans la zone **Filtres** pour trouver des données figurant dans n'importe quelle colonne disponible.

  Vous pouvez faire votre choix parmi les 10 dernières recherches en sélectionnant ces dernières dans la liste déroulante située en regard du champ **Filtres**. La dernière recherche active d'une page persiste au fil des sessions utilisateur.

Affichage des données de colonne

Si la taille des colonnes empêche le bon affichage de toutes les informations dans la cellule du tableau (ceci est indiqué par des points de suspension), vous pouvez afficher l'intégralité des informations dans une fenêtre contextuelle en pointant sur le texte de la cellule.

Configurer les colonnes du tableau

Vous pouvez configurer des tableaux pour afficher les informations importantes pour vous.

- Vous pouvez choisir les colonnes à afficher ou masquer en cliquant sur **Toutes les actions → Définir les colonnes**.
- Vous pouvez réorganiser les colonnes en faisant glisser les en-têtes de colonne vers l'emplacement souhaité.

Modification de la langue de l'interface utilisateur

Vous avez la possibilité de définir la langue de l'interface utilisateur lors de votre première connexion.

Une fois que vous êtes connecté, vous pouvez modifier la langue de l'interface utilisateur en cliquant sur le menu d'actions utilisateur (

), puis en cliquant sur **Modifier la langue**. Sélectionnez la langue que vous voulez afficher.

Remarque : Le système d'aide s'affiche dans la langue définie dans l'interface utilisateur

Obtenir de l'aide

XClarity Orchestrator propose plusieurs moyens d'obtenir de l'aide sur l'interface utilisateur.

- Certaines pages fournissent des détails supplémentaires sur une zone ou un état spécifique à l'aide des icônes **Aide** (
). Passez le curseur sur l'icône pour afficher une fenêtre contextuelle contenant des informations utiles.
- Pour obtenir de l'aide sur l'exécution d'actions spécifiques à partir de l'interface utilisateur, cliquez sur le menu d'actions utilisateur (

), puis cliquez sur **Aide**.

Utilisation de l'application Lenovo XClarity Mobile

Lenovo XClarity Administrator propose une application mobile pour les appareils Android et iOS. Vous pouvez utiliser l'application Lenovo XClarity Mobile pour surveiller de manière sécurisée les systèmes physiques, obtenir des notifications et des alertes d'état en temps réel et agir sur les tâches de niveau système courantes. L'application peut également se connecter directement via un port USB activé à un serveur ThinkSystem et fournir une capacité virtuelle LCD.

En savoir plus :  Présentation de l'application Lenovo XClarity Mobile

Avec l'application XClarity Mobile, vous pouvez effectuer les opérations suivantes :
- Configurer les paramètres et les propriétés réseau
- Afficher le récapitulatif d'état de chaque XClarity Administrator connecté.
- Afficher le récapitulatif d'état de tous les appareils gérés.
- Afficher les vues graphiques (cartes) des châssis, serveurs rack et dispositifs de stockage.
- Affichage des groupes de ressources qui sont définis sur le XClarity Administrator.
- Affichez les informations de port de commutateur de l'armoire et modifiez l'état du port configuré.
- Surveillez l'inventaire et l'état détaillé de chaque appareil géré.
- Surveiller les événements d'audit, de matériel et de gestion, les alertes et les travaux.
- Activer ou désactiver le voyant de localisation sur un appareil géré.
- Mettre sous tension, hors tension, redémarrer ou réinstaller un appareil géré.
- Déclencher la collecte de données de diagnostic.
- Afficher des informations relatives à la garantie et à l'état de l'appareil
- Configurer la notification de problème automatique via l'Appel vers Lenovo.
- Afficher le récapitulatif des tickets de maintenance ouverts et supprimer des tickets de maintenance
- Acheminer les notifications d'événement sur votre appareil mobile (voir Acheminement des événements vers des appareils mobiles).
- Afficher le récapitulatif des utilisateurs actifs et de l'utilisation des ressources système
- Envoyer des commentaires sur cette application mobile au Support Lenovo.
- Connectez votre appareil mobile directement à un serveur ThinkSystem pour gérer le serveur à l'aide de l'application XClarity Mobile (pour les appareils qui prennent en charge le tethering USB).
- Téléchargez les données de maintenance Lenovo XClarity Controller lorsque l'appareil mobile est connecté à un serveur ThinkSystem.

Vous pouvez également connecter votre appareil mobile directement aux serveurs ThinkSystem puis lancer l'application XClarity Mobile et vous connecter au contrôleur de gestion de la carte mère du serveur à l'aide des mêmes données d'identification Web et CLI. Un menu d'informations et des actions supplémentaire sont disponibles, notamment :

- Service
  - Partager des informations récapitulatives via e-mail ou une autre méthode proposée par l'appareil mobile
  - Effacer le journal des événements et du journal d'audit
  - Télécharger le journal des événements et du journal d'audit dans le stockage local de l'appareil mobile ou transmission du journal à l'aide de l'une des méthodes proposées par l'appareil mobile
  - Télécharger le fichier de maintenance BMC FFDC dans le stockage local de l'appareil mobile ou transmission du fichier à l'aide de l'une des méthodes proposées par l'appareil mobile
  - Afficher un graphique historique relatif à l'usage de l'alimentation, des données thermiques et du système
  - Activer le mode de maintenance « One-Touch » qui fournit un récapitulatif immédiat des alertes actives et des informations d'appareil critiques
- Configuration et configuration initiale
  - Gérer un nouveau dispositif à l'aide du XClarity Administrator sélectionné

  - Configurer les propriétés serveur, comme l'emplacement et les informations de contact de la configuration initiale
  - Afficher et modifier des paramètres d'interface réseau BMC IPv4 et IPv6 BMC
  - Indiquer des paramètres relatifs à l'ordre d'amorçage et à l'amorçage unique
  - Modifier l'affectation d'un port USB du panneau frontal
  - Afficher le nombre de réamorçages du serveur et la durée de mise sous tension totale
- Actions d'alimentation
  - Mise sous tension ou hors tension du serveur, redémarrage du serveur, ou déclenchement NMI
  - Réinitialiser le module BMC

Conseil : Une fois l'application ouverte, vous devez l'actualiser afin de voir l'état, l'inventaire, les événements et les travaux mis à jour.

Conditions prérequises

- Les tablettes iOS sont prises en charge avec une résolution d'écran iPhone uniquement. Les tablettes Android ne sont actuellement pas prises en charge.
- Les systèmes d'exploitation mobiles pris en charge sont les suivants :
  - Android 7 – 11
  - iOS 10 et versions ultérieures

    Remarques :

    - Android 5 est pris en charge uniquement pour XClarity Mobile version 2.3.0 et versions précédentes.
    - La reconnaissance faciale utilisée sur les appareils/XR/XS de iPhone X n'est pas prise en charge.
- Vérifiez qu'une connexion réseau est disponible depuis votre appareil mobile vers les instances de XClarity Administrator. L'utilisation d'une solution de réseau privé virtuel peut être nécessaire. Pour obtenir de l'aide, contactez votre administrateur réseau.
- Importez le certificat de l'autorité de certification pour chaque instance de XClarity Administrator.

  Important : Toutes les connexions à XClarity Administrator utilisent HTTPS. Cependant, une chaîne de certificats valide doit exister pour que la connexion soit considérée comme sécurisée et que les données puissent être transmises à l'appareil mobile. Pour créer une chaîne de certificats sécurisée, vous devez importer le certificat d'autorité de certification fonction auto-signé XClarity Administrator sur l'appareil mobile.

  Pour importer le certificat de l'autorité de certification auto-signé pour *chaque XClarity Administrator instance* sur l'appareil mobile, procédez comme suit.

  1. Téléchargez le certificat de l'autorité de certification sur un système local :
     a. Connectez-vous à l'instance de XClarity Administrator à l'aide d'un navigateur Web sur votre système local.
     b. Dans la barre de menu XClarity Administrator, cliquez sur **Administration → Sécurité** pour afficher la page Sécurité.
     c. Cliquez sur **Autorité de certification** dans la section Gestion des certificats. La page Autorité de certification s'affiche.
     d. Cliquez sur **Télécharger le certificat racine de l'autorité de certification**.

        Attention : Normalement, il n'est pas nécessaire de cliquer sur **Regénérer le certificat racine de l'autorité de certification** pour effectuer cette procédure. Cela pourrait interrompre la communication avec les appareils gérés si la procédure appropriée n'est pas respectée. Pour plus d'informations, voir Utilisation de certificats de sécurité.

e. Cliquez sur **Enregistrer sous der** ou **Enregistrer sous pem** pour enregistrer le certificat de l'autorité de certification en tant que fichier DER ou PEM sur votre système local. Le format PEM fonctionne dans la plupart des cas.

2. Transférez le fichier de certificat de l'autorité de certification sur votre appareil mobile, par exemple, au moyen d'un référentiel de stockage accessible (comme Dropbox™), d'un e-mail ou du transfert de fichier via un câble connecté.
3. Importez le certificat sécurisé de l'autorité de certification :
   - (Android) Il suffit généralement de sélectionner **Settings → Security → Install** depuis le stockage du téléphone, puis de sélectionnant le fichier de certificat que vous avez téléchargé.

     Important : Si le certificat de l'autorité de certification que vous avez installé n'est pas signé par un tiers, un message indiquant que le `réseau est peut-être surveillé par un tiers inconnu` s'affiche sur les appareils Android. Étant donné que le certificat de l'autorité de certification est généré dans votre environnement sécurisé, vous pouvez ignorer ce message en toute sécurité. Avant d'ignorer le message, assurez-vous qu'il concerne le certificat de l'autorité de certification de XClarity Administrator.
   - (iOS) Ouvrez l'e-mail sur votre appareil mobile, puis cliquez sur le lien du document afin d'importer le certificat sécurisé de l'autorité de certification.

   Attention : Pour iOS 10.3 et ultérieur, les certificats importés ne sont pas sécurisés par défaut. Pour sécuriser les certificats, sélectionnez **Paramètres → Général → À propos de → Paramètres de sécurisation de certificat**, puis activez la sécurisation de certificat.

Installation et configuration

1. Téléchargez l'application XClarity Mobile depuis iTunes App Store (iOS) ou Google Play Store (Android).
2. Pour installer l'application, suivez les instructions sur l'appareil mobile.

   Important : Un code de sécurité de niveau système d'exploitation mobile pour le déverrouillage de l'accès écran est requis pour utiliser l'application XClarity Mobile. Si aucun n'est déjà configuré, vous êtes invité à en définir un lors de l'installation.
3. Cliquez sur **Paramètres** pour ajouter ou modifier les connexions à plusieurs instances de XClarity Administrator à l'aide de la reconnaissance automatique ou en fournissant une adresse IP et des données d'identification utilisateur, définir un code PIN pour l'application, modifier les paramètres du journal des événements et du journal d'audit, et sélectionner votre langue préférée.

Connexion directement aux serveurs ThinkSystem

Les serveurs Lenovo ThinkSystem comportent un port USB de panneau frontal sur lequel vous pouvez brancher votre appareil mobile pour fournir des fonctionnalités similaires à celles qui étaient disponibles sur le panneau d'affichage LCD des informations système des autres serveurs Lenovo.

Pour gérer un serveur ThinkSystem en vous connectant directement au serveur, procédez comme suit.

1. Faites passer l'USB du panneau frontal du serveur de l'Hôte vers BMC en procédant de l'une des manières suivantes.
   a. Depuis l'interface CLI du contrôleur de gestion, exécutez la commande `usbfp`
   b. Dans l'interface Web du contrôleur de gestion, cliquez sur **Configuration BMC → Réseau → USB panneau frontal vers Gestion**.
   c. Maintenez enfoncé pendant 3 secondes le voyant de localisation bleu jusqu'à ce qu'il clignote toutes les deux secondes.
2. Branchez le câble USB de votre téléphone sur le port USB de panneau frontal sur le serveur ThinkSystem.
3. Sur votre appareil mobile, activez le tethering USB.

a. Pour l'iOS, cliquez sur **Paramètres → Cellulaire → Hotspot personnel**.
b. Pour Android, cliquez sur **Paramètres → Hotspot mobile et connexion → Connexion USB**.

4. Sur votre appareil mobile, lancez l'application XClarity Mobile.
5. Si la reconnaissance automatique est désactivée, cliquez sur **Discovery** sur la page USB Discovery afin de vous connecter au contrôleur de gestion du serveur et de collecter des informations, telles que l'inventaire, la santé, le microprogramme, la configuration réseau, et une liste des derniers événements actifs.

Astuce :

- Assurez-vous d'utiliser un câble USB de haute qualité qui prend en charge les données et l'alimentation. Notez que certains câbles fournis avec les appareils mobiles servent uniquement à des fins d'alimentation.

  Remarque : Pour vous connecter au système ThinkSystem SD530, vous devez également utiliser un câble ou une carte USB à USB micro de qualité.
- Le serveur relié par USB doit être sous tension pour indiquer l'ensemble des statistiques concernant la tension, la température et l'utilisation des cartes d'état récapitulatives.
- Si le serveur relié par USB ne comporte pas de voyant/bouton d'identification « bleu » externe sur le panneau frontal, vous devez utiliser l'interface Web du contrôleur de gestion ou l'interface CLI pour modifier la sélection de port USB de panneau frontal, si nécessaire.
- Les modifications apportées à l'interface réseau du contrôleur de gestion depuis l'application XClarity Mobile prennent effet immédiatement sans qu'il soit nécessaire de redémarrer le contrôleur de gestion. Par exemple, si l'interface IPv4 est définie sur DHCP au lieu d'une adresse statique, elle obtient immédiatement qu'une adresse DHCP lui soit affectée.
- Sous l'onglet Newsfeed, la carte « Derniers événements actifs » affiche initialement jusqu'à trois événements actifs répertoriés sous l'onglet Événements actifs du contrôleur de gestion. Sur l'application mobile, si vous cliquez sur cette carte, tous les événements actifs sont affichés. Notez qu'il s'agit d'une liste des événements actifs et résolus, et non de la liste complète des événements.

Utilisation du mode de démonstration

Vous pouvez activer le **Mode de démonstration** sur la page Paramètres afin d'entrer des données de démonstration pour l'application XClarity Mobile pour deux instances de XClarity Administrator, y compris les armoires et le châssis. Dans ce mode, vous pouvez afficher le récapitulatif de l'état des instances XClarity Administrator, afficher l'état et l'inventaire détaillés des appareils, et surveiller les événements et les alertes. Cependant, les actions de gestion, comme la mise sous tension et hors tension, ne sont pas prises en charge.

Remarques :

- Vous pouvez activer le mode de démonstration uniquement lorsqu'il n'existe aucune connexion aux instances réelles de XClarity Administrator.
- Vous ne pouvez pas ajouter des connexions aux instances réelles de XClarity Administrator lorsque le mode de démonstration est activé.

Recherche

Vous pouvez utiliser la zone **Recherche** pour afficher les appareils gérés avec un nom ou un état spécifique (critique, avertissement, ou normal). Par exemple, si vous effectuez une recherche sur « crit », seuls les appareils à l'état critique et donc le nom inclue « crit » sont affichés.

Résolution des problèmes

incidents liés à l'installation :

- L’application mobile Android est « signée » avec une clé sécurisée pour améliorer la sécurité. La taille de clé sécurisée a été étendue dans la nouvelle édition. Etant donné que l’application signée ne correspond pas à la signature des applications antérieures, le processus de sécurité d'installation Android empêche la mise à jour automatique.

  Pour mettre à jour l’application mobile, désinstallez la version actuelle de l’application mobile, téléchargez la dernière version de l’application Android dans le magasin des application et réinstallez l’application. Sur la plupart des appareils Android, l’application peut être désinstallée à l’aide de l'élément de menu **Paramètres → Applications → Gestionnaire d’applications**.

Problèmes de connectivité :

- La fonction de tethering USB dans iOS 14, 14.0.1 et 14.0.2 ne fonctionne pas correctement, par conséquent, la fonction de tethering de l’application Lenovo XClarity Mobile n’est pas disponible pour ces versions iOS. Cela affecte uniquement la gestion d'appareil portatif avec connexion USB dans le centre de données. La gestion à distance à l’aide d’appareils mobiles qui prennent en charge les communications cellulaires et Wi-Fi n'est pas affectée et peut être utilisée pour connecter et collecter des données à partir de XClarity Administrator ainsi que pour effectuer des actions de gestion sur des appareils gérés.

  Si la fonction de gestion à des appareils portatifs avec connexion USB est nécessaire, n’effectuez pas la mise à niveau vers iOS 14.

  Cette notification sera mise à jour lorsque Apple aura résolu le problème avec iOS 14.
- XClarity Mobile requiert une connexion réseau disponible depuis votre appareil mobile aux instances de XClarity Administrator. L'utilisation d'une solution de réseau privé virtuel peut être nécessaire. Pour obtenir de l'aide, contactez votre administrateur réseau.
- Les connexions depuis votre appareil mobile à chaque instance de XClarity Administrator nécessitent une chaîne de certificats sécurisée. Consultez la documentation en ligne pour savoir comment télécharger et installer les certificats sécurisés de l'autorité de certification sur votre appareil mobile.

  Si le certificat de l'autorité de certification que vous avez installé n'est pas signé par un tiers, un message indiquant que le réseau est peut-être surveillé par un tiers inconnu s'affiche. Étant donné que le certificat de l'autorité de certification est généré dans votre environnement sécurisé, vous pouvez ignorer ce message en toute sécurité. Avant d'ignorer le message, assurez-vous qu'il concerne le certificat de l'autorité de certification de XClarity Administrator.
- Lorsque vous basculez votre appareil mobile d'un réseau privé virtuel vers un réseau local ou inversement, vous pouvez voir un message indiquant que la passerelle sécurisée a rejeté la tentative de connexion. Une nouvelle tentative de connexion à la même passerelle ou à une autre passerelle sécurisée est nécessaire, ce qui implique une nouvelle authentification. Connectez-vous à Lenovo XClarity Mobile pour continuer à utiliser l'application.

Problèmes liés à la sécurité :

- Si vous oubliez votre code PIN, désinstallez et réinstallez l'application XClarity Mobile. Ensuite, rétablissez toutes les connexions.
- Si vous effacez les données d'identification sur un appareil Android, la clé de chiffrement est effacée. Vous devez rétablir toutes les connexions.

Problèmes liés aux événements :

- Par défaut, le journal des événements affiche les événements de matériel et de gestion qui ont été reçus au cours de dernières 24 heures, et le journal d'audit affiche les événements d'audit qui ont été reçus au cours des 2 dernières heures. Si aucun événement n'a été reçu au cours des périodes sélectionnées, le journal des événements et le journal d'audit ne s'affichent pas sur la page Surveillance de XClarity Mobile.
- Si vous avez configuré l'acheminement d'événement dans XClarity Administrator pour l'envoi des événements vers un compte de messagerie, les liens contenus dans l'e-mail peuvent ne pas fonctionner

sur les appareils Android. Assurez-vous que votre version d'Android et votre application de messagerie prennent en charge les hyperliens. Si les hyperliens ne sont pas pris en charge, utilisez une autre application de messagerie.

Problèmes liés au système d’aide :

- Sur certains appareils, le système d’aide ne s'adapte pas correctement à la taille de l’écran. Utilisez les boutons de commande du système d’aide pour optimiser et réduire la page.

Chapitre 2. Administration de Lenovo XClarity Administrator

Plusieurs tâches d'administration, telles que l'ajout d'utilisateurs ou l'affichage de travaux, sont disponibles à partir de Lenovo XClarity Administrator.

Gestion de l'authentification et de l'autorisation

Lenovo XClarity Administrator fournit des mécanismes de sécurité permettant de vérifier les données d'identification d'un utilisateur et de contrôler l'accès à des ressources et à des tâches.

Gestion du serveur d'authentification

Par défaut, Lenovo XClarity Administrator utilise un serveur de protocole LDAP (Lightweight Directory Access Protocol) local pour authentifier les données d'identification de l'utilisateur.

À propos de cette tâche

Serveurs d'authentification pris en charge

Le *serveur d'authentification* est un registre utilisateur utilisé pour authentifier les données d'identification de l'utilisateur. Lenovo XClarity Administrator prend en charge les types de serveurs d'authentification suivants.

- **Serveur d'authentification local**. Par défaut, XClarity Administrator est configuré pour utiliser le serveur LDAP (Lightweight Directory Access Protocol) intégré qui réside sur le serveur de gestion.
- **Serveur LDAP externe**. Actuellement, seulement Microsoft Active Directory et OpenLDAP sont pris en charge. Ce serveur doit se trouver sur un serveur Microsoft Windows externe connecté au réseau de gestion. Lorsqu'un serveur LDAP externe est utilisé, le serveur d'authentification local est désactivé.

  Attention : Pour configurer la méthode de liaison d'Active Directory afin qu'elle utilise des données d'identification de connexion, le contrôleur de gestion de la carte mère de chaque serveur géré doit exécuter un microprogramme de septembre 2016 ou ultérieur.
- **Système de gestion d'identité externe**. Actuellement, seul CyberArk est pris en charge.

  Si des comptes utilisateur destinés à un serveur ThinkSystem ou ThinkAgile sont intégrés à CyberArk, lors de la configuration initiale des serveurs pour la gestion (avec authentification gérée ou locale), XClarity Administrator peut recueillir les données d'identification auprès de CyberArk pour se connecter au serveur. Avant de pouvoir recueillir les données d'identification de CyberArk, les chemins d'accès à CyberArk doivent être définis dans XClarity Administrator. Une confiance mutuelle doit être établie entre CyberArk et XClarity Administrator à l'aide d'une authentification mutuelle TLS via des certificats clients.
- **fournisseur d'identité SAML externe**. Actuellement, seul Microsoft Active Directory Federation Services (AD FS) est pris en charge. Outre la saisie d'un nom d'utilisateur et d'un mot de passe, l'authentification multifacteur peut être configurée pour offrir une sécurité accrue en exigeant un code PIN, la lecture d'une carte à puce et un certificat client. Lorsqu'un fournisseur d'identité SAML externe est utilisé, le serveur d'authentification local n'est pas désactivé. Les comptes utilisateur locaux sont requis pour se connecter directement à un châssis ou à un serveur géré (sauf si l'Encapsulation est activé sur cet appareil), pour l'authentification d'API REST et PowerShell, ainsi que pour la récupération si l'authentification externe n'est pas disponible.

  Vous pouvez choisir d'utiliser à la fois un serveur LDAP externe et un fournisseur d'identité externe. Si les deux sont activés, le serveur LDAP externe est utilisé pour se connecter directement aux appareils gérés, et le fournisseur d'identité est utilisé pour se connecter au serveur de gestion.

Authentification d'appareil

Par défaut, les appareils sont gérés par XClarity Administrator authentification gérée pour la connexion aux appareils. Lors de la gestion de serveurs rack et de châssis Lenovo, vous pouvez choisir d'utiliser l'authentification locale ou l'authentification gérée pour vous connecter aux appareils.

- Lorsque l'*authentification locale* est utilisée pour les serveurs rack, les châssis Lenovo et les commutateurs d'armoire, XClarity Administrator utilise des données d'identification stockées pour l'authentification sur l'appareil. Les *données d'identification stockées* peuvent être un compte utilisateur actif sur l'appareil ou un compte utilisateur dans un serveur Active Directory.

  Vous devez créer des données d'identification stockées dans XClarity Administrator qui correspondent à un compte utilisateur active sur l'appareil ou un compte utilisateur dans un serveur Active Directory avant de gérer l'appareil à l'aide de l'authentification locale (voir Gestion de données d'identification stockées dans la documentation en ligne XClarity Administrator).

  Remarques :

  – Les appareils RackSwitch prennent en charge uniquement les données d'identification stockées pour l'authentification. Les données d'identification utilisateur XClarity Administrator stockées ne sont pas prises en charge.
- L'*authentification gérée* vous permet de gérer et de surveiller plusieurs appareils à l'aide des données d'identification dans le serveur d'authentification XClarity Administrator au lieu des données d'identification locales. Lorsqu'un appareil (autre que des serveurs ThinkServer, System x M4 et des commutateurs) est géré par authentification gérée, XClarity Administrator configure l'appareil géré et ses composants installés afin d'utiliser le serveur d'authentification XClarity Administrator pour la gestion centralisée.

  – Lorsque l'authentification gérée est activée, vous pouvez gérer des appareils à l'aide de saisies manuelles ou de données d'identification stockées (voir Gestion des comptes utilisateur et dans la documentation en ligne de XClarity Administrator).

    Les données d'identification stockées sont utilisées uniquement jusqu'à ce que XClarity Administrator configure les paramètres LDAP sur l'appareil. Ensuite, toute modification apportée aux données d'identification stockées n'a aucun impact sur la gestion ou la surveillance de cet appareil.

    Remarque : Lorsque l'authentification gérée est activée pour un appareil, vous ne pouvez pas modifier les données d'identification stockées pour cet appareil à l'aide de XClarity Administrator.

  – Si un serveur LDAP local ou externe est utilisé comme serveur d'authentification XClarity Administrator, les comptes utilisateur définis dans le serveur d'authentification sont utilisés pour se connecter à XClarity Administrator, aux modules CMM et aux contrôleurs de gestion de la carte mère dans le domaine XClarity Administrator. Les CMM locaux et les comptes utilisateur du contrôleur de gestion sont désactivés.

  – Si un fournisseur d'identité SAML 2.0 est utilisé comme serveur d'authentification XClarity Administrator, les comptes SAML ne sont pas accessibles pour les appareils gérés. Cependant, lorsque vous utilisez un fournisseur d'identité SAML et un serveur LDAP ensemble et que le fournisseur d'identité utilise des comptes qui existent dans le serveur LDAP, les comptes utilisateur LDAP peuvent être utilisés pour se connecter à des appareils gérés, tandis que des méthodes d'authentification plus avancées qui sont fournies par SAML 2.0 (comme l'authentification à plusieurs facteurs et la connexion unique) peuvent être utilisées pour la connexion à XClarity Administrator.

  – L'authentification unique permet à un utilisateur qui est déjà connecté à XClarity Administrator de se connecter automatiquement au contrôle de gestion de la carte mère. La connexion unique est activée par défaut lorsqu'un serveur ThinkSystem ou ThinkAgile est amené dans la gestion par XClarity Administrator (sauf si le serveur est géré avec des mots de passe CyberArk). Vous pouvez configurer le paramètre global pour activer ou désactiver la connexion unique pour tous les serveurs ThinkSystem et ThinkAgile gérés. L'activation de la connexion unique pour un serveur ThinkSystem et ThinkAgile remplace le paramétrage global pour tous les serveurs ThinkSystem et ThinkAgile (voir).

Remarque : La connexion unique est automatiquement désactivée lorsque vous faites appel au système de gestion d'identité CyberArk pour vous connecter.

- Lorsque l'authentification gérée est activée pour les serveurs ThinkSystem SR635 et SR655 :
  - Le microprogramme du contrôleur de gestion de la carte mère prend en charge jusqu'à cinq rôles utilisateur LDAP. XClarity Administrator ajoute ces rôles utilisateur LDAP aux serveurs lors de la gestion : **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin** et **lxc-os-admin**.

    Les utilisateurs doivent être affectés à au moins l'un des rôles utilisateur LDAP spécifiés pour pouvoir communiquer avec les serveurs ThinkSystem SR635 et SR655.
  - Le microprogramme du contrôleur de gestion ne prend pas en charge les utilisateurs LDAP dont le nom d'utilisateur est identique à celui de l'utilisateur local du serveur.
- Pour les serveurs ThinkServer et System x M4, le serveur d'authentification XClarity Administrator n'est pas utilisé. À la place, un compte IPMI est créé sur l'appareil avec le préfixe « LXCA_ » suivi d'une chaîne aléatoire. (Les comptes utilisateur IPMI locaux ne sont pas désactivés.) Lorsque vous annulez la gestion d'un serveur ThinkServer, le compte utilisateur « LXCA_ » est désactivé, et le préfixe « LXCA_ » est remplacé par le préfixe « DISABLED_ ». Pour déterminer si un serveur ThinkServer est géré par une autre instance, XClarity Administrator recherche les comptes IPMI ayant le préfixe « LXCA_ ». Si vous choisissez de forcer la gestion d'un serveur ThinkServer géré, tous les comptes IPMI sur l'appareil avec le préfixe « LXCA_ » sont désactivés et renommés. Pensez à supprimer manuellement les comptes IPMI qui ne sont plus utilisés.

  Si vous utilisez des données d'identification saisies manuellement, XClarity Administrator crée automatiquement des données d'identification stockées et utilise ces dernières pour gérer l'appareil.

  Remarques : Lorsque l'authentification gérée est activée pour un appareil, vous ne pouvez pas modifier les données d'identification stockées pour cet appareil à l'aide de XClarity Administrator.
  - Chaque fois que vous gérez un appareil en utilisant des données d'identification saisies manuellement, de nouvelles données d'identification stockées sont créées pour cet appareil, même si d'autres données d'identification stockées ont été créées pour cet appareil lors d'un processus de gestion précédent.
  - Lorsque vous annulez la gestion d'un appareil, XClarity Administrator ne supprime pas les données d'identification stockées qui ont été créées automatiquement pour cet appareil lors du processus de gestion.

Compte de récupération

Si vous spécifiez un mot de passe de récupération, XClarity Administrator désactive le CMM local ou compte utilisateur du contrôleur de gestion et crée un nouveau compte utilisateur de récupération (`RECOVERY_ID`) sur l'appareil à des fins d'authentification ultérieure. Si le serveur de gestion échoue, vous pouvez utiliser le compte `RECOVERY_ID` pour vous connecter à l'appareil et prendre des mesures de récupération nécessaires pour restaurer les fonctions de gestion des comptes sur l'appareil jusqu'à ce que le nœud de gestion soit restauré ou remplacé.

Si vous annulez la gestion d'un appareil qui possède un compte utilisateur `RECOVERY_ID`, tous les comptes utilisateur locaux sont activés, et le compte `RECOVERY_ID` est supprimé.

- Si vous modifiez les comptes utilisateur locaux désactivés (par exemple, si vous modifiez un mot de passe), les modifications n'ont aucune incidence sur le compte `RECOVERY_ID`. En mode d'authentification gérée, le compte `RECOVERY_ID` est le seul compte utilisateur activé et opérationnel.
- Vous ne devez utiliser le compte `RECOVERY_ID` qu'en cas d'extrême nécessité, par exemple si le serveur de gestion échoue ou si un problème réseau empêche l'appareil de communiquer avec XClarity Administrator pour authentifier des utilisateurs.

- Le mot de passe `RECOVERY_ID` est spécifié lorsque vous découvrez l'appareil. Veillez à noter ce mot de passe pour un usage ultérieur.

Pour plus d'informations sur la récupération de la gestion des dispositifs, voir « Reprise de la gestion avec un module CMM après une défaillance du serveur de gestion » à la page 233, « Récupération de la gestion du serveur au format tour après une défaillance du serveur de gestion » à la page 286.

Configuration d'un serveur d'authentification LDAP externe

Vous pouvez choisir d'utiliser un serveur d'authentification externe LDAP au lieu du serveur d'authentification Lenovo XClarity Administrator local sur le nœud de gestion.

Avant de commencer

La configuration initiale de XClarity Administrator doit être effectuée avant la configuration du serveur d'authentification externe.

Les serveurs d'authentification externes suivants sont pris en charge :

- OpenLDAP
- Microsoft Active Directory. Ils doivent se trouver sur un serveur Microsoft Windows externe connecté au réseau de gestion et/ou au réseau de données

Vérifiez que tous les ports requis pour le serveur d'authentification externe sont ouverts sur le réseau et les pare-feu. Pour plus d'informations sur les exigences liées aux ports, voir Disponibilité de port dans la documentation en ligne de XClarity Administrator.

Vous devez créer ou renommer des groupes de rôles sur le serveur d'authentification local pour qu'ils correspondent aux groupes définis sur le serveur d'authentification externe.

Vérifiez qu'un ou plusieurs utilisateurs disposant des droits **lxc-recovery** sont présents dans le serveur d'authentification local. Vous pouvez utiliser ce compte utilisateur local pour vous authentifier directement auprès de XClarity Administrator si une erreur de communication se produit avec le serveur LDAP externe.

Remarque : Si XClarity Administrator est configuré pour utiliser un serveur d'authentification externe, la page Gestion des utilisateurs dans l'interface Web de XClarity Administrator est désactivée.

Attention : Pour que Active Directory configure la méthode de liaison d' afin qu'elle utilise des données d'identification de connexion, le contrôleur de gestion de la carte mère de chaque serveur géré doit exécuter un microprogramme de septembre 2016 ou ultérieur.

XClarity Administrator vérifie la connectivité toutes les 5 minutes afin de maintenir la connectivité aux serveurs LDAP externes configurés. Les environnements comportant un grand nombre de serveurs LDAP peuvent constater une utilisation UC élevée pendant cette vérification de connectivité. Pour obtenir de meilleures performances, assurez-vous que la plupart ou l'ensemble des serveurs LDAP du domaine sont accessibles, ou définissez la méthode de sélection du serveur d'authentification sur **Utiliser des serveurs préconfigurés** et indiquez uniquement des serveurs LDAP connus et accessibles.

Procédure

Pour configurer XClarity Administrator afin qu'il utilise un serveur d'authentification externe, procédez comme suit.

Etape 1. Configurez la méthode d'authentification de l'utilisateur pour Microsoft Active Directory ou OpenLDAP.

Si vous choisissez d'utiliser l'authentification non sécurisée, aucune configuration supplémentaire n'est requise. Les contrôleurs de domaine Windows Active Directory ou OpenLDAP utilisent l'authentification LDAP non sécurisée par défaut.

Si vous choisissez d'utiliser l'authentification LDAP sécurisée, vous devez configurer les contrôleurs de domaine afin de permettre l'authentification LDAP sécurisée. Pour plus d'informations sur la configuration de l'authentification LDAP sécurisée dans Active Directory, voir le Article à propos du certificat LDAP sur SSL (LDAPS) sur le site Web Microsoft TechNet.

Pour vérifier que les contrôleurs de domaine Active Directory sont configurés pour l'utilisation de l'authentification LDAP sécurisée :

- Recherchez l'événement `LDAP sur Secure Sockets Layer (SSL) est désormais disponible` dans la fenêtre Observateur d'événements des contrôleurs de domaine.
- Utilisez l'outil Windows `ldp.exe` pour tester la connectivité LDAP sécurisée avec les contrôleurs de domaine.

Etape 2. Importez le certificat du serveur Active Directory ou OpenLDAP ou le certificat racine de l'autorité de certification qui a signé le certificat du serveur.

a. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Sécurité**.

b. Cliquez sur **Certificats sécurisés** dans la section Gestion des certificats.

c. Cliquez sur l'icône **Créer** ( ) pour ajouter un certificat.

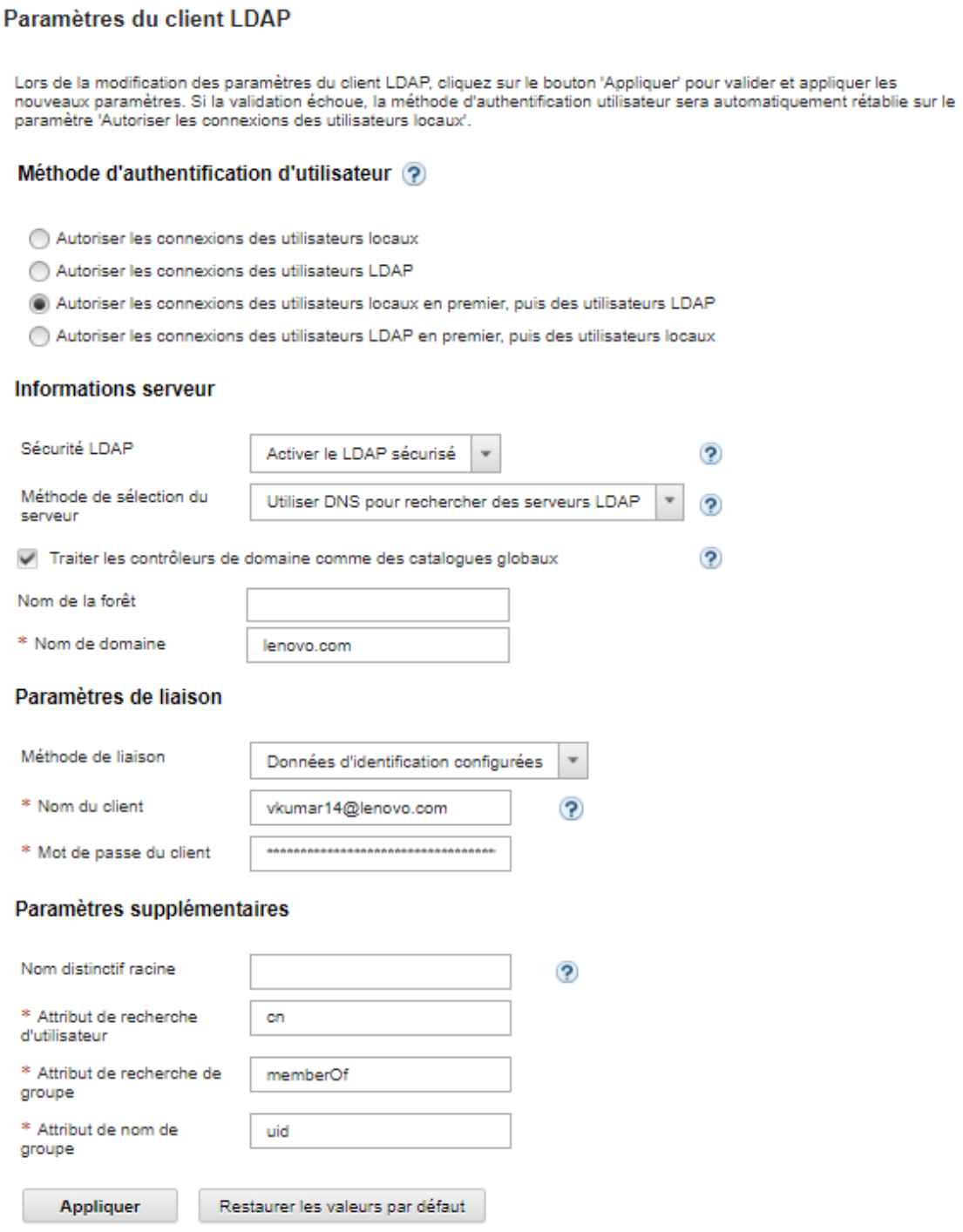
d. Recherchez le fichier ou collez le texte du certificat au format PEM.

e. Cliquez sur **Créer**.

Etape 3. Configurez le client LDAP XClarity Administrator :

a. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Sécurité**.

b. Cliquez sur **Client LDAP** dans la section Utilisateurs et groupes pour afficher la boîte de dialogue Paramètres du client LDAP.



c. Renseignez la boîte de dialogue selon les critères suivants.

1. Sélectionnez l'une de ces méthodes d'authentification d'utilisateur :

   - **Autoriser les connexions des utilisateurs locaux**. L'authentification est exécutée à l'aide de l'authentification locale. Lorsque cette option est sélectionnée, tous les comptes utilisateur existent sur le serveur d'authentification local sur le nœud de gestion.
   - **Autoriser les connexions des utilisateurs LDAP**. L'authentification est exécutée par un serveur LDAP externe. Cette méthode permet de gérer des comptes utilisateur à

distance. Lorsque cette option est sélectionnée, tous les comptes utilisateur existent à distance dans un serveur LDAP externe.

- **Autoriser les connexions des utilisateurs locaux en premier, puis des utilisateurs LDAP**. Le serveur d'authentification local exécute l'authentification en premier. Si cette opération échoue, un serveur LDAP externe exécute l'authentification.
- **Autoriser les connexions des utilisateurs LDAP en premier, puis des utilisateurs locaux**. Un serveur LDAP externe exécute l'authentification en premier. Si cette opération échoue, le serveur d'authentification local exécute l'authentification.

2. Choisissez d'activer ou de désactiver le LDAP sécurisé :
   - **Activer le LDAP sécurisé**. XClarity Administrator utilise le protocole LDAPS pour établir une connexion sécurisée au serveur d'authentification externe. Lorsque cette option est sélectionnée, vous devez également configurer des certificats sécurisés pour activer le support LDAP sécurisé.
   - **Désactiver le LDAP sécurisé**. XClarity Administrator utilise un protocole non sécurisé pour établir une connexion au serveur d'authentification externe. Si vous choisissez ce paramètre, votre matériel peut être plus vulnérable aux attaques de sécurité.
3. Sélectionnez l'une de ces méthodes de sélection de serveur :
   - **Utiliser des serveurs préconfigurés**. XClarity Administrator utilise les adresses IP et ports spécifiés pour reconnaître le serveur d'authentification externe.

     Si vous sélectionnez cette option, indiquez jusqu'à quatre adresses IP de serveur et ports préconfigurés. Le client LDAP essaie de s'authentifier à l'aide de la première adresse du serveur. Si l'authentification échoue, le client LDAP tente de s'authentifier à l'aide de l'adresse IP de serveur suivante.

     Si le numéro de port pour une entrée *n'est pas* explicitement défini sur `3268` ou `3269`, il est considéré que l'entrée identifie un contrôleur de domaine.

     Lorsque le numéro de port est défini sur `3268` ou `3269`, il est considéré que l'entrée identifie un catalogue global. Le client LDAP tente de s'authentifier à l'aide du contrôleur de domaine pour la première adresse IP de serveur configurée. Si cette opération échoue, le client LDAP tente de s'authentifier à l'aide du contrôleur de domaine pour l'adresse IP de serveur suivante.

     Important : Au moins un contrôleur de domaine doit être spécifié, même si le catalogue global est spécifié. Spécifier le catalogue global uniquement peut sembler correct, mais ce n'est pas une configuration valide.

     Lorsque le mode de cryptographie est défini sur NIST-800-131A, XClarity Administrator ne peut peut-être pas se connecter à un serveur LDAP externe à l'aide d'un port sécurisé (par exemple, en utilisant LDAPS sur le port par défaut 636) si le serveur LDAP n'est pas en mesure d'établir une connexion Transport Layer Security (TLS) version 1.2 avec le client LDAP dans XClarity Administrator.
   - **Utiliser DNS pour rechercher des serveurs LDAP**. XClarity Administrator utilise le nom de domaine spécifié ou le nom de la forêt pour reconnaître le serveur d'authentification externe de manière dynamique. Le nom de domaine et le nom de la forêt sont utilisés pour obtenir une liste des contrôleurs de domaine, et le nom de la forêt est utilisé pour obtenir une liste des serveurs de catalogue global.

     Attention : Lors de l'utilisation de DNS pour rechercher les serveurs LDAP, vérifiez que le compte utilisateur à utiliser pour s'authentifier auprès du serveur d'authentification externe est hébergé sur des contrôleurs de domaine spécifiés. Si le compte utilisateur est hébergé sur un contrôleur de domaine enfant, ajoutez le contrôleur de domaine enfant dans la liste de demande de service.

4. Sélectionnez l'une des méthodes de liaison suivantes :

   - **Données d'identification configurées**. Utilisez cette méthode de liaison pour utiliser le nom et le mot de passe du client afin de lier XClarity Administrator au serveur d'authentification externe. Si la liaison échoue, la procédure d'authentification échoue également.

     Le nom du client peut être un nom pris en charge par le serveur LDAP, y compris un nom distinctif, un nom AMAccountName, un nom NetBIOS ou un nom UserPrincipalName. Le nom du client doit être un compte utilisateur au sein du domaine qui possède au minimum des droits en lecture seule. Par exemple :
     ```
     cn=username,cn=users,dc=example,dc=com
     domain\username
     username@domain.com
     username
     ```

     Attention : Si vous modifiez le mot de passe client sur le serveur d'authentification externe, veillez à mettre également à jour le nouveau mot de passe dans XClarity Administrator. Pour plus d'informations, voir Impossible de se connecter à XClarity Administrator dans la documentation en ligne de XClarity Administrator.

   - **Données d'identification de connexion**. Utilisez cette méthode de liaison pour utiliser le nom et le mot de passe d'un utilisateur Active Directory ou OpenLDAP pour lier XClarity Administrator au serveur d'authentification externe.

     L'ID utilisateur et le mot de passe que vous définissez sont uniquement utilisés pour tester la connexion au serveur d'authentification. Si l'opération réussit, les paramètres du client LDAP sont enregistrés, mais les données d'identification de connexion de test que vous avez spécifiées ne sont pas enregistrées. Toutes les futures liaisons utilisent le nom d'utilisateur et le mot de passe que vous avez utilisés pour vous connecter à XClarity Administrator.

     Remarques :

     – Vous devez être connecté à XClarity Administrator avec un ID utilisateur qualifié complet (par exemple, `administrator@domain.com`) ou `DOMAIN\admin`.

     – Vous devez utiliser un nom de client de test qualifié complet pour la méthode de liaison.

     Attention : Pour configurer la méthode de liaison afin d'utiliser des données d'identification de connexion, le contrôleur de gestion de chaque serveur géré doit exécuter un microprogramme de septembre 2016 ou ultérieur.

5. Dans la zone **Nom distinctif racine**, il est recommandé de ne pas indiquer de nom distinctif racine, en particulier pour les environnements possédant plusieurs domaines. Lorsque cette zone est vide, XClarity Administrator interroge le serveur d'authentification externe pour les contextes de désignation. Si vous utilisez DNS pour reconnaître le serveur d'authentification externe ou si vous indiquez plusieurs serveurs (par exemple, `dc=example,dc=com`), vous pouvez éventuellement indiquer la première entrée dans votre arborescence de répertoires LDAP. Dans ce cas, les recherches sont lancées avec le nom distinctif racine spécifié en tant que base de recherche.
6. Indiquez l'attribut à utiliser pour rechercher le nom d'utilisateur.

   Lorsque la méthode de liaison est définie sur **Données d'identification configurées**, la liaison initiale au serveur LDAP est suivie d'une demande de recherche qui récupère des informations spécifiques sur l'utilisateur, dont le nom distinctif, les autorisations de connexion et l'appartenance à un groupe. Cette demande de recherche doit spécifier le nom d'attribut représentant les ID d'utilisateur sur ce serveur. Ce nom d'attribut est configuré dans cette zone. Si cette zone est laissée vide, la valeur par défaut est **cn**.

7. Indiquez le nom d'attribut utilisé pour identifier les groupes auxquels un utilisateur appartient. Si cette zone est laissée vide, le nom d'attribut du filtre correspond par défaut à **memberOf**.
8. Indiquez le nom d'attribut utilisé pour identifier le nom de groupe qui est configuré par le serveur LDAP. Si cette zone est laissée vide, la valeur par défaut est **uid**.

d. Cliquez sur **Appliquer**.

XClarity Administrator tente de tester la configuration pour détecter les erreurs communes. Si le test échoue, il affiche des messages d'erreur qui indiquent la source des erreurs. Si le test aboutit et que les connexions aux serveurs spécifiés aboutissent, l'authentification utilisateur peut tout de même échouer si :

- Il n'existe aucun utilisateur local possédant des droits **lxc-recovery**.
- Le nom distinctif racine est incorrect.
- L'utilisateur n'est pas membre d'au moins un groupe dans le serveur d'authentification externe qui correspond au nom d'un groupe de rôles sur le serveur d'authentification de XClarity Administrator. XClarity Administrator ne peut pas le détecter si le nom distinctif racine est correct ; toutefois, il peut le détecter si un utilisateur est membre d'au moins un groupe. Si un utilisateur n'est pas membre d'au moins un groupe, un message d'erreur s'affiche lorsque l'utilisateur tente de se connecter à XClarity Administrator. Pour plus d'informations sur le dépannage des problèmes liés aux serveurs d'authentification externes, voir Problèmes de connectivité dans la documentation en ligne de XClarity Administrator.

Etape 4. Créez un compte utilisateur externe pouvant accéder à XClarity Administrator :

a. Depuis le serveur d'authentification externe, créez un compte utilisateur. Pour plus de détails, consultez la documentation. Active Directory ou OpenLDAP.

b. Créez un groupe global Active Directory ou OpenLDAP avec le nom d'un groupe prédéfini et autorisé. Le groupe doit exister dans le contexte du nom distinctif racine défini dans le client LDAP.

c. Ajoutez l'utilisateur Active Directory ou OpenLDAP comme membre du groupe de sécurité que vous avez créé précédemment.

d. Connectez-vous à XClarity Administrator avec le nom d'utilisateur Active Directory ou OpenLDAP.

e. **Facultatif :** définissez et créez des groupes supplémentaires. Vous pouvez ensuite les autoriser et leur affecter des rôles depuis la page Utilisateurs et groupes.

f. Si le LDAP sécurisé est activé, importez des certificats sécurisés vers le serveur LDAP externe (voir Installation d'un certificat de serveur personnalisé à signature externe).

Résultats

XClarity Administrator valide la connexion au serveur LDAP. Si la validation réussit, l'authentification utilisateur se produit sur le serveur d'authentification externe lorsque vous vous connectez à XClarity Administrator, à CMM et au contrôleur de gestion.

Si la validation échoue, le mode d'authentification est automatiquement modifié pour revenir au paramètre **Autoriser les connexions des utilisateurs locaux**, et un message décrivant la cause de l'échec s'affiche.

Remarque : Les groupes de rôles appropriés doivent être configurés dans XClarity Administrator et les comptes utilisateur doivent être définis en tant que membre de l'un de ces groupes de rôles sur le serveur Active Directory. Dans le cas contraire, l'authentification utilisateur échoue.

Configuration d'un SAML externe fournisseur d'identité

Vous pouvez choisir d'utiliser un langage Security Assertion Markup Language (SAML) 2.0 fournisseur d'identité pour effectuer l'authentification et l'autorisation de Lenovo XClarity Administrator.

Avant de commencer

La configuration initiale de XClarity Administrator doit être effectuée avant la configuration du fournisseur d'identité.

Le fournisseur d'identité doit être Microsoft Active Directory Federated Service (AD FS) et il peut être connecté au réseau de gestion et/ou au réseau de données. Comme l'authentification est effectuée via votre navigateur web, ce dernier doit pouvoir être en mesure d'accéder à XClarity Administrator et au serveur SAML.

Vous pouvez télécharger les métadonnées IDP à l'aide de l'URL suivante : `https://<ADFS_IP_Address>/federationmetadata/2007-06/federationmetadata.xml`, où *<ADFS_IP_Address>* est l'adresse IP de AD FS (par exemple, https://10.192.0.0/federationmetadata/2007-06/federationmetadata.xml).

Vous devez créer ou renommer des groupes de rôles sur le serveur d'authentification de l'emplacement pour qu'ils correspondent aux groupes définis sur le serveur d'authentification externe.

Pour configurer un fournisseur d'identité SAML, vous devez être connecté en tant qu'utilisateur membre du groupe **lxc_admin** ou **lxc_supervisor**.

À propos de cette tâche

XClarity Administrator prend en charge l'utilisation d'un langage Security Assertion Markup Language 2.0 fournisseur d'identité pour l'authentification et l'autorisation des utilisateurs. Outre la saisie d'un nom d'utilisateur et d'un mot de passe, le fournisseur d'identité peut être configuré pour exiger des critères supplémentaires pour la validation de l'identité d'un utilisateur, comme la saisie d'un code PIN, la lecture d'une carte à puce et l'authentification à l'aide d'un certificat client.

Lorsque XClarity Administrator est configuré pour l'utilisation d'un fournisseur d'identité, les demandes de connexion interactives depuis l'interface Web de XClarity Administrator sont redirigées vers le fournisseur d'identité pour l'authentification. Une fois que l'utilisateur est authentifié, le navigateur Web est redirigé vers XClarity Administrator.

Remarque : Si le fournisseur d'identité est activé, vous pouvez omettre le fournisseur d'identité et vous connecter à XClarity Administrator à l'aide du serveur serveur d'authentification LDAP local ou externe en ouvrant votre navigateur Web sur la page de connexion de XClarity Administrator (par exemple, `https://<ip_address>/ui/login.htm`).

Lorsque XClarity Administrator est configuré pour l'utilisation d'un profil fournisseur d'identité, la page Gestion des utilisateurs dans l'interface Web de XClarity Administrator n'est pas désactivée. Les comptes utilisateur locaux sont requis pour se connecter directement à un châssis ou à un serveur géré (sauf lorsque l'Encapsulation est activé sur cet appareil), ainsi que pour l'authentification PowerShell et API REST.

Procédure

Pour configurer un fournisseur d'identité SAML externe, (AD FS), procédez comme suit.

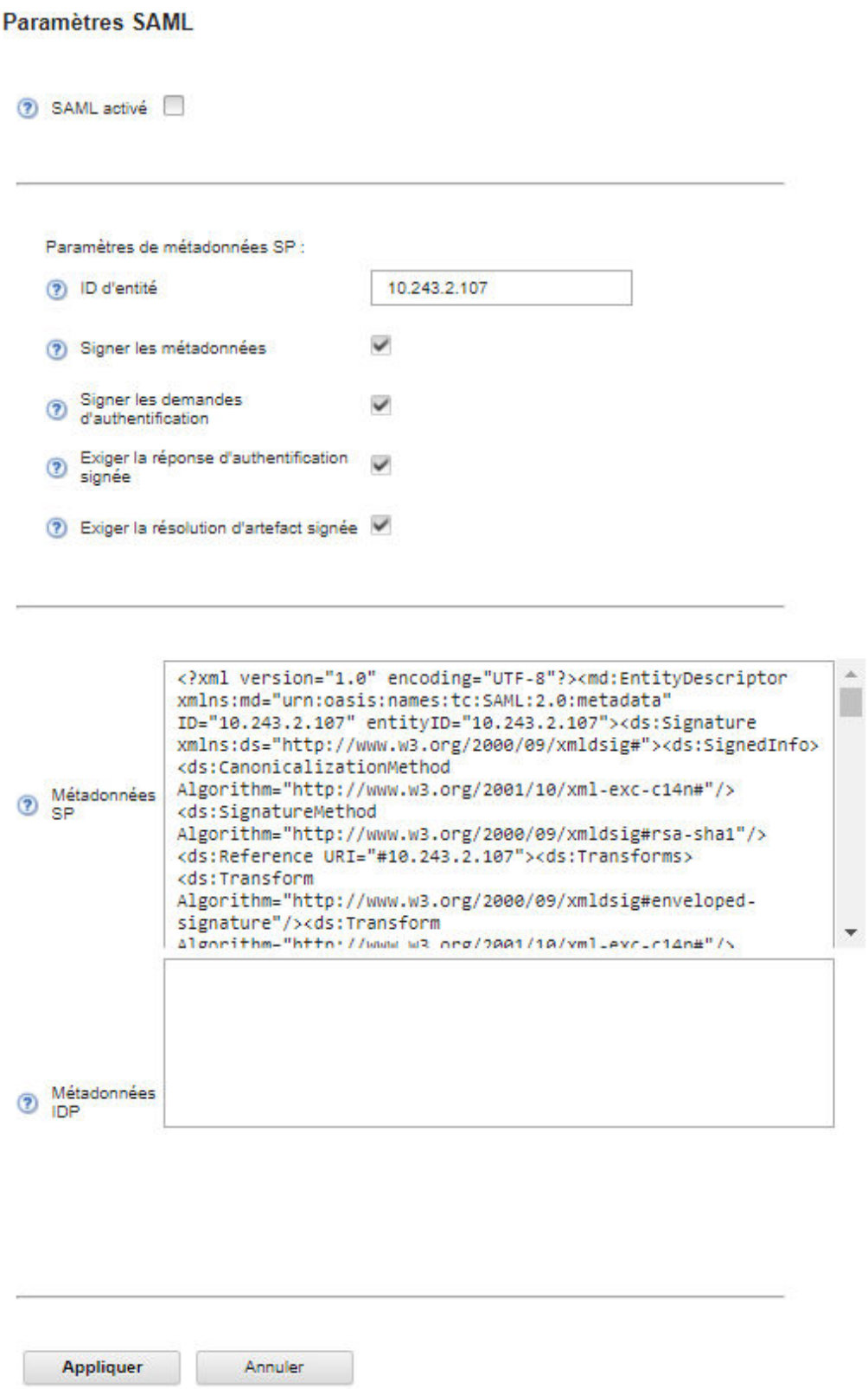
Etape 1. Créez un compte utilisateur de récupération qui peut être utilisé pour se connecter à XClarity Administrator si le fournisseur d'identité devient indisponible (voir Gestion des comptes utilisateur).

Etape 2. Procédez à l'extraction des métadonnées fournisseur d'identité (IDP) fournisseur d'identité, puis enregistrez le fichier sur l'hôte XClarity Administrator.

Etape 3. Configurez le client SAML XClarity Administrator.

a. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Sécurité**.

b. Cliquez sur **Paramètres SAML** sous la section Utilisateurs et groupes pour afficher la boîte de dialogue Paramètres SAML.



c. Complétez les zones de la page Paramètres SAML :

   1. Vérifiez que l'ID d'entité correspond à l'adresse IP du serveur de gestion XClarity Administrator.
   2. Indiquez si les métadonnées générées doivent être signées de façon numérique.

3. Indiquez si les demandes d'authentification doivent être signées.
4. Indiquez si les réponses d'authentification doivent être signées.
5. Indiquez si les demandes de résolution d'artefact envoyées au fournisseur d'identité distant doivent être signées.
6. Collez les métadonnées fournisseur d'identité (IDP) SAML générées par le fournisseur d'identité et extraites à l'étape Etape 2 3 à la page 26 dans la zone **Métadonnées IDP**.

d. Cliquez sur **Appliquer** pour appliquer les modifications et mettre à jour le texte dans la zone Métadonnées SP.

Attention : *Ne* sélectionnez pas **SAML activé** à ce stade. Vous activerez SAML ultérieurement pour redémarrer XClarity Administrator.

e. Copiez et collez les données de la zone **Métadonnées SP** dans un fichier, puis enregistrez le fichier avec l'extension .XML (par exemple, sp_metadata.xml). Copiez ce fichier sur l'hôte AD FS.

Etape 4. Configurez AD FS.

a. Ouvrez l'outil de gestion AD FS.
b. Cliquez sur **ADFS → Sécurisations de partie utilisatrice**.
c. Cliquez avec le bouton droit de la souris sur **Sécurisations de partie utilisatrice**, puis cliquez sur **Ajouter la sécurisation de partie utilisatrice** pour afficher l'assistant
d. Cliquez sur **Démarrer**
e. Sur la page Sélectionner une source de données, sélectionnez **Importer des données concernant la partie utilisatrice depuis un fichier**, puis sélectionnez le fichier de métadonnées SP que vous avez enregistré à l'étape 3e.
f. Entrez un nom d'affichage.
g. Cliquez sur **Suivant** sur toutes les pages pour choisir les valeurs par défaut.
h. Cliquez sur **Terminer** pour afficher la page Règles de réclamation
i. Conservez la valeur par défaut pour **Envoyer des attributs LDAP comme réclamations** et cliquez sur **Suivant**.
j. Entrez un nom de règle de réclamation.
k. Sélectionnez **Active Directory** comme magasin d'attributs.
l. Ajoutez un mappage. Dans la partie gauche, sélectionnez **SAM-Account-Name**, et sur la droite, sélectionnez **ID nom** comme type de réclamation sortant.
m. Ajoutez un autre mappage. Dans la partie gauche, sélectionnez **Token-Groups-Unqualified Names**, et sur la droite, sélectionnez **Groupe** comme type de réclamation sortant.
n. Cliquez sur **OK**.
o. Recherchez la sécurisation que vous venez de créer dans la liste de **Sécurisations de partie utilisatrice**.
p. Cliquez avec le bouton droit de la souris sur la sécurisation, puis cliquez sur **Sélectionner les propriétés**. La boîte de dialogue des propriétés de sécurisation s'affiche.
q. Cliquez sur l'onglet **Avancé**, puis sélectionnez `SHA-1` comme algorithme de hachage sécurisé.

Etape 5. Enregistrez le certificat du serveur à partir d'AD FS.

a. Cliquez sur **Console AD FS → Service → Certificats**.
b. Sélectionnez le **Certificat** sous la signature de jeton.
c. Cliquez avec le bouton droit de la souris sur le certificat, puis cliquez sur **Afficher le certificat**.
d. Cliquez sur l'onglet **Détails**.

e. Cliquez sur **Copier dans le fichier**, puis enregistrez le certificat en tant que fichier X.509 binaire codé par DER (.CER).

f. Copiez le fichier .CER du certificat du serveur sur l'hôte XClarity Administrator.

Etape 6. Importez le certificat sécurisé de AD FS dans l'interface Web de XClarity Administrator.

a. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Sécurité**.

b. Cliquez sur **Certificats sécurisés** dans la section Gestion des certificats.

c. Cliquez sur l'icône **Créer** ( ) pour ajouter un certificat.

d. Sélectionnez le fichier .CER du certificat du serveur que vous avez enregistré à l'étape précédente.

e. Cliquez sur **Créer**.

Etape 7. Cliquez sur **Paramètres SAML** sous la section Utilisateurs et groupes pour afficher la boîte de dialogue Paramètres SAML.

Etape 8. Sélectionnez **SAML activé** pour activer la gestion des comptes utilisateur à l'aide d'un fournisseur d'identité externe. Lorsque cette option est sélectionnée, tous les comptes utilisateur existent à distance dans un fournisseur d'identité.

Etape 9. Cliquez sur **Appliquer** pour appliquer les modifications et redémarrer le serveur de gestion.

Etape 10. Patientez quelques minutes le temps que XClarity Administrator redémarre.

Attention : Ne redémarrez pas le dispositif virtuel manuellement pendant ce processus.

Etape 11. Fermez puis rouvrez le navigateur Web.

Etape 12. Connectez-vous à l'interface Web de XClarity Administrator depuis le fournisseur d'identité.

Résultats

XClarity Administrator tente de tester la configuration pour détecter les erreurs communes. Si le test échoue, il affiche des messages d'erreur qui indiquent la source des erreurs.

XClarity Administrator valide la connexion à fournisseur d'identité. Si la validation aboutit, l'authentification utilisateur a lieu sur le fournisseur d'identité lorsque vous vous connectez à XClarity Administrator.

Configuration d’un système de gestion d’identité externe

Un *système de gestion d’identité* se définit comme un coffre-fort externe pour mots de passe qui peut, de manière facultative, être utilisé avec Lenovo XClarity Administrator pour stocker les données d’identification de XClarity Administrator et XClarity Controller. Si un système de gestion d’identité est associé à XClarity Administrator, alors XClarity Administrator récupère les mots de passe depuis le système de gestion d’identité, et non les serveurs d’authentification.

À propos de cette tâche

XClarity Administrator prend en charge le système de gestion d’identité suivant.

- CyberArk

Configuration d’un système de gestion d’identité CyberArk

CyberArk est un coffre-fort externe pour mots de passe, qui peut, de manière facultative, être utilisé avec Lenovo XClarity Administrator pour stocker les données d’identification de XClarity Administrator et Lenovo XClarity Controller. Dès que le mot de passe d’un compte est stocké dans CyberArk, celui-ci est géré par CyberArk.

À propos de cette tâche

XClarity Administrator vous permet de stocker vos mots de passe XCC dans des systèmes de gestion d'identité fournis par CyberArk, un tiers. Lenovo n'est pas responsable des services proposés par CyberArk ; vous êtes responsable de votre relation directe avec CyberArk.

Si des comptes utilisateur destinés à un serveur ThinkSystem ou ThinkAgile sont intégrés à CyberArk, lors de la configuration initiale des serveurs pour la gestion (avec authentification gérée ou locale), XClarity Administrator peut recueillir les données d'identification auprès de CyberArk pour se connecter au serveur. Avant de pouvoir recueillir les données d'identification de CyberArk, les chemins d'accès à CyberArk doivent être définis dans XClarity Administrator. Une confiance mutuelle doit être établie entre CyberArk et XClarity Administrator à l'aide d'une authentification mutuelle TLS via des certificats clients.

Procédure

Pour configurer XClarity Administrator en vue d'utiliser CyberArk, procédez comme suit.

Etape 1. Configurez CyberArk.

1. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Sécurité**.
2. Cliquez sur **CyberArk** dans la section Gestion de l'identité.
3. Cliquez sur **Modifier les détails du serveur CyberArk** dans la barre d'outils.
4. Indiquez le nom d'hôte ou l'adresse IP CyberArk, ainsi que le numéro de port.
5. Cliquez sur **Appliquer**.

Etape 2. Importez le certification d'authentification mutuelle de XClarity Administrator dans CyberArk.

1. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Sécurité**.
2. Cliquez sur **Certificat du serveur** dans la section Gestion des certificats.
3. Cliquez sur l'onglet **Certificat client**.
4. Sélectionnez le type de serveur **CyberArk**.
5. Cliquez sur **Régénérer le certificat** afin de générer un nouveau certificat d'authentification mutuelle TLS pour CyberArk.

   Attention : Si vous régénérez le certificat d'authentification mutuelle TLS pour CyberArk suite à l'établissement d'une connexion entre XClarity Administrator et CyberArk, alors la connexion est perdue jusqu'à l'importation d'un nouveau certificat dans CyberArk.
6. Cliquez sur **Télécharger le certificat**, puis cliquez sur **Enregistrer sous der** ou **Enregistrer sous pem** pour enregistrer le certificat en tant que fichier sur votre système local.
7. Importez le certificat téléchargé dans CyberArk.

Etape 3. Importez le certificat de l'autorité de certification racine CyberArk dans XClarity Administrator

1. Téléchargez le certificat de l'autorité de certification racine depuis CyberArk.
2. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Sécurité**.
3. Cliquez sur **Certificats sécurisés** dans la section Gestion des certificats.
4. Cliquez sur l'icône **Créer** ( ) pour ajouter un certificat.
5. Recherchez le fichier ou collez le texte du certificat au format PEM.
6. Cliquez sur **Créer**.

Etape 4. Ajoutez des chemins d'accès permettant d'identifier l'emplacement des comptes utilisateurs intégrés dans CyberArk.

1. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Sécurité**.
2. Cliquez sur **CyberArk** dans la section Gestion de l'identité.
3. Cliquez sur l'onglet **Chemins d'accès**.

4. Cliquez sur l'icône **Créer** ( ) pour afficher la boîte de dialogue Create un chemin d'accès CyberArk.

5. Le cas échéant précisez l'ID de l'application, le coffre-fort et le dossier dans lesquels les comptes utilisateur sont stockés dans CyberArk.

   Si vous spécifiez l'ID de l'application, le coffre-fort et éventuellement le dossier, XClarity Administrator tente de trouver le compte utilisateur dans l'emplacement spécifié.

   Si vous spécifiez une combinaison de zones autres que l'ID d'application et le coffre-fort (par exemple, si vous spécifiez uniquement l'ID d'application, seuls le dossier et le coffre-fort, ou uniquement l'ID d'application et le dossier), XClarity Administrator filtre le chemin à l'aide de ces valeurs.
6. Cliquez sur **Appliquer**.

Après avoir terminé

- Modifiez un chemin d'accès CyberArk sélectionné en cliquant sur l'icône **Modifier** ( ).
- Supprimer un chemin d'accès CyberArk sélectionné en cliquant sur l'icône **Supprimer** ( ).

Détermination du type de méthode d'authentification qui est utilisé par Lenovo XClarity Administrator

Vous pouvez déterminer le type de méthode d'authentification en cours d'utilisation dans les onglets **Client LDAP** et **Paramètres SAML** sur la page Sécurité.

À propos de cette tâche

Le *serveur d'authentification* est un registre utilisateur utilisé pour authentifier les données d'identification de l'utilisateur. Lenovo XClarity Administrator prend en charge les types de serveurs d'authentification suivants.

- **Serveur d'authentification local**. Par défaut, XClarity Administrator est configuré pour utiliser le serveur LDAP (Lightweight Directory Access Protocol) intégré qui réside sur le serveur de gestion.
- **Serveur LDAP externe**. Actuellement, seulement Microsoft Active Directory et OpenLDAP sont pris en charge. Ce serveur doit se trouver sur un serveur Microsoft Windows externe connecté au réseau de gestion. Lorsqu'un serveur LDAP externe est utilisé, le serveur d'authentification local est désactivé.

  Attention : Pour configurer la méthode de liaison d'Active Directory afin qu'elle utilise des données d'identification de connexion, le contrôleur de gestion de la carte mère de chaque serveur géré doit exécuter un microprogramme de septembre 2016 ou ultérieur.
- **Système de gestion d'identité externe**. Actuellement, seul CyberArk est pris en charge.

Si des comptes utilisateur destinés à un serveur ThinkSystem ou ThinkAgile sont intégrés à CyberArk, lors de la configuration initiale des serveurs pour la gestion (avec authentification gérée ou locale), XClarity Administrator peut recueillir les données d'identification auprès de CyberArk pour se connecter au serveur. Avant de pouvoir recueillir les données d'identification de CyberArk, les chemins d'accès à CyberArk doivent être définis dans XClarity Administrator. Une confiance mutuelle doit être établie entre CyberArk et XClarity Administrator à l'aide d'une authentification mutuelle TLS via des certificats clients.

- **fournisseur d'identité SAML externe**. Actuellement, seul Microsoft Active Directory Federation Services (AD FS) est pris en charge. Outre la saisie d'un nom d'utilisateur et d'un mot de passe, l'authentification multifacteur peut être configurée pour offrir une sécurité accrue en exigeant un code PIN, la lecture d'une carte à puce et un certificat client. Lorsqu'un fournisseur d'identité SAML externe est utilisé, le serveur d'authentification local n'est pas désactivé. Les comptes utilisateur locaux sont requis pour se connecter directement à un châssis ou à un serveur géré (sauf si l'Encapsulation est activé sur cet appareil), pour l'authentification d'API REST et PowerShell, ainsi que pour la récupération si l'authentification externe n'est pas disponible.

  Vous pouvez choisir d'utiliser à la fois un serveur LDAP externe et un fournisseur d'identité externe. Si les deux sont activés, le serveur LDAP externe est utilisé pour se connecter directement aux appareils gérés, et le fournisseur d'identité est utilisé pour se connecter au serveur de gestion.

Procédure

Pour déterminer le type de serveur d'authentification utilisé par le logiciel de gestion, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Sécurité**.

Etape 2. Cliquez sur **Client LDAP** dans la section Utilisateurs et groupes pour afficher la boîte de dialogue Paramètres du client LDAP.

Vérifiez quelle méthode d'authentification de l'utilisateur est sélectionnée :

- **Autoriser les connexions des utilisateurs locaux**. L'authentification est exécutée à l'aide de l'authentification locale. Lorsque cette option est sélectionnée, tous les comptes utilisateur existent sur le serveur d'authentification local sur le nœud de gestion.
- **Autoriser les connexions des utilisateurs LDAP**. L'authentification est exécutée par un serveur LDAP externe. Cette méthode permet de gérer des comptes utilisateur à distance. Lorsque cette option est sélectionnée, tous les comptes utilisateur existent à distance dans un serveur LDAP externe.
- **Autoriser les connexions des utilisateurs locaux en premier, puis des utilisateurs LDAP**. Le serveur d'authentification local exécute l'authentification en premier. Si cette opération échoue, un serveur LDAP externe exécute l'authentification.
- **Autoriser les connexions des utilisateurs LDAP en premier, puis des utilisateurs locaux**. Un serveur LDAP externe exécute l'authentification en premier. Si cette opération échoue, le serveur d'authentification local exécute l'authentification.

Etape 3. Cliquez sur **Paramètres SAML** sous la section Utilisateurs et groupes pour afficher la page Paramètres SAML.

Si vous sélectionnez **SAML activé**, un fournisseur d'identité est utilisé.

Accès à Lenovo XClarity Administrator après une défaillance de serveur LDAP externe

Si vous utilisez le serveur d'authentification LDAP externe et que le serveur échoue ou n'est pas disponible, utilisez la procédure suivante pour récupérer l'accès à l'interface Web de Lenovo XClarity Administrator à l'aide du serveur d'authentification local du nœud de gestion.

Procédure

Pour modifier les paramètres du client LDAP, procédez comme suit.

Etape 1. Connectez-vous à l'interface Web XClarity Administrator avec un compte utilisateur disposant des droits **lxc-recovery**. Pour plus d'informations sur le nom de domaine client, voir Configuration d'un serveur d'authentification LDAP externe.

Etape 2. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Sécurité**.

Etape 3. Cliquez sur **Client LDAP** dans la section Utilisateurs et groupes pour afficher la boîte de dialogue Client LDAP.

Etape 4. Sélectionnez **Autoriser les connexions des utilisateurs locaux** pour la méthode d'authentification utilisateur afin d'activer la gestion locale des comptes utilisateur. Lorsque cette option est sélectionnée, tous les comptes utilisateur existent localement sur le serveur de gestion.

Etape 5. Cliquez sur **Appliquer**.

Résultats

Vous pouvez désormais utiliser les comptes utilisateur dans le serveur d'authentification local pour accéder au serveur de gestion XClarity Administrator. Une fois votre serveur d'authentification externe restauré et disponible sur le serveur de gestion, vous pouvez modifier les paramètres du client LDAP sur le serveur d'authentification externe.

Accès à Lenovo XClarity Administrator après une défaillance fournisseur d'identité SAML externe

Si vous utilisez le fournisseur d'identité d'un SAML externe et que le serveur échoue ou n'est pas disponible, utilisez la procédure suivante pour récupérer l'accès à l'interface Web de Lenovo XClarity Administrator à l'aide du serveur d'authentification local de XClarity Administrator.

Procédure

Pour modifier le paramètre client SAML, procédez comme suit.

Etape 1. Affichez votre navigateur Web sur la page de connexion de XClarity Administrator (par exemple, `https://<ip_address>/ui/login.html`).

Etape 2. Connectez-vous à l'interface Web de XClarity Administrator à l'aide d'un compte utilisateur de récupération local que vous avez créé lors de la configuration de fournisseur d'identité.

Etape 3. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Sécurité**.

Etape 4. Cliquez sur **Paramètres SAML** sous la section Utilisateurs et groupes pour afficher la boîte de dialogue Paramètres SAML.

Etape 5. Désélectionnez **Activer SAML** afin de désactiver le fournisseur d'identité SAML. Lorsque cette option est désélectionnée, le serveur d'authentification local ou le serveur LDAP externe (si configuré) est utilisé pour l'authentification.

Etape 6. Cliquez sur **Appliquer**.

Résultats

Vous pouvez désormais utiliser les comptes utilisateur dans le serveur d'authentification local pour accéder au serveur de gestion XClarity Administrator. Une fois votre fournisseur d'identité externe restauré et disponible pour le serveur de gestion, vous pouvez définir la méthode d'authentification sur fournisseur d'identité.

Gestion des comptes utilisateur

Les comptes utilisateurs permettent de se connecter à et de gérer Lenovo XClarity Administrator, ainsi que tous les châssis et serveurs gérés par XClarity Administrator. Les comptes utilisateurs XClarity Administrator sont soumis à deux processus interdépendants : l'authentification et l'autorisation.

À propos de cette tâche

L'*authentification* est le mécanisme de sécurité par lequel les données d'identification d'un utilisateur sont vérifiées. Le processus d'authentification utilise les données d'identification de l'utilisateur qui sont stockées sur le serveur d'authentification configuré. Il empêche également les serveurs de gestion non autorisés ou les applications parasites des systèmes gérés d'accéder aux ressources. Après l'authentification, un utilisateur peut accéder à XClarity Administrator. Toutefois, pour accéder à une ressource spécifique ou exécuter une tâche précise, l'utilisateur doit également disposer de l'autorisation appropriée.

L'*autorisation* vérifie les droits de l'utilisateur authentifié et contrôle l'accès aux ressources en fonction de l'appartenance de l'utilisateur à un groupe de rôles. Les *groupes de rôles* sont utilisés pour affecter des rôles spécifiques à un ensemble de comptes utilisateur définis et gérés sur le serveur d'authentification. Par exemple, si un utilisateur est membre d'un groupe de rôles doté des droits de superviseur (Supervisor), il peut créer, modifier et supprimer des comptes utilisateur de XClarity Administrator. Si un utilisateur dispose de droits d'opérateur (Operator), il peut uniquement consulter les informations de compte utilisateur.

Remarque : Les comptes utilisateurs SYSMGR_* et SYSRDR_* (* étant un suffixe choisi de manière aléatoire et composé de caractères A-Z et 0-9) sont générés et utilisés par XClarity Administrator comme comptes utilisateur de maintenance. Ils sont utilisés pour des fonctions, comme par exemple, authentification gérée, déploiement de SE et mises à jour de microprogramme. Les mots de passe SYSMGR_* et SYSRDR_* sont modifiés à chaque fois que XClarity Administrator démarre et peu de temps avant la période d'avertissement d'expiration du mot de passe.

Création d'un utilisateur

Les comptes utilisateur permettent de gérer l'autorisation et l'accès aux ressources.

À propos de cette tâche

Le premier compte utilisateur que vous créez doit posséder le rôle Superviseur et doit être activé.

Pour plus de sécurité, créez au moins deux comptes utilisateur dotés du rôle **Superviseur**. Prenez soin d'enregistrer les mots de passe de ces comptes utilisateur et de les stocker dans un endroit sûr au cas où vous seriez amené à restaurer Lenovo XClarity Administrator.

Procédure

Pour ajouter un utilisateur à XClarity Administrator, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Sécurité**.

Etape 2. Cliquez sur **Utilisateurs locaux** sous la section Utilisateurs et groupes pour afficher la page Gestion des utilisateurs.

Etape 3. Cliquez sur l'icône **Créer** ( ) pour créer un utilisateur. La boîte de dialogue Créer un nouvel utilisateur s'affiche.

Etape 4. Entrez les informations ci-après dans la boîte de dialogue.

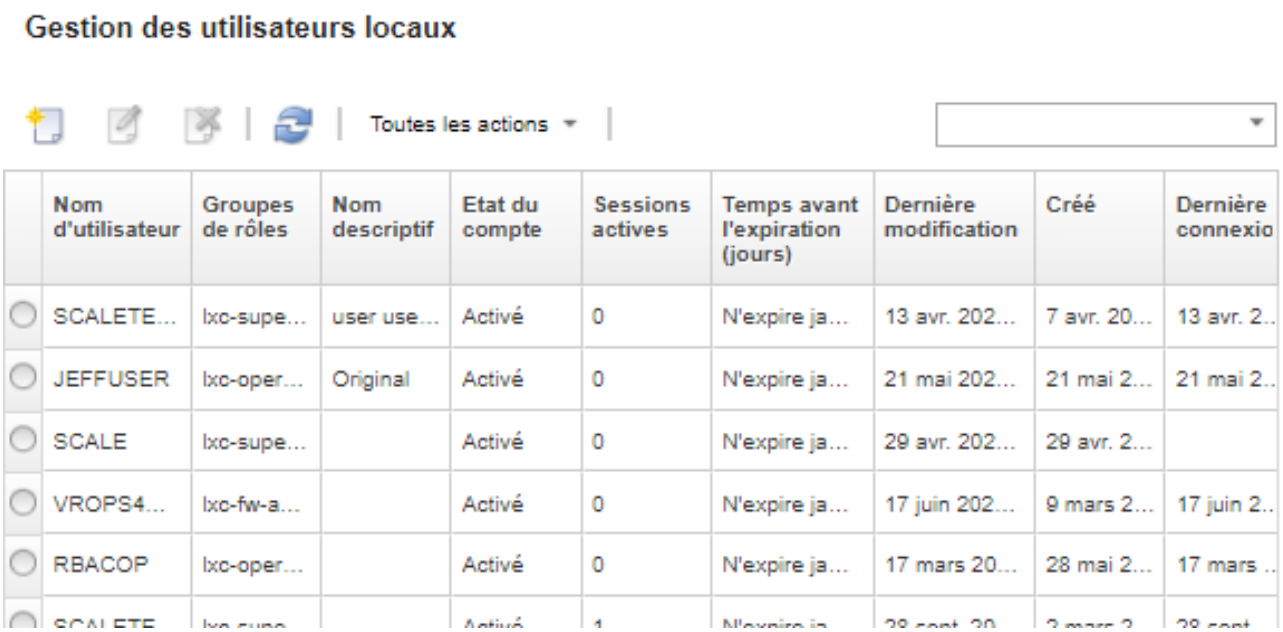
- Entrez un nom d'utilisateur et une description pour l'utilisateur.
- Entrez le nouveau mot de passe et confirmez-le. Les règles relatives aux mots de passe sont basées sur les paramètres de sécurité de compte en vigueur.

- Sélectionnez un ou plusieurs groupes de rôles pour autoriser l'utilisateur à effectuer des tâches appropriées.Pour plus d'informations sur les groupes de rôles et pour savoir comment créer des groupes de rôles personnalisés de rôle, voir Création d'un groupe du rôle personnalisé.
- (Facultatif) Affectez à l'option **Modifier le mot de passe lors du premier accès** la valeur `Yes` si vous souhaitez forcer l'utilisateur à modifier le mot de passe la première fois qu'il se connecte à XClarity Administrator.

Etape 5. Cliquez sur **Créer**.

Après avoir terminé

Le compte utilisateur s'affiche dans le tableau Gestion des utilisateurs. Le tableau présente les groupes de rôles associés et l'état de chaque compte utilisateur.



Après avoir créé un compte utilisateur, vous pouvez exécuter les actions suivantes sur un compte utilisateur sélectionné :

- Modifiez le nom d'utilisateur, la description et le rôle d'un compte utilisateur en cliquant sur l'icône **Éditer** ( ).
- Supprimez le compte utilisateur en cliquant sur l'icône **Supprimer** ( ).
- Réinitialisez le mot de passe du compte utilisateur (voir Réinitialisation du mot de passe d'un utilisateur).
- Déverrouillez le compte (voir Déverrouillage d'un utilisateur).
- Activez ou désactivez un compte utilisateur (voir Activation ou désactivation d'un utilisateur).

Activation ou désactivation d'un utilisateur

Vous pouvez activer ou désactiver un compte utilisateur local sur le serveur d'authentification.

Procédure

Pour activer ou désactiver un compte utilisateur, procédez comme suit.

- Si le serveur d'authentification local est utilisé :
  1. Dans la barre de titre de Lenovo XClarity Administrator, cliquez sur **Administration → Sécurité**.

2. Cliquez sur **Utilisateurs locaux** sous la section Utilisateurs et groupes pour afficher la page Gestion des utilisateurs.
3. Sélectionnez un compte utilisateur.
4. Si le compte utilisateur est activé, cliquez sur **Toutes les actions → Désactiver le compte sélectionné** pour désactiver l'utilisateur. L'état du compte affiché dans le tableau devient `Disabled`.
5. Si le compte utilisateur est désactivé, cliquez sur **Toutes les actions → Activer le compte sélectionné** pour activer l'utilisateur. L'état du compte affiché dans le tableau devient `Enabled`.

- Si un serveur LDAP externe est utilisé, activez ou désactivez un compte utilisateur dans Microsoft Active Directory.
- Si un fournisseur d'identité SAML externe est utilisé, activez ou désactivez un compte utilisateur dans le fournisseur d'identité.

Déconnexion d'un utilisateur actif

Vous pouvez déconnecter (mettre fin à la session) un utilisateur actif de Lenovo XClarity Administrator.

Vous devez être connecté à XClarity Administrator à l'aide d'un compte utilisateur disposant des droits **lxc-supervisor** ou **lxc-security-admin**.

Procédure

Pour déconnecter un utilisateur actif, procédez comme suit.

Etape 1. Dans la barre de titre de XClarity Administrator, cliquez sur **Administration → Sécurité**.

Etape 2. Cliquez sur **Sessions actives** sous la section Utilisateurs et groupes pour afficher la page Gestion des sessions actives.

Etape 3. Sélectionnez un ou plusieurs comptes utilisateur.

Etape 4. Cliquez sur **Déconnecter l'utilisateur**.

Modification du mot de passe de votre compte utilisateur

Vous pouvez modifier le mot de passe de votre compte utilisateur.

Procédure

Procédez comme suit pour modifier votre mot de passe.

- Si le serveur d'authentification local est utilisé :
  1. Dans la barre de titre de Lenovo XClarity Administrator, cliquez sur le menu d'actions utilisateur (ADMIN_USER), puis cliquez sur **Modifier le mot de passe**. La boîte de dialogue Modifier le mot de passe s'affiche.

2. Entrez le mot de passe en cours.
3. Entrez le nouveau mot de passe et confirmez-le. Les règles relatives aux mots de passe sont basées sur les paramètres de sécurité de compte en vigueur.
4. Cliquez sur **Modifier**.

- Si un serveur d'authentification externe est utilisé, modifiez votre mot de passe dans Microsoft Active Directory.

  Attention : Si vous avez mis à jour Microsoft Active Directory avec un nouveau mot de passe pour le compte client qui est utilisé afin d'établir une liaison entre XClarity Administrator et le serveur d'authentification externe, prenez soin de mettre à jour également le nouveau mot de passe dans l'interface Web de XClarity Administrator (voir Configuration d'un serveur d'authentification LDAP externe).
- Si un fournisseur d'identité SAML externe est utilisé, modifiez votre mot de passe dans le fournisseur d'identité.

Réinitialisation du mot de passe d'un utilisateur

Le mot de passe de n'importe quel compte utilisateur peut être réinitialisé.

Procédure

Pour réinitialiser un mot de passe, procédez comme suit.

- Si le serveur d'authentification local est utilisé, réinitialisez le mot de passe à partir de l'interface Web de Lenovo XClarity Administrator :
  1. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Sécurité**.
  2. Cliquez sur **Utilisateurs locaux** sous la section Utilisateurs et groupes pour afficher la page Gestion des utilisateurs.
  3. Sélectionnez un compte utilisateur dans le tableau.
  4. Si le compte utilisateur est activé, cliquez sur **Toutes les actions → Réinitialiser le mot de passe de l'utilisateur sélectionné**. La boîte de dialogue Réinitialiser le mot de passe s'affiche.

a. Entrez le nouveau mot de passe et confirmez-le. Les règles relatives aux mots de passe sont basées sur les paramètres de sécurité de compte en vigueur.
b. Affectez éventuellement à l'option **Modifier lors du premier accès** la valeur `Yes` si vous souhaitez forcer l'utilisateur à modifier le mot de passe la première fois qu'il se connecte à XClarity Administrator.
c. Cliquez sur **Réinitialiser**.

- Si un serveur LDAP externe est utilisé, réinitialisez le mot de passe dans Microsoft Active Directory.
- Si un fournisseur d'identité SAML externe est utilisé, réinitialisez le mot de passe dans le fournisseur d'identité.
- Si vous ne parvenez pas à vous connecter à XClarity Administrator en utilisant un autre compte du superviseur ou s'il n'existe pas d'autre compte du superviseur, vous pouvez réinitialiser le mot de passe d'un utilisateur local doté de droits de récupération ou de superviseur en montant une image ISO qui contient un fichier de configuration avec le nouveau mot de passe. Pour plus d'informations, voir Le mot de passe d'un utilisateur de récupération ou de superviseur local est oublié dans la documentation en ligne de XClarity Administrator.

Déverrouillage d'un utilisateur

Vous pouvez déverrouiller un compte utilisateur dont l'accès à Lenovo XClarity Administrator est bloqué. Un compte utilisateur peut être temporairement verrouillé si le nombre de tentatives de connexion non valides de la part de l'utilisateur est trop élevé.

À propos de cette tâche

Les paramètres de sécurité de compte utilisateur contrôlent la période qui doit s'écouler avant qu'un utilisateur dont l'accès à un compte est bloqué, puisse tenter de se reconnecter. Si le paramètre **Période de verrouillage après le nombre maximal d'échecs de connexion** a pour valeur `0`, le compte utilisateur reste verrouillé jusqu'à ce qu'il soit déverrouillé explicitement par l'administrateur. Pour plus d'informations sur la période de verrouillage pour le nombre maximal d'échecs de connexion, voir Modification des paramètres de sécurité d'un compte utilisateur.

Vous pouvez également désactiver ou activer un compte utilisateur de façon définitive. Pour plus d'informations, voir Activation ou désactivation d'un utilisateur.

Remarque : Vous devez disposer des droits Superviseur pour déverrouiller un compte utilisateur.

Astuce : Vous pouvez utiliser XClarity Administrator pour déverrouiller des comptes utilisateur gérés à l'aide du serveur d'authentification local. Vous ne pouvez pas déverrouiller des comptes utilisateur dans un serveur d'authentification externe à l'aide de XClarity Administrator.

Procédure

Pour déverrouiller un compte utilisateur, procédez comme suit.

- Si le serveur d'authentification local est utilisé :
  1. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Sécurité**.
  2. Cliquez sur **Utilisateurs locaux** sous la section Utilisateurs et groupes pour afficher la page Gestion des utilisateurs.
  3. Sélectionnez le compte utilisateur dans le tableau.
  4. Cliquez sur **Toutes les actions → Déverrouiller le compte de l'utilisateur sélectionné**.
- Si un serveur LDAP externe est utilisé, déverrouillez le compte utilisateur dans Microsoft Active Directory.

- Si un fournisseur d'identité SAML externe est utilisé, déverrouillez le compte utilisateur dans le fournisseur d'identité.

Surveillance des utilisateurs actifs

Vous pouvez déterminer qui est connecté à l'interface Web de Lenovo XClarity Administrator à partir de la page Tableau de bord.

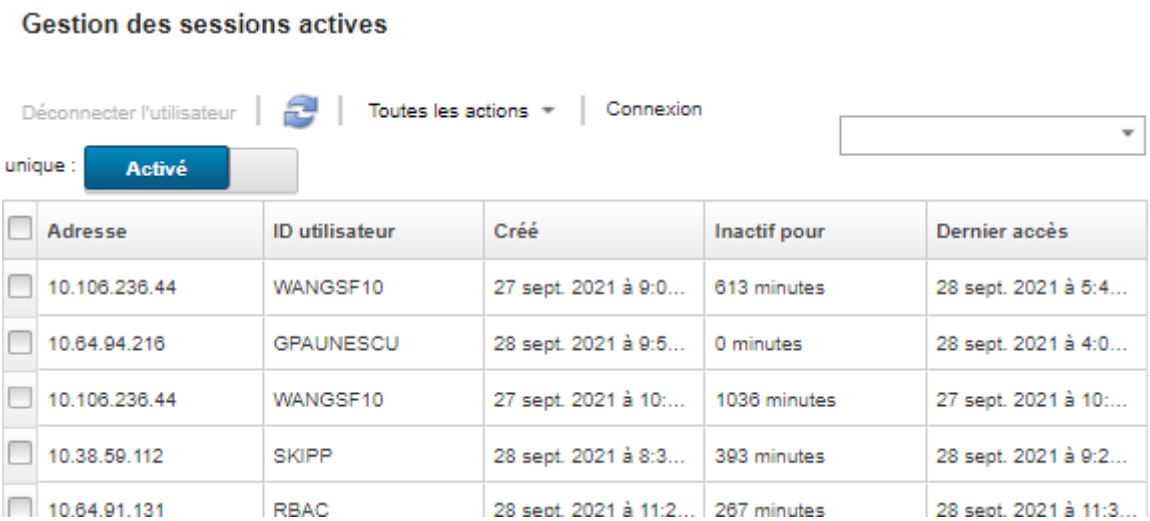
Procédure

- Vous pouvez obtenir une liste d'utilisateurs actifs et les adresses IP correspondantes en cliquant sur **Tableau de bord** dans la barre de menus de XClarity Administrator.

  Les sessions utilisateur actives sont répertoriées dans la section Activité.

- Vous pouvez obtenir la liste de tous les utilisateurs actifs (autres que l'utilisateur en cours) et les adresses IP correspondantes en cliquant sur **Administration → Sécurité** dans la barre de menus de XClarity Administrator, puis en cliquant sur **Sessions actives**.

  Remarque : Les sessions utilisateur qui sont inactives pendant une durée spécifique sont automatiquement déconnectées. Vous pouvez définir le délai d'inactivité en cliquant sur **Administration → Sécurité** à partir de la barre de menu XClarity Administrator, en cliquant sur Paramètres de sécurité de compte, puis en définissant la valeur de **Délai d'attente d'inactivité de session Web**. Notez que la modification n'affecte pas les sessions utilisateur actives. Elle affecte uniquement les sessions utilisateur qui démarrent une fois le paramètre modifié.



Gestion de données d'identification stockées

Les *données d'identification stockées* sont utilisés pour gérer l'autorisation et l'accès aux chassis et aux serveurs qui sont gérés par Lenovo XClarity Administrator à l'aide de l'authentification locale.

Avant de commencer

Vous devez disposer de droits **lxc-supervisor** ou **lxc-security-admin** pour créer, modifier ou supprimer des données d'identification stockées.

À propos de cette tâche

Des données d'identification stockées doivent être un compte utilisateur local sur un appareil ou un compte utilisateur dans un serveur Active Directory.

Si vous choisissez de gérer des appareils à l'aide de l'authentification locale à la place de l'authentification gérée XClarity Administrator, vous devez sélectionner un compte à données d'identification stockées pendant la procédure de gestion.

Important : XClarity Administrator ne valide pas le nom d'utilisateur et le mot de passe que vous spécifiez pour les données d'identification stockées. Il vous incombe de veiller à ce que les informations spécifiées correspondent à un compte d'utilisateur actif sur l'appareil local ou dans Active Directory (si l'appareil géré est configuré de sorte d'utiliser Active Directory pour authentification).

Attention : Les données d’identification stockées doivent avoir accès superviseur ou des droits suffisants pour apporter des modifications de configuration sur l’appareil. Si vous essayez de gérer un serveur avec des données d’identification stockées qui n’ont pas de droits suffisants sur l’appareil, le processus de gestion peut aboutir, mais des actions de l'inventaire administratif supplémentaires sur l’appareil risquent d’échouer en raison d'erreur d'accès refusé, ce qui peut conduire à des problèmes de connectivité perçus avec l’appareil.

Procédure

Pour ajouter des données d'identification stockées à XClarity Administrator, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Sécurité**. La page Sécurité s'affiche.

Etape 2. Cliquez sur **Données d'identification stockées** sous la section Authentification gérée pour afficher la page Données d'identification stockées.

Etape 3. Cliquez sur l'icône **Créer** ( ) pour créer des données d'identification stockées. La boîte de dialogue Créer de nouvelles données d'identification stockées s'affiche

Etape 4. Entrez les informations ci-après dans la boîte de dialogue.
- Entrez un nom d'utilisateur et une description (facultatif) pour les données d'identification stockées.
- Entrez et confirmez le mot de passe des données d'identification stockées.
- Vous pouvez, si vous le souhaitez, saisir et confirmer le mot de passe associé aux données d'identification de récupération RECOVERY_ID stockées.

Etape 5. Cliquez sur **Créer des données d'identification stockées**.

Après avoir terminé

Le compte des données d'identification stockées s'affiche dans le tableau Données d'identification stockées. Le tableau présente l'ID et la description associées de chaque compte de données d'identification stockées.

Sur la page Données d'identification stockées, vous pouvez effectuer les actions suivantes sur un compte de données d'identification stockées sélectionné :

- Modifiez le nom d'utilisateur, le mot de passe et la description d'un compte de données d'identification stockées en cliquant sur l'icône **Éditer** ( ).

  Remarque : Si vous gérez un appareil en utilisant des données d'identification stockées et activez l'authentification gérée, vous ne pouvez pas éditer ces données d'identification stockées.

- Supprimez le compte de données d'identification stockées en cliquant sur l'icône **Supprimer** ( ).

Pour résoudre les données d'identification stockées qui ont expiré ou sont non valides, voir Résolution de données d'identification expirées ou non valides pour un serveur.

Gestion des rôles et des groupes du rôle

Un *rôle* permet de contrôler l'accès utilisateur aux ressources et de restreindre les actions que les utilisateurs peuvent exécuter sur ces ressources. Un *groupe de rôles* est un ensemble d'un ou de plusieurs rôles, utilisé pour affecter ces rôles à plusieurs utilisateurs. Les rôles que vous configurez pour un groupe de rôles déterminent le niveau d'accès qui est accordé à chaque utilisateur membre de ce groupe de rôles. Chaque utilisateur Lenovo XClarity Administrator doit être membre d'au moins un groupe de rôles.

Création d'un rôle personnalisé

Un *rôle* est un ensemble de *privilèges*, ou d'autorisation, pour réaliser une action spécifique. Lenovo XClarity Administrator inclut plusieurs rôles prédéfinis par défaut. Vous pouvez créer des rôles personnalisés qui appliquent un ensemble de privilèges que les utilisateurs peuvent exploiter.

Avant de commencer

Vous devez disposer de droits **lxc-supervisor** ou **lxc-security-admin** pour réaliser cette tâche.

À propos de cette tâche

Pour créer un rôle personnalisé, sélectionnez un ou plusieurs rôles prédéfinis qui sont les plus proches de la portée pour le rôle que vous souhaitez créer, puis désélectionnez les privilèges individuels que vous souhaitez limiter. Cela garantit que vous obtenez tous les privilèges prévus et que le rôle est correctement construit avec les privilèges dépendants.

Certains privilèges XClarity Administrator dépendent des privilèges du module de gestion correspondants pour effectuer des actions sur les appareils gérés (voir Privilèges de module de gestion v1 et Privilèges de module de gestion v2). Un privilège XClarity Administrator peut vous permettre de demander une action sur un appareil géré, mais l'appareil refusera la demande si vous ne disposez pas des privilèges correspondants pour le module CMM, IMM ou XCC. Par exemple, si vous créez un rôle personnalisé pour effectuer des

actions d’alimentation sur des appareils gérés, vous ajoutez le privilège **lxc-inventory-modify-device-power-state** et :

- Pour un serveur ThinkSystem dans une armoire, ajoutez le privilège **mm-power-and-restart-access-v1**.
- Pour un châssis Flex System entier (y compris les appareils du châssis), ajoutez le privilège **mm-power-and-restart-access-v1**.
- Pour un serveur ThinkSystem dans un châssis, ajoutez le privilège **mm-power-and-restart-access-v1**, **mm-blade-operator-v2** et **mm-blade-#-scope-v2** qui correspond au serveur cible.

Tous les rôles contiennent des privilèges en lecture seule. Aucun rôle personnalisé ne peut être plus restrictif que le rôle **lxc-operator**.

Si un utilisateur ne dispose pas des privilèges pour effectuer des actions spécifiques, les éléments de menu, les icônes de barre d’outils et les boutons qui exécutent ces actions sont désactivés (en grisé).

XClarity Administrator fournit un groupe de rôles pour chaque rôle prédéfini, qui utilisent le même nom que le rôle. Envisagez de créer un groupe de rôles pour les nouveaux rôles que vous créez. Pour plus d'informations sur les groupes de rôles, voir Création d'un groupe du rôle personnalisé.

- **lxc-supervisor**. Les utilisateurs auxquels ce rôle est affecté peuvent accéder, configurer et effectuer toutes les opérations disponibles sur le serveur de gestion et tous les appareils gérés.Les utilisateurs auxquels ce rôle est affecté ont accès à tous les appareils gérés. Vous ne pouvez pas limiter l'accès aux appareils pour ce rôle.
- **lxc-admin**. Les utilisateurs auxquels ce rôle est affecté peuvent modifier les paramètres non liés à la sécurité et exécuter toutes les opérations non liées à la sécurité sur le serveur de gestion, comme la mise à jour et le redémarrage du serveur de gestion. Ce rôle offre également la possibilité d'afficher toutes les informations de configuration et d'état sur le serveur de gestion et les appareils gérés.
- **lxc-security-admin**. Les utilisateurs auxquels ce rôle est affecté peuvent modifier les paramètres de sécurité et effectuer des opérations liées à la sécurité sur le serveur de gestion et les appareils gérés. Ce rôle offre également la possibilité d'afficher toutes les informations de configuration et d'état sur le serveur de gestion et les appareils gérés.

  Les utilisateurs auxquels ce rôle est affecté ont accès à tous les appareils gérés. Vous ne pouvez pas limiter l'accès aux appareils pour ce rôle.
- **lxc-hw-admin**. Les utilisateurs auxquels ce rôle est affecté peuvent modifier les paramètres non liés à la sécurité et effectuer des opérations non liées à la sécurité sur le matériel géré, comme la mise à jour et le redémarrage des appareils gérés. Ce rôle offre également la possibilité d'afficher toutes les informations de configuration et d'état sur le serveur de gestion et tous les appareils gérés.
- **lxc-fw-admin**. Les utilisateurs auxquels ce rôle est affecté peuvent créer des stratégies de microprogramme et déployer ces stratégies sur des appareils gérés. Les utilisateurs qui n'ont pas ce rôle peuvent uniquement afficher les informations sur les règles.
- **lxc-os-admin**. Les utilisateurs ayant ce rôle peuvent télécharger et déployer des systèmes d'exploitation et des mises à jour de pilote de périphérique sur les serveurs gérés. Les utilisateurs qui n'ont pas ce rôle peuvent uniquement afficher les informations sur le système d'exploitation et le pilote de périphérique.
- **lxc-service-admin**. Les utilisateurs auxquels ce rôle est affecté peuvent collecter et télécharger des fichiers de maintenance pour XClarity Administrator et les appareils gérés. Les utilisateurs qui n’ont pas ce rôle peuvent collecter, mais pas télécharger des données de maintenance.
- **lxc-hw-manager**. Les utilisateurs auxquels ce rôle est affecté peuvent reconnaître de nouveaux appareils et placer ces derniers sous le contrôle de gestion de XClarity Administrator. Ce rôle interdit aux utilisateurs d'effectuer des opérations ou de modifier des paramètres de configuration sur le serveur de gestion et les appareils gérés, au-delà de ces opérations qui sont nécessaires pour reconnaître et gérer de nouveaux appareils.
- **lxc-operator**. Les utilisateurs auxquels ce rôle est affecté peuvent afficher toutes les informations de configuration et d'état sur le serveur de gestion et les appareils gérés. Ce rôle interdit aux utilisateurs d'effectuer des opérations ou de modifier des paramètres de configuration sur le serveur de gestion et les appareils gérés.

- **lxc-recovery**. Les utilisateurs auxquels ce rôle est affecté peuvent modifier les paramètres de sécurité et effectuer des opérations liées à la sécurité sur le serveur de gestion. Ces utilisateurs peuvent aussi s'authentifier directement auprès de XClarity Administrator même si la méthode d'authentification est définie sur un serveur LDAP externe. Ce rôle fournit un mécanisme de récupération en cas d'erreur de communication avec le serveur LDAP externe qui utilise la configuration « Données d'identification de connexion ».

  Les utilisateurs auxquels ce rôle est affecté ont accès à tous les appareils gérés. Vous ne pouvez pas limiter l'accès aux appareils pour ce rôle.

Les rôles prédéfinis suivants sont *réservés* et ne peuvent pas être utilisés pour créer des groupes de rôles ou être affectés à de nouveaux utilisateurs.
- **lxc-sysrdr**
- **lxc-sysmgr**

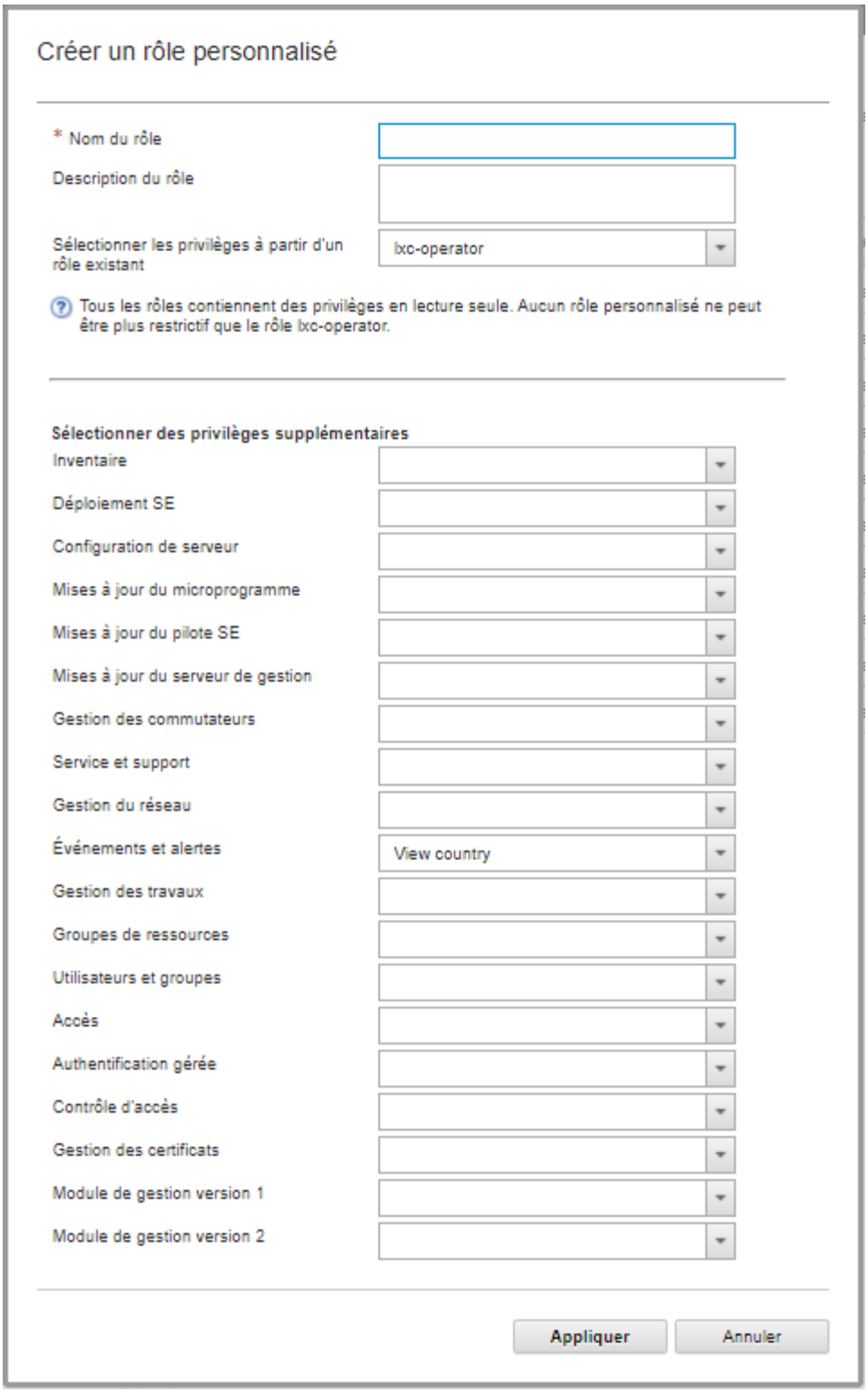
Procédure

Pour créer un rôle personnalisé, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Sécurité**.

Etape 2. Cliquez sur **Rôles** sous la section Utilisateurs et groupes afin d'afficher la page Gestion de groupe de rôle.

Etape 3. Cliquez sur l'icône **Créer** ( ) pour créer un rôle. La boîte de dialogue Créer un rôle personnalisé s'affiche.



Etape 4. Entrez un nom et une description du rôle.

Etape 5. Sélectionnez un rôle prédéfini comme point de départ pour ce rôle personnalisé.

Si vous sélectionnez un rôle existant, les privilèges associés à ce rôle sont sélectionnés dans cette boîte de dialogue.

Etape 6. Modifiez les privilèges pour ce nouveau rôle en sélectionnant ou en supprimant les privilèges à partir des menus déroulants **Sélectionner des privilèges supplémentaires**.

Remarque : Si vous sélectionnez tous les privilèges d'une catégorie spécifique et que les privilèges sont ajoutés à cette catégorie lorsque vous mettez à jour ou à niveau XClarity Administrator, les nouveaux privilèges sont automatiquement ajoutés au rôle personnalisé.

Etape 7. Cliquez sur **Créer**. Le nouveau rôle est ajouté au tableau de la page Gestion des rôles.

Résultats

Vous pouvez également réaliser les actions suivantes.

- Afficher les privilèges associés à un rôle spécifique en sélectionnant ce rôle et en cliquant sur l'icône **Afficher** ( ).
- Renommer ou éditer le rôle personnalisé en cliquant sur l'icône **Éditer** ( ). Lorsque vous éditez un rôle personnalisé, vous pouvez modifier les privilèges sélectionnés, la description et les listes des utilisateurs associés à ce rôle.

  Remarque : Vous ne pouvez pas modifier un rôle prédéfini
- Supprimer le rôle prédéfini ou personnalisé en cliquant sur l'icône **Supprimer** ( ).
- Ajouter ou supprimer des rôles à partir d'un groupe de rôles (voir Ajout et retrait de plusieurs utilisateurs d'un groupe de rôles).
- Restaurer tous les rôles prédéfinis qui ont été supprimés en cliquant sur **Toutes les actions → Rôles Restaurer la valeur par défaut**.

Autorisations prédéfinies

Lenovo XClarity Administrator fournit un ensemble de *privilèges* (autorisations) qui permettent à un utilisateur de réaliser une action spécifique. Les privilèges sont organisés en catégories, en fonction du type d'action.

Privilèges d'accès

Ces privilèges fournissent des autorisations permettant de modifier les modes cryptographique et SSL/TLS.

Nom du privilège	Description du privilège	rôles par défaut
lxc-sec-apply-crypto-settings	Appliquer les paramètres cryptographiques	lxc-recovery, lxc-security-admin, lxc-supervisor

Privilèges de contrôle d'accès

Ces privilèges fournissent des autorisations permettant de contrôler l'accès aux ressources.

Nom du privilège	Description du privilège	rôles par défaut
lxc-sec-modify-resource-access-control	Éditer les paramètres de contrôle d'accès aux ressources	lxc-recovery, lxc-security-admin, lxc-supervisor

Privilèges de gestion des certificats

Ces privilèges fournissent des autorisations de gestion des certificats de sécurité dans Lenovo XClarity Administrator.

Nom du privilège	Description du privilège	Rôles par défaut
lxc-sec-add-external-certificates	Ajouter un certificat externe	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-add-trusted-certificates	Ajouter un certificat sécurisé	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-certificate-signing	Générer une demande de signature de certificat	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-external-certificates	Supprimer un certificat externe existant	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-trusted-certificates	Supprimer un certificat existant	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-download-ca	Télécharger le certificat racine de l'autorité de certification	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-download-server-certificate	Télécharger le certificat de serveur	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-certificate-revocation-list	Modifier ou remplacer la liste de révocation de certificat	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-regenerate-ca	Regénérer le certificat racine de l'autorité de certification	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-regenerate-download-ca	Regénérer le certificat racine de l'autorité de certification	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-regenerate-server-certificate	Regénérer le certificat du serveur	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-resolve-untrusted-certificates	Résoudre les certificats non sécurisés	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-upload-server-certificate	Charger le certificat de serveur	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc_sec_view_certpol_settings	Afficher les paramètres de stratégie de certificat	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc_sec_apply_certpol_settings	Appliquer les paramètres de stratégie de certificat	lxc-security-admin, lxc-supervisor

Privilèges de surveillance et d'événements

Ces privilèges fournissent des autorisations de gestion des événements et des alertes.

Nom du privilège	Description du privilège	Rôles par défaut
lxc-event-audit	Gérer les journaux des événements et d'audit	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-monitoring-create-edit-event-forwarders	Crée et modifier des réexpéditeurs d'événements	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-monitoring-create-edit-push-services	Crée et modifier des services Push	lxc-admin, lxc-hw-admin, lxc-supervisor

Nom du privilège	Description du privilège	Rôles par défaut
lxc-monitoring-remove-event-forwarders	Supprimer les réexpéditeurs d'événement	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-monitoring-remove-push-services	Supprimer des services push	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-monitoring-set-event-thresholds	Définir les seuils d'événement	lxc-admin, lxc-hw-admin, lxc-supervisor

Privilèges de mises à jour de microprogramme.

Ces privilèges fournissent des autorisations permettant de gérer et d'appliquer des mises à jour de microprogramme, ainsi que les UpdateXpress System Packs.

Nom du privilège	Description du privilège	rôles par défaut
lxc-fwUpdates-apply-assign-policy	Affecter une stratégie de conformité de microprogramme aux appareils	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-apply-perform-updates	Appliquer des mise à jour du microprogramme	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-policies-create-policies	Créer, copier, éditer et importer des stratégies de conformité de microprogramme	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-policies-delete-policies	Supprimer les stratégies de conformité	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-repository-delete-packages	Supprimer des modules de mise à jour de microprogramme	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-repository-download-packages	Télécharger et importer des modules de mise à jour de microprogramme et réactualiser le catalogue des packages de mise à jour de microprogramme	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor
lxc-fwUpdates-repository-export-packages	Exporter des modules de mise à jour de microprogramme	lxc-admin, lxc-fw-admin, lxc-hw-admin, lxc-supervisor

Privilèges du groupe de ressources

Ces privilèges fournissent des autorisations d'utilisation des groupes de ressources.

Nom du privilège	Description du privilège	Rôles par défaut
lxc-resource-create-edit-group	Créer et modifier des groupes de ressources	lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-resource-delete-group	Supprimer des groupes de ressources	lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor

Privilèges de l'inventaire

Ces privilèges fournissent des autorisations permettant de détecter et de gérer des appareils, ainsi que de consulter l'inventaire des appareils.

Nom du privilège	Description du privilège	rôles par défaut
lxc-dm-manage-device	Gérer les châssis, les serveurs, le stockage et les commutateurs	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-dm-modify-ip-settings	Activer ou désactiver le contrôle des adresses IP en double dans le même sous-réseau	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-inventory-modify-device-power-state	Modifier l'état d'alimentation des cartouches, des CMM, des nœuds, du stockage et des commutateurs	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-inventory-modify-device-properties	Modifier les propriétés des armoires, des cartouches, des châssis, des CMM, des nœuds, du stockage et des commutateurs	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-inventory-modify-node-pfa-config-settings	Modifier les paramètres de configuration des alertes d'échec prévu	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

Privilèges de gestion des travaux

Ces privilèges fournissent des autorisations de gestion de travaux (tâches).

Nom du privilège	Description du privilège	Rôles par défaut
lxc-tasks-remove-jobs	Supprimer les travaux	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-tasks-schedule-jobs	Planifier les travaux	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor

Privilèges d'authentification gérée

Ces privilèges fournissent des autorisations permettant de gérer l’authentification, y compris les données d’identification stockées.

Nom du privilège	Description du privilège	rôles par défaut
lxc-sec-delete-stored-credentials	Supprimer les données d'identification stockées	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-stored-credentials	Éditer les données d'identification existantes	lxc-recovery, lxc-security-admin, lxc-supervisor

Privilèges de module de gestion v1

Ces privilèges sont associés aux bits d’autorisation LDAP (bitstrings) qui sont appliqués par les modules de gestion pour pour les serveurs rack et l'intégralité du châssis Flex System (y compris tous les appareils dans ce châssis).

Lenovo XClarity Administrator n'applique pas ces autorisations. Ces autorisation sont mises en place par les appareils gérés utilisant un compte utilisateur XClarity Administrator.

Si l'appareil est géré à l'aide de l'*authentification gérée* (via le serveur d'authentification local), ce dernier utilise ces autorisations pour indiquer aux appareils gérés les autorisations à accorder lorsque l'utilisateur se connecte.

Vous configurerez les mêmes autorisations que dans un serveur LDAP externe. Lorsque vous utilisez un serveur LDAP externe avec XClarity Administrator, assurez-vous d’ajouter des groupes dans ce serveur dont

les noms correspondent aux noms de groupe de rôle de XClarity Administrator et que les utilisateurs LDAP externes sont ajoutés à un ou plusieurs de ces groupes. Les utilisateurs LDAP externes doivent faire partie d'un groupe LDAP dont le nom correspond à un groupe de rôle XClarity Administratorcontenant des rôles associés aux chaînes de bits du module de gestion. XClarity Administrator utilise ces groupes pour lier les utilisateurs LDAP externes aux groupes de rôle de XClarity Administrator et aux chaînes de bits appliquées par le module de gestion. Ensuite, lorsqu'un utilisateur se connecte à un appareil géré à l'aide d'un compte utilisateur LDAP externe, le module de gestion sait s'il doit accorder des privilèges au superviseur utilisateur ou à l'opérateur.

Remarque : Les privilèges du module de gestion v1 ne sont pas pris en charge pour les commutateurs FlexSystem sur lesquels Secure IOM n'est pas activé, les commutateurs RackSwitch, les dispositifs de stockage et les serveurs ThinkServer.

Pour plus d'informations sur les bits d'autorisation LDAP pour chaque module de gestion, voir la documentation en ligne.
- Configuration de LDAP dans la documentation en ligne CMM et CMM2
- Configuration de LDAP dans la documentation en ligne IMM et IMM2
- Configuration de LDAP dans la documentation en ligne XCC

Nom du privilège	Description du privilège	rôles par défaut
mm-advanced-adaptor-configuration-v1	Configuration avancée d'adaptateur	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-basic-configuration-v1	Configuration de base	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-clear-event-logs-v1	Effacer les journaux des événements	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-deny-always-v1	Refuser toujours	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-networking-and-security-v1	Réseau et sécurité	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-power-and-restart-access-v1	Activation/redémarrage de l'accès aux serveurs et aux commutateurs Flex	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-remote-console-access-v1	Accès au contrôle à distance pour les serveurs	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-remote-console-and-virtual-media-access-v1	Accès à la console à distance et aux médias virtuels pour les serveurs	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-supervisor-v1	Accès superviseur	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-user-account-management-v1	Gestion des utilisateurs	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor

Privilèges de module de gestion v2

Ces privilèges sont associés aux bits d'autorisation LDAP (bitstrings) qui sont appliqués par les modules de gestion pour des appareils FlexSystem et ThinkSystem individuels dans un châssis (châssis, serveurs et commutateurs avec Secure IOM activé).

Lenovo XClarity Administrator n'applique pas ces autorisations. Ces autorisation sont mises en place par les appareils gérés utilisant un compte utilisateur XClarity Administrator.

Si l'appareil est géré à l'aide de l'*authentification gérée* (via le serveur d'authentification local), ce dernier utilise ces autorisations pour indiquer aux appareils gérés les autorisations à accorder lorsque l'utilisateur se connecte.

Vous configurerez les mêmes autorisations que dans un serveur LDAP externe. Lorsque vous utilisez un serveur LDAP externe avec XClarity Administrator, assurez-vous d'ajouter des groupes dans ce serveur dont les noms correspondent aux noms de groupe de rôle de XClarity Administrator et que les utilisateurs LDAP externes sont ajoutés à un ou plusieurs de ces groupes. Les utilisateurs LDAP externes doivent faire partie d'un groupe LDAP dont le nom correspond à un groupe de rôle XClarity Administratorcontenant des rôles associés aux chaînes de bits du module de gestion. XClarity Administrator utilise ces groupes pour lier les utilisateurs LDAP externes aux groupes de rôle de XClarity Administrator et aux chaînes de bits appliquées par le module de gestion. Ensuite, lorsqu'un utilisateur se connecte à un appareil géré à l'aide d'un compte utilisateur LDAP externe, le module de gestion sait s'il doit accorder des privilèges au superviseur utilisateur ou à l'opérateur.

Remarques :

- Vous devez également spécifier des droits du module de gestion v1 pour l'intégralité du châssis (voir Privilèges de module de gestion v1).
- Les privilèges de module de gestion v2 ne sont pas pris en charge pour les commutateurs FlexSystem sur lesquels Secure IOM n'est pas activé.
- Pour le châssis Lenovo ThinkSystem, assurez-vous que le IMM2 est installé afin de permettre l'« administration du nœud » pour le rôle personnalisé. Si vous souhaitez que le rôle personnalisé contrôle tous les appareils du châssis Lenovo ThinkSystem, assurez-vous que le modèle IMM2 est installé afin de lui permettre également d'avoir une « Portée Node X »

Pour plus d'informations sur les bits d'autorisation LDAP pour chaque module de gestion, voir la documentation en ligne.
- Configuration de LDAP dans la documentation en ligne CMM et CMM2
- Configuration de LDAP dans la documentation en ligne IMM et IMM2
- Configuration de LDAP dans la documentation en ligne XCC

Nom du privilège	Description du privilège	Rôles par défaut
mm-blade-1-scope-v2	Portée du nœud 1	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-2-scope-v2	Portée du nœud 2	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-3-scope-v2	Portée du nœud 3	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-4-scope-v2	Portée du nœud 4	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-5-scope-v2	Portée du nœud 5	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-6-scope-v2	Portée du nœud 6	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-7-scope-v2	Portée du nœud 7	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

Nom du privilège	Description du privilège	Rôles par défaut
mm-blade-8-scope-v2	Portée du nœud 8	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-9-scope-v2	Portée du nœud 9	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-10-scope-v2	Portée du nœud 10	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-11-scope-v2	Portée du nœud 11	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-12-scope-v2	Portée du nœud 12	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-13-scope-v2	Portée du nœud 13	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-14-scope-v2	Portée du nœud 14	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-administration-v2	Administration du nœud	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-configuration-v2	Configuration de nœud	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-operator-v2	Opérateur du serveur lame	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-blade-remote-presence-v2	Présence d'un nœud distant	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-chassis-administration-v2	Administration du châssis	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-chassis-configuration-v2	Configuration du châssis	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-chassis-log-management-v2	Gestion du compte du châssis de journalisation	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-chassis-operator-v2	Opérateur de châssis	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-chassis-scope-v2	Portée du châssis	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-chassis-user-account-management-v2	Gestion des utilisateurs	lxc-admin, lxc-hw-admin, lxc-recovery, lxc-security-admin, lxc-supervisor
mm-deny-always-v2	Refuser toujours	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-io-module-1-scope-v2	Portée du module d'E-S 1	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-io-module-2-scope-v2	Portée du module d'E-S 2	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

Nom du privilège	Description du privilège	Rôles par défaut
mm-io-module-3-scope-v2	Portée du module d'E-S 3	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-io-module-4-scope-v2	Portée du module d'E-S 4	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-switch-administration-v2	Administration du commutateur	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-switch-configuration-v2	Configuration du commutateur	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
mm-switch-operator-v2	Opérateur de commutateur	lxc-admin, lxc-hw-admin, lxc-supervisor
mm-supervisor-v2	Accès superviseur	lxc-admin, lxc-hw-admin, lxc-supervisor

Autorisations du serveur de gestion

Ces privilèges fournissent des autorisations de mise à jour du serveur de gestion.

Nom du privilège	Description du privilège	rôles par défaut
lxc-mgmtserverupdates-delete-updates	Supprimer les mises à jour du serveur de gestion	lxc-admin, lxc-fw-admin, lxc-supervisor
lxc-mgmtserverupdates-download-updates	Télécharger et importer les mises à jour du serveur de gestion et réactualiser le catalogue du serveur de gestion	lxc-admin, lxc-fw-admin, lxc-supervisor
lxc-mgmtserverupdates-perform-updates	Appliquer les mises à jour du serveur de gestion	lxc-admin, lxc-fw-admin, lxc-supervisor

Privilèges de gestion du réseau

Ces privilèges fournissent des autorisations pour configurer les paramètres réseau.

Nom du privilège	Description du privilège	Rôles par défaut
lxc-network-edit	Modifier l'accès réseau	lxc-admin, lxc-supervisor

Privilèges du déploiement du système d'exploitation

Ces privilèges fournissent des autorisations de gestion et de déploiement des systèmes d'exploitation.

Nom du privilège	Description du privilège	Rôles par défaut
lxc-osdeploy-create-edit-remote-file-server	Créer et éditer une entrée de serveur de fichiers distant	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-create-import-export-edit-os-files	Créer, importer, exporter et éditer des images SE et des fichiers personnalisés	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-delete-os-files	Supprimer des images SE et des fichiers personnalisés	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-delete-remote-file-server	Supprimer une entrée de serveur de fichiers distant	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor

Nom du privilège	Description du privilège	Rôles par défaut
lxc-osdeploy-edit-global-settings	Éditer les informations dans la boîte de dialogue des paramètres globaux **Remarque :** La modification des paramètres d'affectation IP globale affecte les paramètres réseau. Par conséquent, pour apporter des modifications aux paramètres d'affectation IP globaux, vous devez également disposer de privilèges **lxc-osdeploy-edit-settings-and-deploy-os-images-**.	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osdeploy-edit-settings-and-deploy-os-images	Modifier les paramètres de déploiement et déployer les images SE sur un ou plusieurs serveurs	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor

Privilèges de mises à jour du pilote du système d'exploitation

Ces privilèges fournissent des autorisations de gestion et d'application des pilotes de périphérique SE.

Nom du privilège	Description du privilège	rôles par défaut
lxc-osDriverUpdates-apply-assign-uxsp	Attribuer des pilotes de périphérique SE UXSP aux appareils	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-apply-check-authentication	Vérifier l'authentification SE	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-apply-check-compliance	Contrôler la conformité du pilote de périphérique SE	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-apply-perform-updates	Appliquer des mises à jour du pilote de périphérique SE	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-repository-delete-packages	Supprimer des modules de mise à jour du pilote de périphérique SE	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor
lxc-osDriverUpdates-repository-download-packages	Télécharger et importer des packages de mise à jour de pilote de périphérique du système d'exploitation et actualiser le catalogue UXSP de pilote de périphérique du système d'exploitation	lxc-admin, lxc-hw-admin, lxc-os-admin, lxc-supervisor

Privilèges des utilisateurs et des groupes

Ces privilèges fournissent des autorisations permettant de gérer les comptes utilisateur et les groupes.

Nom du privilège	Description du privilège	rôles par défaut
lxc-sec-apply-saml-settings	Appliquer les paramètres SAML	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-role-groups	Supprimer un groupe de rôle	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-delete-roles	Suppression d'un rôle	lxc-recovery, lxc-security-admin, lxc-supervisor

Nom du privilège	Description du privilège	rôles par défaut
lxc-sec-delete-users	Supprimer un utilisateur	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-edit-account-settings	Modifier les paramètres de sécurité de compte	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-ldap-settings	Appliquer les paramètres LDAP	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-role-groups	Modifier un groupe de rôle	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-roles	Modifier un rôle	lxc-recovery, lxc-security-admin, lxc-supervisor
lxc-sec-modify-users	Modifier un utilisateur	lxc-recovery, lxc-security-admin, lxc-supervisor

Privilèges de configuration de serveur

Ces privilèges fournissent des autorisations de distribuer ou de prédistribuer des serveurs à l'aide des modèles de configuration.

Nom du privilège	Description du privilège	Rôles par défaut
lxc-cp-edit-management-ip	Modifier la gestion des adresses IP pour le châssis	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-edit-preferences	Définir des préférences de modèles de configuration	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-address-pools	Gérer les pools d'adresses	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-patterns	Gérer les modèles	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-placeholders	Gérer les marques de réservation	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-manage-profiles	Déployez des modèles, déployer des marques de réservation sur le châssis et gérer les profils	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-cp-other-server-config	Réinitialiser le stockage local et appliquer l'opération de sécurité Optane DCPMM	lxc-admin, lxc-hw-admin, lxc-supervisor

Privilèges de service

Ces privilèges permettent de définir des contacts de support pour chaque appareil géré, de collecter et d'envoyer des fichiers de maintenance au support Lenovo, de configurer la notification automatique à des prestataires de services lorsque certains événements réparables se produisent sur des appareils spécifiques, et d'afficher un état du ticket de maintenance, et les informations relatives à la garantie ainsi qu'à collecter et à transmettre des données de service.

Nom du privilège	Description du privilège	Rôles par défaut
lxc-ss-alter-backup-credentials	Modifier les données d'identification FFDC pour la sauvegarde	lxc-admin, lxc-hw-admin, lxc-service-admin, lxc-supervisor
lxc-ss-call-home	Effectuer un appel vers Lenovo	lxc-admin, lxc-hw-admin, lxc-supervisor

Nom du privilège	Description du privilège	Rôles par défaut
lxc-ss-change-service-recovery-password	Modification du mot de passe de récupération de service	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-ss-change-service-tickets	Modifier les tickets de maintenance	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-ss-remove-service-tickets	Supprimer des tickets de maintenance	lxc-admin, lxc-hw-admin, lxc-supervisor
lxc-ss-run-service-forwarders	Exécuter les réexpéditeurs de service	lxc-admin, lxc-hw-admin, lxc-supervisor

Privilèges de configuration de commutateur

Ces privilèges fournissent des autorisations pour configurer les commutateurs et pour sauvegarder et restaurer les données de configuration du commutateur.

Nom du privilège	Description du privilège	rôles par défaut
lxc-netcfg-template-management	Créer, modifier, supprimer et déployer les modèles de configuration de commutateur et suppression d'un déploiement de configuration de commutateur	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-swirm-config-management	Sauvegarder, restaurer, supprimer, exporter et importer une configuration de commutateur - fichiers de données	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor
lxc-swirm-port-management	Modifier l'état du port de commutateur	lxc-admin, lxc-hw-admin, lxc-hw-manager, lxc-supervisor

Création d'un groupe du rôle personnalisé

Un *groupe du rôle* est un ensemble de rôles et un ensemble d'utilisateurs membres du même ensemble de rôles. Le niveau d'accès accordé à chaque utilisateur du groupe de rôle est basé sur les rôles attribués à ce groupe de rôle. XClarity Administrator fournit les groupes de rôles prédéfinis, qui correspondent à chaque rôle prédéfini. Vous pouvez également créer des groupes de rôle.

À propos de cette tâche

Chaque utilisateur XClarity Administrator doit être membre d'au moins un groupe de rôles.

Les groupes de rôles suivants sont prédéfinis dans XClarity Administrator :

- **LXC-SUPERVISOR**. Inclut le rôle **lxc-supervisor**.
- **LXC-ADMIN**. Inclut le rôle **lxca-admin**.
- **LXC-SECURITY-ADMIN**. Inclut le rôle **lxc-security-admin**.
- **LXC-HW-ADMIN**. Inclut le rôle **lxc-hw-admin**.
- **LXC-FW-ADMIN**. Inclut le rôle **lxc-fw-admin**.
- **LXC-OS-ADMIN**. Inclut le rôle **lxc-os-admin**.
- **LXC-SERVICE-ADMIN**. Inclut le rôle **lxc-service-admin**.
- **LXC-HW-MANAGER**. Inclut le rôle **lxc-hw-manager**.
- **LXC-OPERATOR**. Inclut le rôle **lxc-operator**.

- **LXC-RECOVERY**. Inclut le rôle **lxc-recovery**.

Les rôles prédéfinis suivants sont *réservés* et ne peuvent pas être utilisés pour créer des groupes de rôles ou être affectés à de nouveaux utilisateurs.
- **lxc-sysrdr**
- **lxc-sysmgr**

Procédure

Pour créer un groupe de rôles, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Sécurité**.

Etape 2. Cliquez sur **Groupes de rôles** sous la section Utilisateurs et groupes afin d'afficher la page Gestion de groupe.

Etape 3. Cliquez sur l'icône **Créer** () pour créer un groupe de rôles. La boîte de dialogue Créer un groupe de rôles s'affiche.

Etape 4. Entrez un nom et une description du groupe.

Remarque : Astuce : pour le nom du groupe, vous pouvez utiliser des lettres, des chiffres, des espaces blancs, des traits de soulignement, des tirets et des points.

Etape 5. Sélectionnez un ou plusieurs rôles à affecter à ce groupe de rôle.

Etape 6. Sélectionnez un ou plusieurs utilisateurs en tant que membres de ce groupe de rôle.

Etape 7. Cliquez sur **Créer**. Le nouveau groupe de rôles est ajouté au tableau de la page Gestion des groupes.

Résultats

Le groupe de rôles s'affiche dans le tableau Groupes de rôles. Le tableau indique les rôles d'autorisation associés et les membres de chaque groupe de rôles.

Après avoir créé un groupe de rôles, vous pouvez exécuter les actions suivantes sur un groupe de rôles sélectionné :

- Pour ajouter ou supprimer des rôles affectés à ce groupe du rôle, cliquez sur l'icône **Éditer** ( ).
- Ajouter ou retirer des utilisateurs comme membres du groupe de rôles (voir « Ajout et retrait de plusieurs utilisateurs d'un groupe de rôles » à la page 58).
- Exporter des informations sur les groupes de rôles, comme les droits d'accès, en cliquant sur **Toutes les actions → Exporter au format CSV**.
- Supprimer le groupe de rôles en cliquant sur l'icône **Supprimer** ( ).Vous ne pouvez pas supprimer les groupes de rôle prédéfinis.

Une fois qu'un groupe de rôles est créé, édité ou supprimé, la modification est immédiatement distribuée à chaque appareil géré.

Ajout et retrait de plusieurs utilisateurs d'un groupe de rôles

Vous pouvez modifier l'appartenance dans un groupe de rôles en ajoutant ou en retirant plusieurs utilisateurs.

Procédure

Pour ajouter et retirer des utilisateurs dans un groupe de rôles, procédez comme suit.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Administration → Sécurité**.

Etape 2. Cliquez sur **Groupes de rôles** sous la section Utilisateurs et groupes afin d'afficher la page Gestion de groupe.

Etape 3. Cliquez sur l'icône **Éditer** ( ) pour modifier le groupe de rôles. La boîte de dialogue Modifier le groupe du rôle s'affiche.

Etape 4. Cliquez sur la liste déroulante **Liste d'utilisateurs**, puis sélectionnez les utilisateurs à inclure ou désélectionnez l'utilisateur à exclure de ce groupe de rôles.

Etape 5. Cliquez sur **Enregistrer**. La colonne **Liste d'utilisateurs** affiche l'appartenance utilisateur en cours dans le groupe de rôles.

Gestion de l'accès aux appareils

Le contrôle d'accès aux appareils est désactivé par défaut. Il ne prend effet que lorsque vous l'activez

Lorsque les appareils sont initialement gérés par Lenovo XClarity Administrator, un ensemble prédéfini de groupes de rôles dispose par défaut du droit d'accès à ces appareils. Cet ensemble prédéfini est vide par défaut, jusqu'à ce qu'il soit configuré.

Vous pouvez modifier les groupes de rôles qui peuvent accéder à des appareils gérés spécifiques. Lors qu'une autorisation est accordée à certains groupes de rôles, seuls les utilisateurs qui sont membres de ces groupes peuvent afficher ces appareils spécifiques et agir sur ces derniers.

Contrôle de l'accès à des appareils spécifiques

Lorsque les appareils sont initialement gérés par Lenovo XClarity Administrator, un ensemble prédéfini de groupes de rôles dispose par défaut du droit d'accès à ces appareils. Vous pouvez modifier les groupes de rôles qui peuvent accéder à des appareils gérés spécifiques. Lors qu'une autorisation est accordée à certains groupes de rôles, seuls les utilisateurs qui sont membres de ces groupes peuvent afficher ces appareils spécifiques et agir sur ces derniers.

Avant de commencer

Seuls les utilisateurs disposant des droits **lxc-supervisor**, **lxc-security-admin** ou **lxc-recovery** peuvent effectuer cette action.

À propos de cette tâche

Le contrôle d'accès est défini sur des appareils individuels. Il n'est pas défini pour des conteneurs, tels que les armoires et les groupes de ressources.

Pour les composants dans un châssis ou un boîtier, les utilisateurs doivent disposer d'au moins un accès en lecture au châssis ou au boîtier pour les composants d'affichage dans ce châssis ou ce boîtier. Même s'ils ne disposent pas d'un accès en lecture seule au châssis ou boîtier, ces utilisateurs peuvent voir tout de même les composants du châssis dans certaines vues mais pas nécessairement dans toutes les vues.

Les utilisateurs disposant des droits **lxc-supervisor** peuvent afficher et effectuer des actions sur toutes les ressources, qu'ils se trouvent ou non dans un groupe de rôles auquel des droits d'accès à une ressource ont été spécifiquement octroyés. Vous ne pouvez retirer l'accès à aucune des ressources pour le groupe de rôles **lxc-supervisor**.

Si un utilisateur n'est pas membre d'un groupe de rôles ayant accès à un appareil géré spécifique, il ne peut pas afficher cet appareil spécifique ou agir sur ce dernier. Cela inclut le lancement de l'interface Web du contrôleur de gestion via Lenovo XClarity Administrator. En outre, pour les appareils Flex et System x, les utilisateurs ne peuvent pas se connecter directement à un module CMM ou à un contrôleur de gestion auxquels ils n'ont pas accès.

Les paramètres de contrôle d'accès par défaut permettent de définir les droits d'accès aux appareils lorsque ceux-ci sont initialement gérés par XClarity Administrator et de rétablir les droits d'accès par défaut pour un appareil spécifique. Le fait de modifier les paramètres de contrôle d'accès par défaut ne modifie pas automatiquement les droits d'accès aux appareils déjà gérés.

Important :

- Si un utilisateur est membre de plusieurs groupes de rôles et que ces groupes sont affectés à des appareils différents, les actions que l'utilisateur est autorisé à exécuter sur chaque appareil peuvent être différentes. Par exemple, si l'utilisateur est membre des groupes de rôles par défaut LXC-FW-ADMIN et LXC-OS-ADMIN, et si seul le groupe LXC-FW-ADMIN est autorisé à accéder au serveur A, l'utilisateur peut mettre à jour le microprogramme sur ce serveur mais il ne peut pas y déployer un système d'exploitation. En revanche, si seul le groupe LXC-OS-ADMIN avait eu accès au serveur B, ce même utilisateur aurait pu déployer un système d'exploitation sur le serveur B mais il n'aurait pas pu mettre à jour le microprogramme sur ce serveur.
- Lorsque l'accès à un appareil ayant une ressource parent (telle qu'un serveur ou un commutateur dans un châssis Flex) est limité, un utilisateur doit disposer au minimum d'une autorisation d'accès en lecture seule à la ressource parent afin de pouvoir interagir pleinement avec l'appareil. Si un utilisateur dispose au minimum d'un accès en lecture seule à l'appareil mais pas à la ressource parent, il ne sera pas en mesure de voir les vues d'inventaire de l'appareil, mais pourra voir des informations au sujet de l'appareil dans certaines vues, par exemple les tâches et les événements.

  Par exemple, vous pouvez créer un groupe du rôle pour le parent et assigner ce groupe du rôle au rôle **lxc-operator**. Incluez tous les utilisateurs qui devraient avoir accès à l'un des enfants (par exemple, un serveur ou un commutateur dans un châssis Flex) dans ce groupe du rôle. Incluez ensuite ce groupe du rôle dans l'un des groupes ayant accès à la ressource parent.

Procédure

Pour contrôler l'accès à des appareils spécifiques en associant des groupes de rôles à ces appareils, procédez comme suit.

Etape 1. Dans le menu principal de Lenovo XClarity Administrator, cliquez sur **Administration → Sécurité**.

Etape 2. Cliquez sur **Vue des ressources** dans le panneau de navigation de gauche. La page Vue des ressources s'affiche.

Vous pouvez trier les colonnes du tableau afin de faciliter la recherche de dispositifs spécifiques. Vous pouvez également sélectionner un type d'appareil dans le menu déroulant **Type de ressource**, un groupe de rôles dans le menu déroulant **Groupes de rôles**, un groupe de ressources dans le menu déroulant **Groupes de ressources** et saisir du texte (un nom de ressource ou un type, par exemple) dans la zone **Filtre** pour répertorier uniquement les appareils qui répondent aux critères sélectionnés.

Etape 3. Sélectionnez un ou plusieurs appareils dont vous souhaitez contrôler l'accès.

Etape 4. Cliquez sur l'icône **Éditer** (). La boîte de dialogue Éditer les ressources s'affiche avec les appareils cibles répertoriés dans la zone **Nom de la ressource**.

Etape 5. Dans la liste déroulante **Groupes de rôles**, sélectionnez les groupes de rôles auxquels vous souhaitez accorder des droits d'accès aux appareils cibles.

Remarque : Si l'appareil dispose d'une ressource parent (par exemple, un serveur ou un commutateur dans un châssis Flex), vous pouvez spécifier l'accès à la fois pour l'appareil (la colonne de droite) et la ressource parent (la colonne de gauche).

Etape 6. Affectez à **Accès public** la valeur `No`. Cela signifie que seuls les utilisateurs qui sont membres des groupes de rôles sélectionnés peuvent accéder aux appareils cibles.

Etape 7. Cliquez sur **Enregistrer**.

Etape 8. Une fois l'affectation des droits terminée, cliquez sur le bouton **Désactivé** pour définir **Contrôle d'accès aux ressources** sur activé.

Vous pouvez activer le contrôle d'accès aux ressources à tout moment, avant ou après la configuration de l'accès à des appareils spécifiques. Lorsque ce paramètre est activé, la

configuration affichée dans le tableau prend effet, empêchant notamment aux utilisateurs qui ne disposent pas des droits de superviseur d'accéder aux appareils dont l'accès n'est configuré pour aucun groupe de rôles.

Après avoir terminé

Vous pouvez également contrôler l'accès aux appareils en procédant comme suit :

- Modifiez les droits des paramètres Groupes de rôles et Accès public par défaut en cliquant sur l'icône **Éditer** (), puis en cliquant sur **Réinitialisation aux valeurs par défaut**.
- Modifiez les paramètres Groupe de rôles et Accès public par défaut (voir Modification des droits par défaut).
- Désactivez le contrôle d'accès aux ressources en cliquant sur le bouton **Activé** pour définir **Contrôle d'accès aux ressources** sur désactivé. Cela signifie que tous les groupes de rôles peuvent accéder à tous les appareils gérés.

Désactivation du contrôle d'accès aux ressources

Vous pouvez désactiver le contrôle d'accès pour tous les appareils ou pour des appareils spécifiques afin que tous les utilisateurs puissent afficher et agir sur ces appareils.

À propos de cette tâche

Seuls les utilisateurs disposant des droits **lxc-supervisor**, **lxc-security-admin** ou **lxc-recovery** peuvent effectuer cette action.

Procédure

Pour désactiver le contrôle d'accès aux ressources, procédez comme suit.

- Pour tous les appareils gérés
  1. Dans le menu principal de Lenovo XClarity Administrator, cliquez sur **Administration → Sécurité**.
  2. Cliquez sur **Vue des ressources** dans le panneau de navigation de gauche. La page Vue des ressources s'affiche.
  3. Cliquez sur le bouton **Activé** pour définir **Contrôle d'accès aux ressources** sur désactivé.
- Pour des appareils gérés spécifiques
  1. Dans le menu principal de XClarity Administrator, cliquez sur **Administration → Sécurité**.
  2. Cliquez sur **Vue des ressources** dans le panneau de navigation de gauche. La page Vue des ressources s'affiche.

     Vous pouvez trier les colonnes du tableau afin de faciliter la recherche de dispositifs spécifiques. Vous pouvez également sélectionner un type d'appareil dans le menu déroulant **Type de ressource**, un groupe de rôles dans le menu déroulant **Groupes de rôles**, un groupe de ressources dans le menu déroulant **Groupes de ressources** et saisir du texte (un nom de ressource ou un type, par exemple) dans la zone **Filtre** pour répertorier uniquement les appareils qui répondent aux critères sélectionnés.
  3. Sélectionnez un ou plusieurs appareils pour lesquels vous souhaitez modifier l'accès.
  4. Cliquez sur l'icône **Éditer** (). La boîte de dialogue Éditer les ressources s'affiche avec les appareils sélectionnés répertoriés dans la zone **Nom de la ressource**.
  5. Affectez à **Accès public** la valeur `Yes`. Cela signifie que tous les groupes de rôles peuvent accéder aux appareils cibles quels que soient les groupes répertoriés dans la liste déroulante **Groupes de rôles**.

6. Cliquez sur **Enregistrer**.

Modification des droits par défaut

Deux paramètres permettre de déterminer si les groupes de rôles peuvent accéder à des appareils lorsqu'ils sont initialement gérés parLenovo XClarity Administrator : il s'agit des paramètres Accès public et Groupes de rôles. Le paramètre Accès public indique si tous les groupes de rôles peuvent accéder aux appareils cibles ou si seul un ensemble spécifique de ces groupes peut y accéder. Par défaut, ce paramètre est défini sur `Yes`, ce qui signifie que tous les groupes de rôles peuvent accéder aux appareils cibles. Vous pouvez modifier le comportement par défaut en définissant le paramètre Accès public sur `No`, puis en sélectionnant l'ensemble de groupes de rôles pouvant accéder aux appareils cibles.

À propos de cette tâche

Seuls les utilisateurs disposant des droits **lxc-supervisor**, **lxc-security-admin** ou **lxc-recovery** peuvent effectuer cette action.

Les utilisateurs disposant des droits **lxc-supervisor**, **lxc-security-admin** ou **lxc-recovery** peuvent accéder à tous les appareils gérés. Vous ne pouvez retirer l'accès à aucun appareil de ces groupes de rôles.

Les paramètres de contrôle d'accès par défaut permettent de définir les droits d'accès aux appareils lorsque ceux-ci sont initialement gérés par XClarity Administrator et de rétablir les droits d'accès par défaut pour un appareil spécifique. Le fait de modifier les paramètres de contrôle d'accès par défaut ne modifie pas automatiquement les droits d'accès aux appareils déjà gérés.

Procédure

Pour modifier les contrôles d'accès par défaut, procédez comme suit.

Etape 1. Dans le menu principal de XClarity Administrator, cliquez sur **Administration → Sécurité**.

Etape 2. Cliquez sur **Vue des ressources** dans le panneau de navigation de gauche. La page Vue des ressources s'affiche.

Vous pouvez trier les colonnes du tableau afin de faciliter la recherche de dispositifs spécifiques. Vous pouvez également sélectionner un type d'appareil dans le menu déroulant **Type de ressource**, un groupe de rôles dans le menu déroulant **Groupes de rôles**, un groupe de ressources dans le menu déroulant **Groupes de ressources** et saisir du texte (un nom de ressource ou un type, par exemple) dans la zone **Filtre** pour répertorier uniquement les appareils qui répondent aux critères sélectionnés.

Etape 3. Cliquez sur **Toutes les actions → Éditer les ressources par défaut**. La boîte de dialogue Éditer les ressources par défaut s'affiche.

Etape 4. Dans la liste déroulante **Groupes de rôles**, sélectionnez les groupes de rôles que vous souhaitez définir comme groupes par défaut.

Etape 5. Sélectionnez le paramètre **Accès public** par défaut.

- **Oui**. Lorsqu'un appareil est initialement géré, tous les groupes de rôles peuvent accéder à cet appareil quels que soient les groupes répertoriés dans la liste déroulante **Groupes de rôles**.
- **Non**. Lorsqu'un appareil est initialement géré, seuls les groupes de rôles répertoriés dans la liste déroulante **Groupes de rôles** peuvent accéder à cet appareil par défaut.

Etape 6. Cliquez sur **Enregistrer**.

Implémentation d'un environnement sécurisé

Il est important que vous évaluiez les exigences de sécurité dans votre environnement, que vous compreniez tous les risques liés à la sécurité, et que vous réduisiez ces risques. Lenovo XClarity Administrator inclut

plusieurs fonctions qui peuvent vous aider à sécuriser votre environnement. Utilisez les informations suivantes pour implémenter le plan de sécurité de votre environnement.

À propos de cette tâche

Important : Vous êtes responsable de l'évaluation, de la sélection et de l'implémentation des fonctions de sécurité, des procédures d'administration et des commandes appropriées pour votre environnement système. L'implémentation des fonctions de sécurité décrites dans la présente section ne sécurise pas votre environnement intégralement.

Tenez compte des informations suivantes lorsque vous évaluez les exigences de sécurité pour votre environnement :

- La sécurité physique de votre environnement est importante. Limitez l'accès aux salles et aux armoires dans lesquelles se trouve le matériel de gestion des systèmes.
- Utilisez un pare-feu basé sur un logiciel pour protéger votre matériel réseau et vos données des menaces à la sécurité connues et émergentes telles que des virus et des accès non autorisés.
- Ne modifiez pas les paramètres de sécurité par défaut des commutateurs réseau et des modules passe-système. Les paramètres par défaut définis à l'usine pour ces composants désactivent l'utilisation de protocoles non sécurisés et activent l'obligation de mises à jour du microprogramme signées.
- Les applications de gestion des modules CMM, contrôleurs de gestion de la carte mère, FSP et des commutateurs autorisent uniquement les modules de mise à jour du microprogramme signés pour ces composants afin de garantir que seul le microprogramme sécurisé est installé.
- Seuls les utilisateurs autorisés à mettre à jour des composants du microprogramme doivent avoir des droits de mise à jour du microprogramme.
- Vérifiez au moins que les mises à jour du microprogramme critiques sont installées. Après avoir apporté des modifications, sauvegardez toujours la configuration.
- Assurez-vous que toutes les mises à jour relatives à la sécurité des serveurs DNS sont installées rapidement et maintenues à jour.
- Informez vos utilisateurs de ne pas accepter de certificats non sécurisés. Pour plus d'informations, voir Utilisation de certificats de sécurité.
- Des options anti-fraude sont disponibles pour le matériel Flex System. Si le matériel est installé dans une armoire non verrouillée ou située dans une zone ouverte, installez les options anti-fraude pour dissuader et identifier les intrusions. Pour plus d'informations sur les options anti-fraude, consultez la documentation livrée avec vos produits Flex System.
- Lorsque cela est possible et réalisable, placez le matériel de gestion des systèmes sur un sous-réseau distinct. Généralement, seuls les administrateurs doivent avoir accès au matériel de gestion des systèmes ; aucun utilisateur de base ne doit y avoir accès.
- Lorsque vous choisissez des mots de passe, n'utilisez pas d'expressions faciles à deviner du type « mot de passe » ou le nom de votre entreprise. Conservez les mots de passe dans un endroit sécurisé et assurez-vous que leur accès est restreint. Mettez en place une politique de mot de passe pour votre entreprise.

  Important : Changez toujours le nom d'utilisateur et le mot de passe par défaut. Des règles de mot de passe strictes doivent être obligatoires pour tous les utilisateurs.
- Instaurez des mots de passe à la mise sous tension pour les utilisateurs afin de contrôler l'accès aux données et aux programmes de configuration sur les serveurs. Pour plus d'informations sur les mots de passe à la mise sous tension, consultez la documentation livrée avec vos serveurs.
- Utilisez les divers niveaux d'autorisation disponibles pour les différents utilisateurs de votre environnement. N'autorisez pas tous les utilisateurs à travailler avec le même ID utilisateur de superviseur.

- Vérifiez que votre environnement répond aux critères suivants de la norme NIST 800-131A pour la prise en charge des communications sécurisées :
  - Utilisation de SSL (Secure Sockets Layer) avec le protocole TLS v1.2.
  - Utilisation de SHA-256 ou de fonctions de hachage plus fortes pour les signatures numériques et de SHA-1 ou de fonctions de hachage plus fortes pour les autres applications.
  - Utilisation de RSA-2048 ou niveau supérieur ou de courbes elliptiques conformes à NIST de 224 bits ou plus.
  - Utilisation d'un chiffrement symétrique conforme à NIST avec des clés d'au moins 128 bits de longueur.
  - Utilisation de générateurs de nombres aléatoires conformes à NIST.
  - Lorsque cela est possible, prise en charge de mécanismes d'échange de clés Diffie-Hellman ou Elliptic Curve Diffie-Hellman.

  Pour plus d'informations sur les paramètres de cryptographie, voir Configuration des paramètres cryptographiques sur le serveur de gestion. Pour plus d'informations sur les paramètres NIST, voir Implémentation de la conformité avec la norme NIST SP 800-131A.

Modification des paramètres de sécurité d'un compte utilisateur

Les paramètres de sécurité d'un compte utilisateur contrôlent la complexité du mot de passe, le verrouillage du compte, ainsi que le délai d'attente d'inactivité de session Web. Vous pouvez modifier les valeurs des paramètres.

Procédure

Procédez comme suit pour remplacer les paramètres de sécurité de compte utilisateur en vigueur.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Sécurité**.

Etape 2. Cliquez sur **Paramètres de sécurité de compte** sous la section Utilisateurs et groupes pour afficher la page Gestion des utilisateurs.

Etape 3. Pour chacun des paramètres ci-dessous à modifier, sélectionnez la nouvelle valeur.

Tableau 1. Paramètres de sécurité de compte

Paramètre de sécurité	Description	Valeurs autorisées	Valeurs par défaut
Période d'expiration du mot de passe	Durée, en jours, pendant laquelle un utilisateur peut utiliser un mot de passe avant que sa modification ne soit requise. Plus la période est courte et moins les pirates informatiques auront l'occasion de deviner les mots de passe Si ce paramètre est défini sur **0**, cela signifie que les mots de passe n'expirent jamais. **Remarque :** Ce paramètre s'applique uniquement lorsque les comptes utilisateur sont gérés à l'aide du serveur d'authentification local. Il ne s'applique pas lorsque le serveur d'authentification externe est utilisé.	**0 – 365**	**90**
Période d'avertissement d'expiration du mot de passe	Période, en jours, précédant la date d'expiration du mot de passe, au cours de laquelle les utilisateurs commencent à recevoir des avertissements concernant l'expiration imminente du mot de passe utilisateur Si ce paramètre est défini sur **0**, les utilisateurs ne reçoivent pas d'avertissement. **Remarque :** Ce paramètre s'applique uniquement lorsque les comptes utilisateur sont gérés à l'aide du serveur d'authentification local. Il ne s'applique pas lorsque le serveur d'authentification externe est utilisé.	**0 –** *Paramètre d'expiration du mot de passe maximal*	**5**
Cycle de réutilisation du mot de passe minimum	Nombre minimal de fois qu'un utilisateur doit entrer un mot de passe unique lorsqu'il change de mot de passe, avant que l'utilisateur puisse réutiliser un mot de passe déjà utilisé Si ce paramètre est défini sur **0**, les utilisateurs peuvent réutiliser des mots de passe immédiatement.	**0 – 10**	**5**
Intervalle minimal de modification de mot de passe	Période minimale, en heures, qui doit s'écouler avant qu'un utilisateur puisse modifier à nouveau un mot de passe après l'avoir modifié une fois. La valeur spécifiée pour ce paramètre ne peut pas dépasser la valeur définie pour la période d'expiration du mot de passe. Si ce paramètre est défini sur **0**, les utilisateurs peuvent modifier des mots de passe immédiatement.	**0 – 1440**	**24**
Nombre maximal d'échecs de connexion	Nombre maximal de fois qu'un utilisateur peut tenter de se connecter avec un mot de passe incorrect avant que le compte utilisateur ne soit verrouillé. Le nombre défini par la période de verrouillage après le nombre maximal d'échecs de connexion détermine la période pendant laquelle un compte utilisateur est bloqué. Les comptes bloqués ne peuvent pas être utilisés pour accéder au système même si un mot de passe valide est fourni. Si ce paramètre est défini sur **0**, les comptes ne sont jamais bloqués. Le compteur de nombre d'échecs de connexion est remis à zéro après une connexion réussie.	**0 – 100**	**20**

Tableau 1. Paramètres de sécurité de compte (suite)

Paramètre de sécurité	Description	Valeurs autori-sées	Valeurs par défaut
Période de verrouillage après le nombre maximal d'échecs de connexion	Période minimale, en minutes, qui doit s'écouler avant qu'un utilisateur dont l'accès à un compte est bloqué, puisse tenter de se reconnecter Si ce paramètre est défini sur **0**, le compte reste bloqué jusqu'à ce qu'un administrateur le débloque explicitement. Si ce paramètre a pour valeur 0, votre système sera plus exposé aux attaques de déni de service sérieuses, dans lesquelles des échecs de connexion délibérés peuvent bloquer de façon permanente les comptes. **Astuce :** Tout utilisateur possédant le rôle Superviseur peut déverrouiller un compte utilisateur. Pour plus d'informations, voir Déverrouillage d'un utilisateur. **Remarque :** Ce paramètre s'applique uniquement lorsque les comptes utilisateur sont gérés à l'aide du serveur d'authentification local. Il ne s'applique pas lorsque le serveur d'authentification externe est utilisé.	**0 – 2880**	**60**
Délai d'attente d'inactivité de session Web	Période, en minutes, pendant laquelle une session utilisateur établie avec XClarity Administrator peut rester inactive avant que l'utilisateur ne soit déconnecté Si ce paramètre est défini sur **0**, la session Web n'expire jamais. **Remarque :** Lors de la modification de cette valeur, seules les sessions utilisateur commençant après la modification du paramètre sont affectées.	**0 – 1440**	**1440**
Longueur de mot de passe minimum	Nombre minimum de caractères pouvant être utilisés dans un mot de passe valide	**8 – 20**	**8**

Tableau 1. Paramètres de sécurité de compte (suite)

Paramètre de sécurité	Description	Valeurs autori-sées	Valeurs par défaut
Nombre de règles de complexité à suivre lors de la création d'un nouveau mot de passe	Nombre de règles de complexité à suivre lors de la création d'un nouveau mot de passe Les règles sont appliquées à partir de la règle 1, et jusqu'au nombre de règles spécifié. Par exemple, si la complexité du mot de passe est définie sur 4, les règles 1, 2, 3 et 4 doivent être suivies. Si la complexité du mot de passe est définie sur 2, les règles 1 et 2 doivent être suivies. XClarity Administrator prend en charge les règles de complexité de mot de passe suivantes. • (1) Doit contenir au moins un caractère alphabétique et ne peut pas avoir plus de deux caractères séquentiels, notamment des séquences de caractères alphabétiques, des chiffres et des touches de clavier QWERTY (par exemple, les séquences « abc », « 123 » et « asd » ne sont pas autorisées). • (2) Doit contenir au moins un nombre (0 à 9). • (3) Doit contenir au moins *deux* des caractères suivants : – Des caractères alphabétiques en majuscule (A – Z) – Des caractères alphabétiques en minuscule (a – z) – Des caractères spéciaux ; @ _ ! ' $ & + • (4) Ne doit pas répéter ou inverser le nom d'utilisateur. • (5) Ne doit pas contenir plus de deux caractères consécutifs (par exemple, les séquences « aaa », « 111 » et « ... » ne sont pas autorisées). Si ce paramètre est défini sur **0**, les mots de passe ne sont pas tenus de respecter les règles de complexité.	**0 – 5**	**4**
Nombre maximum de sessions actives pour un utilisateur spécifique	Nombre maximal de sessions actives pour un utilisateur spécifique qui est autorisé à un moment donné Si ce paramètre est défini sur **0**, le nombre de sessions actives autorisées pour un utilisateur spécifique est illimité.	**1 – 20**	**3**
Forcer l'utilisateur à changer de mot de passe lors du premier accès	Indique si un utilisateur doit modifier son mot de passe lors sa connexion à XClarity Administrator pour la première fois	**Oui** ou **Non**	**Oui**

Etape 4. Cliquez sur **Appliquer**.

Après avoir terminé

Une fois enregistrés, les nouveaux paramètres prennent effet immédiatement. Si vous modifiez le paramètre relatif au délai d'inactivité de session Web, les sessions actives sont affectées.

Si vous modifiez des stratégies de mot de passe, ces stratégies sont appliquées de force la prochaine fois qu'un utilisateur se connecte ou modifie son mot de passe.

Configuration des paramètres cryptographiques sur le serveur de gestion

Vous pouvez configurer la version et le paramètre de chiffrement SSL/TLS pour le serveur de gestion.

Avant de commencer

Consultez les remarques sur le chiffrement avant de modifier les paramètres sur le serveur de gestion (voir Gestion cryptographique dans la documentation en ligne de XClarity Administrator).

À propos de cette tâche

Le *mode cryptographique* détermine la façon dont les communications sécurisées sont gérées entre XClarity Administrator et tous les systèmes gérés. Si des communications sécurisées sont exécutées, elles définissent les longueurs de clé de chiffrement à utiliser.

Remarque : Quel que soit le mode cryptographique sélectionné, les générateurs de bits aléatoires numériques approuvés par le NIST sont toujours utilisés, et seules les clés de 128 bits au minimum sont utilisées pour le chiffrement symétrique.

Pour modifier le paramètre de sécurité des appareils gérés, voir Configuration des paramètres de sécurité pour un serveur géré.

Procédure

Pour changer les paramètres cryptographiques sur le serveur de gestion, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Sécurité**.

Etape 2. Choisissez l'un des modes cryptographiques suivants à utiliser pour les communications sécurisées :

- **Compatibilité**. Ce mode est le mode par défaut. Il est compatible avec les anciennes versions de microprogramme, les navigateurs et les autres clients réseau qui n'implémentent pas les normes de sécurité strictes requises pour une compatibilité avec NIST SP 800-131A.
- **NIST SP 800-131A**. Ce mode est conçu pour être conforme à la norme NIST SP 800-131A. XClarity Administrator est conçu pour toujours utiliser une cryptographie renforcée en interne et, le cas échéant, pour utiliser des connexions réseau à cryptographie forte. Toutefois, dans ce mode, les connexions réseau à l'aide d'une cryptographie qui n'est pas approuvée par NIST SP 800-131A ne sont pas autorisées, ce qui inclus le rejet des certificats de la sécurité de la couche de transport (TLS) signés avec SHA-1 ou un hachage plus faible.

  Si vous sélectionnez ce mode :

  - Pour tous les ports autres que le port 8443, tous les chiffrements TLS CBC et ceux qui ne prennent pas en charge Perfect Forward Secrecy sont désactivés.
  - Les notifications d'événements peuvent ne pas être correctement envoyées à certaines souscriptions d'appareil mobile (voir Acheminement des événements vers des appareils mobiles). Certains services externes, tels qu'Android et iOS, présentent des certificats signés avec SHA-1, qui est un algorithme non conforme aux exigences plus strictes du mode

NIST SP 800-131A. Par conséquent, toutes les connexions à ces services peuvent échouer avec une exception de certificat ou un échec d'établissement d'une liaison.

Pour plus d'informations sur la conformité à NIST SP 800-131A, voir Implémentation de la conformité avec la norme NIST SP 800-131A.

Etape 3. Choisissez la version du protocole TLS minimale à utiliser pour les connexions client à d'autres serveurs (par exemple le serveur LDAP). Vous pouvez choisir l'option suivante.

- **TLS1.2**. Applique les protocoles cryptographique TLS v1.2.
- **TLS1.3**. Applique les protocoles cryptographique TLS v1.3.

Etape 4. Choisissez la version du protocole TLS minimale à utiliser pour les connexions serveur (par exemple le serveur Web). Vous pouvez choisir l'option suivante.

- **TLS1.2**. Applique les protocoles cryptographique TLS v1.2.
- **TLS1.3**. Applique les protocoles cryptographique TLS v1.3.

Etape 5. Choisissez la version de protocole TLS minimale à utiliser pour le déploiement du système d'exploitation et les mises à jour de pilote de périphérique SE XClarity Administrator. Vous pouvez choisir l'option suivante.

- **TLS1.2**. Applique les protocoles cryptographique TLS v1.2.
- **TLS1.3**. Applique les protocoles cryptographique TLS v1.3.

Remarque : Seuls les systèmes d'exploitation dont le processus d'installation prend en charge l'algorithme de chiffrement sélectionné ou un algorithme fort peuvent être déployés et mis à jour via XClarity Administrator.

Etape 6. Sélectionnez la longueur de la clé de chiffrement et l'algorithme de hachage à utiliser pour toutes les parties du certificat, y compris le certificat de l'autorité de certification racine, le certificat du serveur et la demande CSR pour les certificats à signature externe.

- **RSA 2048 bits / SHA-256** (par défaut)

  Ce mode peut être utilisé lorsque les appareils gérés sont en mode Compatibilité, NIST SP 800-131A ou Sécurité standard. Ce mode *ne peut pas* être utilisé lorsqu'un ou plusieurs appareils gérés sont en mode **Sécurité Entreprise Strict**.

- **RSA 3072 bits / SHA-384**

  Ce mode est requis lorsque les appareils gérés sont en mode **Sécurité Entreprise Strict**.

  Important : Seuls les serveurs équipés de XCC2 prennent en charge les signatures de certificat RSA-3072/SHA-384. Après avoir configuré XClarity Administrator avec un certificat basé sur RSA-3072/SHA-384, la gestion des appareils non XCC2 prend fin. Pour gérer les appareils non XCC2, vous avez besoin d'une instance distincte de XClarity Administrator.

Etape 7. Cliquez sur **Appliquer**.

Etape 8. Redémarrez XClarity Administrator (voir Redémarrage de XClarity Administrator).

Etape 9. Si vous avez modifié la longueur de clé de chiffrement, regénérez le certificat racine de l'autorité de certification en utilisant la clé de la bonne longueur et l'algorithme de hachage approprié (voir Régénération ou restauration du certificat de serveur auto-signé Lenovo XClarity Administrator ou Déploiement de certificats de serveur personnalisé sur Lenovo XClarity Administrator).

Après avoir terminé

Si vous recevez une alerte indiquant que le certificat du serveur n'est pas sécurisé pour un appareil géré, consultez Résolution d'un certificat du serveur non sécurisé.

Configuration des paramètres de sécurité pour un serveur géré

Vous pouvez configurer la version et le paramètre de chiffrement SSL/TLS pour les serveurs gérés.

À propos de cette tâche

Tenez compte des impacts suivants de la modification du mode cryptographique.

- La permutation du mode **Mode de sécurité compatibilité** ou du mode **Sécurité standard** ou au mode **Sécurité Entreprise Strict** n'est pas pris en charge.
- Si vous effectuez une mise à niveau du mode **Mode de sécurité compatibilité** au mode **Sécurité standard**, vous recevez un avertissement si les certificats ou les clés publiques SSH importés ne sont pas conformes, mais vous pouvez tout de même passer au mode **Sécurité standard**.
- Si vous rétrogradez du mode **Sécurité Entreprise Strict** au mode **Mode de sécurité compatibilité** ou au mode **Sécurité standard** :
  - Le serveur est automatiquement redémarré pour que le mode de sécurité prenne effet.
  - Si la clé FoD du mode strict est manquante ou expirée sur XCC2, et si XCC2 utilise un certificat TLS autosigné, XCC2 regénère le certificat TLS autosigné à partir de l'algorithme de conformité Strict standard. XClarity Administrator affiche un échec de connexion en raison d'une erreur de certificat. Pour résoudre l'erreur de certificat non sécurisé, voir Résolution d'un certificat du serveur non sécurisé dans la documentation en ligne de XClarity Administrator. Si XCC2 utilise un certificat TLS personnalisé, XCC2 autorise la rétrogradation et vous avertir que vous devez importer un certificat de serveur basé sur la cryptographie du mode **Sécurité standard**.
- Le mode **NIST SP 800-131A** n'est pas pris en charge pour les serveurs équipés de XCC2.
- Si le mode cryptographique pour XClarity Administrator est défini sur TLS v1.2, et si un serveur géré utilisant l'authentification gérée est en mode de sécurité TLS v1.2, le fait de faire passer le mode de sécurité du serveur au mode TLS v1.3 à l'aide de XClarity Administrator ou de XCC aura pour effet la mise hors connexion permanente du serveur.
- Si le mode cryptographique de XClarity Administrator est défini sur TLS v1.2 et que vous tentez de gérer un serveur équipé de XCC dont le mode de sécurité est TLS v1.3, le serveur ne peut pas être géré à l'aide de l'authentification gérée.

Vous pouvez modifier les paramètres de sécurité pour les appareils suivants.
- Serveurs Lenovo ThinkSystem avec processeurs Intel ou AMD (à l'exception de SR635 / SR655)
- Serveurs Lenovo ThinkSystem V2
- Serveurs Lenovo ThinkSystem V3 avec processeurs Intel ou AMD
- Serveurs Lenovo ThinkEdge SE350 / SE450
- Serveurs Lenovo System x

Procédure

Pour modifier les paramètres de sécurité pour certains serveurs gérés, procédez comme suit.

Etape 1. Dans le menu XClarity Administrator, cliquez sur **Matériel → Serveurs**. La page Serveurs qui s'affiche présente une vue tabulaire de tous les serveurs gérés.

Etape 2. Sélectionnez un ou plusieurs serveurs.

Etape 3. Configurez le mode de sécurité.

1. Cliquez sur **Toutes les actions → Sécurité → Définir le mode de sécurité système** pour afficher la boîte de dialogue Définir le mode de sécurité système.

   La boîte de dialogue répertorie le nombre de serveurs qui peuvent être définis sur chaque mode. Passez le curseur au-dessus de chaque numéro pour afficher une fenêtre contextuelle qui présente la liste des noms de serveur applicables.

2. Sélectionnez le mode de sécurité. Les valeurs possibles sont les suivantes.

   - **Mode de sécurité compatibilité**. Sélectionnez ce mode lorsque les services et les clients nécessitent une cryptographie non compatible CNSA/FIPS. Ce mode prend en charge un grand nombre d'algorithmes de cryptographie et permet d'activer tous les services.
   - **NIST SP 800-131A**. Sélectionnez ce mode pour garantir la conformité avec la norme NIST SP 800-131A. Cela comprend la restriction des clés RSA à 2 048 octets ou plus, la restriction des hachages utilisés pour les signatures numériques à SHA-256 ou plus et l'assurance que seul les algorithme de chiffrement symétrique conformes à la norme NIST sont utilisés. Ce mode requiert de définir le mode SSL/TLS sur **Serveur et client TLS 1.2**.

     Ce mode *n'est pas* pris en charge pour les serveurs XCC2.
   - **Sécurité standard**. (Serveurs avec XCC2 uniquement) Il s'agit du mode de sécurité par défaut pour les serveurs avec XCC2. Sélectionnez ce mode pour garantir la conformité avec la norme FIPS 140-3. Pour que XCC fonctionne en mode validé FIPS 140-3, seuls les services qui prennent en charge la cryptographie de niveau FIPS 140-3 peuvent être activés. Les services qui ne prennent pas en charge la cryptographie de niveau FIPS 140-2/140-3 sont désactivés par défaut mais peuvent être activés si nécessaire. Si un service utilisant une cryptographie de niveau autre que FIPS 140-3 est activé, le XCC ne peut pas fonctionner en mode validé FIPS 140-3. Ce mode requiert des certificats de niveau FIP.
   - **Sécurité Entreprise Strict**. (serveurs avec XCC2 uniquement) Il s'agit du mode le plus sécurisé. Sélectionnez ce mode pour garantir la conformité avec la norme CNSA. Seuls les services qui prennent en charge la cryptographie de niveau CNSA sont autorisés. Les services non sécurisés sont désactivés par défaut et ne peuvent pas être activés. Ce mode requiert des certificats de niveau CNSA.

     XClarity Administrator utilise des signatures de certificat RSA-3072/SHA-384 pour les serveurs en mode **Sécurité Entreprise Strict**.

     Important :

     – La clé XCC2 Feature On Demand doit être installée sur chaque serveurs avec XCC2 sélectionné pour utiliser ce mode.

     – Dans ce mode, si XClarity Administrator utilise un certificat autosigné, XClarity Administrator doit utiliser le certificat racine et le certificat de serveur basés sur la norme RSA3072/SHA384. Si XClarity Administrator utilise un certificat à signature externe, XClarity Administrator doit générer une demande CSR basée sur RSA3072/SHA384 et contacter l'autorité de certification externe pour signer un nouveau certificat de serveur basé sur RSA3072/SHA384.

     – Lorsque XClarity Administrator utilise un certificat basé sur RSA3072/SHA384, XClarity Administrator est susceptible de déconnecter des appareils autres que les serveurs et le châssis Flex System (CMMS), les serveurs ThinkSystem, les serveurs ThinkServer, les serveurs System x M4 et M5, les commutateurs Lenovo ThinkSystem série DB, les commutateurs Lenovo RackSwitch, les commutateurs Flex System, les commutateurs Mellanox, les dispositifs de stockage ThinkSystem DE/DM, le stockage de la bandothèque IBM et les serveurs ThinkSystem SR635/SR655 sur lesquels est copié un microprogramme antérieur à 22C. Pour continuer à gérer les appareils déconnectés, configurez une nouvelle instance de XClarity Administrator avec un certificat basé sur RSA2048/SHA384.

3. Cliquez sur **Appliquer**.

Etape 4. Configurez la version TLS minimale.

1. Cliquez sur **Toutes les actions → Sécurité → Définir la version TLS du système** pour afficher la boîte de dialogue Définir la version TLS du système.

2. Sélectionnez la version du protocole TLS minimale à utiliser pour les connexions client à d'autres serveurs (telles que les connexions du client LDAP à un serveur LDAP). La valeur est configurée sur les appareils sélectionnés qui prennent en charge ce paramètre. Vous pouvez choisir l'option suivante.
   - **TLS1.2**. Applique les protocoles cryptographique TLS v1.2.
   - **TLS1.3**. Applique les protocoles cryptographique TLS v1.3.

   Remarque : Les appareils System x et CMM ne prennent en charge que la version TLS v1.2.
3. Cliquez sur **Appliquer**.

Utilisation de certificats de sécurité

Lenovo XClarity Administrator utilise des certificats SSL pour établir des communications sécurisées et approuvées entre XClarity Administrator et ses appareils gérés (tels que des châssis et des processeurs de maintenance sur les serveurs System x), ainsi que des communications avec XClarity Administrator par les utilisateurs ou avec différents services. Par défaut, XClarity Administrator, les modules CMM et les contrôleurs de gestion de la carte mère utilisent des certificats générés par XClarity Administrator qui sont autosignés et émis par une autorité de certification interne.

Avant de commencer

Cette section s'adresse aux administrateurs qui ont une compréhension de base du SSL standard et des certificats SSL, y compris ce qu'ils sont et comment les gérer. Pour plus d'informations sur les certificats de clé publique, voir Page Web X.509 dans Wikipedia et Page Web Certificat d'infrastructure de clé publique Internet X.509 et profil de liste de révocation de certificat (CRL) (RFC5280).

À propos de cette tâche

Le certificat du serveur auto-signé par défaut, qui est généré de manière unique dans chaque instance de XClarity Administrator, fournit une sécurité suffisante pour de nombreux environnements. Vous pouvez choisir de laisser XClarity Administrator gérer les certificats pour vous, ou vous pouvez jouer un rôle plus actif en personnalisant ou en remplaçant les certificats du serveur. XClarity Administrator inclut des options pour la personnalisation des certificats pour votre environnement. Par exemple, vous pouvez choisir de :

- Générez une nouvelle paire de clés en regénérant l'autorité de certification interne et/ou le certificat du serveur final qui utilise des valeurs spécifiques à votre organisation.
- Générez une demande de signature de certificat (CSR) qui peut être envoyée à l'autorité de certification de votre choix pour signer un certificat personnalisé qui peut être téléchargé vers XClarity Administrator en vue d'une utilisation comme certificat de serveur final pour tous ses services hébergés.
- Téléchargez le certificat serveur sur votre système local pour pouvoir importer ce certificat dans la liste de certificats sécurisés de votre navigateur Web.

XClarity Administrator fournit plusieurs services qui acceptent les connexions SSL/TLS entrantes. Lorsqu'un client, par exemple, un appareil géré ou un navigateur Web, se connecte à l'un de ces services, XClarity Administrator fournit son *certificat serveur* afin d'être identifié par le client lors des tentatives de connexion. Le client doit gérer une liste de certificats approuvés. Si le certificat du serveur XClarity Administrator n'est pas inclus dans la liste du client, ce dernier se déconnecte de XClarity Administrator afin d'éviter d'échanger toutes les informations de sécurité sensibles avec une source non sécurisée.

XClarity Administrator fait office de client lors de la communication avec des appareils gérés et des services externes. Lorsque XClarity Administrator se connecte à un appareil ou service externe, l'appareil ou le service externe fournit son certificat de serveur pour être identifié par XClarity Administrator. XClarity Administrator gère une liste des certificats approuvés et fiables. Si le *certificat sécurisé* fourni par l'appareil géré ou le service externe n'est pas répertorié, XClarity Administrator se déconnecte de l'appareil géré ou du

service externe pour éviter d'échanger toutes les informations de sécurité sensibles avec une source non sécurisée.

La catégorie de certificats suivante est utilisée par les services XClarity Administrator et doit être fiable pour tout client qui se connecte à lui.

- **Certificat de serveur**. Lors de l'amorçage initiale, une clé unique et un certificat auto-signé sont générés. Ils sont utilisés en tant qu'autorité de certification racine par défaut, qui peut être gérée sur la page de l'autorité de certification dans les paramètres de sécurité de XClarity Administrator. Il n'est pas nécessaire de regénérer ce certificat racine, sauf si la clé a été compromise ou si votre organisation dispose d'une règle indiquant que tous les certificats doivent être remplacés régulièrement (voir Régénération ou restauration du certificat de serveur auto-signé Lenovo XClarity Administrator).

  De même, lors de la configuration initiale, une clé distincte est générée et un certificat de serveur est créé, et signé par l'autorité de certification interne. Ce certificat est utilisé en tant que certificat de serveur XClarity Administrator par défaut. Il se regénère automatiquement à chaque fois que XClarity Administrator détecte que ses adresses de mise en réseau (adresses IP ou DNS) ont changé pour garantir que le certificat contient les adresses exactes pour le serveur. Il peut être personnalisé et généré à la demande (voir Régénération ou restauration du certificat de serveur auto-signé Lenovo XClarity Administrator).

  Vous pouvez choisir d'utiliser un certificat de serveur à signature externe au lieu du certificat de serveur auto-signé par défaut en générant une demande de signature de certificat (CSR), en faisant signer la CSR par une autorité de certification racine de certificat privée ou commerciale, puis en important l'intégralité de la chaîne de certificats dans XClarity Administrator (voir Déploiement de certificats de serveur personnalisé sur Lenovo XClarity Administrator).

  Si vous décidez d'utiliser le certificat de serveur auto-signé par défaut, il est recommandé d'importer le certificat de serveur dans votre navigateur Web en tant qu'autorité racine sécurisée afin d'éviter les messages d'erreur de certificat dans votre navigateur (voir Importation du certificat de l'autorité de certification dans un navigateur Web).
- **Certificat de déploiement de SE**. Un certificat séparé est utilisé par le service de déploiement du système d'exploitation pour garantir que le programme d'installation du système d'exploitation peut se connecter de manière sécurisée au service de déploiement lors du processus d'installation du système d'exploitation. Si la clé a été compromise, vous pouvez la regénérer en redémarrant le serveur de gestion.

La catégorie suivante (fichiers de clés certifiées) de certificats est utilisée par les clients XClarity Administrator.

- **Certificats sécurisés**.

  Ce fichier de clés certifiées gère des certificats qui sont utilisés pour établir une connexion sécurisée aux ressources locales lorsque XClarity Administrator fait office de client. Les exemples de ressources locales sont des appareils gérés, des logiciels locaux lors d'un événement de réacheminement et un serveur LDAP externe.
- **Certificats pour services externes**. Ce fichier de clés certifiées gère des certificats qui sont utilisés pour établir une connexion sécurisée avec des ressources externes lorsque XClarity Administrator fait office de client. Exemples de services externes : les services du support Lenovo en ligne utilisés pour récupérer les informations de garantie ou créer des tickets de maintenance, des logiciels externes (comme Splunk) auxquels les événements peuvent être acheminés, ainsi que les serveurs de notification push Apple et Google si les notifications push Lenovo XClarity Mobile sont activées sur un appareil iOS ou Android. Il contient des certificats sécurisés et préconfigurés, issus des autorités de certification racine de certains fournisseurs d'autorité de certificats fiables et reconnus dans le monde entier, comme Digicert et Globalsign).

Lorsque vous configurez XClarity Administrator afin d'utiliser une fonction qui nécessite une connexion à un autre service externe, reportez-vous aux documents afin de déterminer si vous devez ajouter manuellement un certificat à ce fichier de clés certifiées.

Veuillez noter que les certificats dans ce fichier de clés certifiées ne sont pas sécurisés lors de l'établissement de connexions pour d'autres services (comme LDAP), sauf si vous les ajoutez également au principal fichier de clés certifiées de certificats sécurisés. Le fait de retirer des certificats de ce fichier de clés certifiées empêche le bon fonctionnement de ces services.

XClarity Administrator prend en charge les signatures de certificat RSA-3072/SHA-384, RSA-2048/SHA-256 et ECDSA p256/SHA-256. D'autres algorithmes tels que SHA-1 de niveau supérieur ou des hachages SHA peuvent être pris en charge selon votre configuration. Tenez compte du mode cryptographique sélectionné dans XClarity Administrator (voir Configuration des paramètres cryptographiques sur le serveur de gestion), des paramètres de sécurité sélectionnés pour les serveurs gérés (Configuration des paramètres de sécurité pour un serveur géré) et des fonctionnalités des autres logiciels et dispositifs de votre environnement. Les certificats ECDSA qui sont basés sur certaines courbes elliptiques (y compris p256), mais pas sur toutes les courbes elliptiques, sont pris en charge sur la page Certificats sécurisés et dans la chaîne de signature du certificat XClarity Administrator mais *ne sont pas* actuellement prise en charge pour une utilisation par le certificat du serveur XClarity Administrator.

Remarque : XClarity Administrator utilise les signatures de certificat RSA- 3072/SHA-384 pour les serveurs avec XCC2 en mode Strict.

Installation d'un certificat de serveur personnalisé à signature externe

Vous pouvez choisir d'utiliser un certificat de serveur qui a été signé par une autorité de certification privée ou commerciale (CA).

Avant de commencer

Assurez-vous que l'autorité de certification racine est celle générée par votre organisation et utilisée pour signer des certificats dans cette organisation, ou une autorité fiable et reconnue dans le monde entier (voir Page Web Liste des autorités de certifications fiables).

Assurez-vous que les algorithmes des clés et des signatures de la certification de l'autorité de certification racine sont pris en charge. Seules les signatures RSA-3072/SHA-384 et RSA-2048/SHA-256 sont prises en charge. Les signatures RSA-PSS ne sont pas prises en charge à ce stade.

Vérifiez que la dernière version du microprogramme est installée sur tous les appareils gérés avant de démarrer une tâche qui peut avoir un impact sur les connexions entre les appareils gérés. Pour mettre à niveau le microprogramme sur les appareils gérés, voir Mise à jour du microprogramme sur les appareils gérés.

Vérifiez que XClarity Administrator communique correctement avec tous les appareils gérés en cliquant sur **Matériel**, puis en cliquant sur le type d'appareils (châssis ou serveur). Une page s'affiche avec une vue tabulaire de tous les appareils gérés de ce type. Si un dispositif possède un état « Hors ligne, » assurez-vous que la connectivité réseau est opérationnelle entre le serveur de gestion et le dispositif, et résolvez les certificats de serveur non sécurisés si besoin (voir Résolution d'un certificat du serveur non sécurisé).

À propos de cette tâche

Lorsque vous installez un certificat de serveur à signature externe et personnalisé dans XClarity Administrator ou un contrôleur de gestion de la carte mère ou CMM, vous devez fournir le groupe de certificats qui contient l'intégralité de la chaîne de signature de l'autorité de certification.

Lorsque vous installez un certificat de serveur personnalisé dans un châssis ou un serveur qui n'est pas géré par XClarity Administrator, installez le groupe de certificats sur le module CMM avant de l'installer sur les contrôleurs de gestion du module CMM.

Lorsque vous installez un certificat de serveur personnalisé sur un châssis géré, vous devez d'abord ajouter la chaîne de signature CA au fichier de clés certifiées XClarity Administrator, installer le certificat de serveur sur chaque contrôleur de gestion et module CMM, puis télécharger le certificat du serveur sur XClarity Administrator. Notez bien que cela peut être aisément contourné en ajoutant/autorisant tous les certificats de l'autorité de certification racine, mais pas toutes les chaînes de certificats de chaque appareil géré. Le nombre de certificats importés doit être égal au nombre de certificats de l'autorité de certification racine (certificats de l'autorité de certification racine + tous les certificats de l'autorité de certification intermédiaires). Pour plus d'informations, voir Déploiement de certificats de serveur personnalisé sur des appareils gérés.

Vous devez ajouter le certificat racine CA et tous les certificats intermédiaires, un par un, dans le fichier de clés certifiées XClarity Administrator. L'ordre n'importe pas. Chaque certificat doit être installé une fois, de sorte que si tous les dispositifs utilisent les mêmes certificats de CA et intermédiaires, la CA et chaque certificat intermédiaire doivent être installés une fois dans le fichier de clés certifiées XClarity Administrator. Si plusieurs autorités de certification ou une autorité de certification intermédiaire est utilisée, vérifiez que chaque certificat racine CA unique ou certificat intermédiaire utilisé dans la chaîne de signature d'un dispositif géré est importé suivant ces étapes.

Conseil : si le nouveau certificat de serveur n'est pas signé par un tiers de confiance, la prochaine fois que vous vous connecterez à XClarity Administrator, votre navigateur affichera un message de sécurité et une boîte de dialogue vous invitant à accepter le nouveau certificat dans le navigateur. Pour éviter les messages de sécurité, vous pouvez importer un certificat de serveur téléchargé dans la liste de votre navigateur Web de certificats sécurisés. Pour plus d'informations sur l'importation des certificats de serveur, voir Importation du certificat de l'autorité de certification dans un navigateur Web.

Déploiement de certificats de serveur personnalisé sur Lenovo XClarity Administrator

Vous pouvez choisir de générer une demande de signature de certificat (CSR) à signer par l'autorité de certification de votre organisation ou une autorité de certification tierce. La CSR crée une chaîne de certificats complète que vous pouvez importer et utiliser à la place des certificats uniques signés en interne par défaut.

Avant de commencer

Assurez-vous que les détails du certificat incluent les exigences suivantes.

- L'utilisation clé doit contenir
  - Accord clé
  - Signature numérique
  - Chiffrage clé
- Utilisation clé étendu doit contenir
  - Authentification serveur (1.3.6.1.5.5.7.3.1)
  - Authentification client (1.3.6.1.5.5.7.3.2)

À propos de cette tâche

Attention : Si NIST SP 800-131A est activé (voir Implémentation de la conformité avec la norme NIST SP 800-131A) et si vous utilisez ou souhaitez utiliser des certificats à signature externe ou personnalisés dans un NIST, tous les certificats présents dans la chaîne doivent être basés sur les fonctions de hachage SHA-256.

Lorsque le certificat du serveur est téléchargé, XClarity Administrator tente de distribuer le nouveau certificat de l'autorité de certification sur tous les appareils gérés. Si le processus de distribution aboutit, XClarity

Administrator démarre immédiatement à l'aide du nouveau certificat de serveur. Si le processus échoue, des messages d'erreur s'affichent et vous indiquent comment corriger des problèmes manuellement avant d'appliquer le certificat de serveur nouvellement importé. Une fois les erreurs corrigées, terminez l'installation du certificat précédemment téléchargé.

Remarque : Si XClarity Administrator utilisait déjà un certificat signé par la même autorité racine, l'autorité de certification ne doit pas être envoyée aux dispositifs et XClarity Administrator commence à utiliser le certificat immédiatement.

Après avoir téléchargé un certificat dans XClarity Administrator versions 1.1.0 et ultérieures, le serveur Web redémarrait et mettait fin automatiquement à toutes les sessions de navigateur. XClarity Administrator versions 1.1.1 et ultérieures démarre avec le nouveau certificat sans arrêter les sessions existantes. Toutes les nouvelles sessions sont établies avec le nouveau certificat. Pour afficher le nouveau certificat en cours d'utilisation, redémarrez votre navigateur Web.

Procédure

Pour générer et déployer un certificat de serveur personnalisé à signature externe sur Lenovo XClarity Administrator, procédez comme suit.

Etape 1. Créez et téléchargez une demande de signature de certificat (CSR) pour XClarity Administrator

a. Dans la barre de menu XClarity Administrator, cliquez sur **Administration → Sécurité** pour afficher la page Sécurité.

b. Cliquez sur **Certificat du serveur** dans la section Gestion des certificats pour afficher la page Certificat du serveur.

c. Cliquez sur l'onglet **Générer une demande de signature de certificat (CSR)**.

d. Renseignez les champs de la demande.
- Pays ou région
- État ou Province
- Ville ou localité
- Organisation
- Unité organisationnelle (facultatif)
- Nom commun

Attention : Sélectionnez un nom commun correspondant à l'adresse IP ou au nom d'hôte utilisé par XClarity Administrator pour la connexion au dispositif géré. La sélection d'une valeur incorrecte peut engendrer des connexions non sécurisées.

e. Personnalisez les autres noms de sujet (SAN) qui sont ajoutées à l'extension X.509 « subjectAltName » lorsque le fichier CSR est généré.

Par défaut, XClarity Administrator définit automatiquement les autres noms de sujet (SAN) pour la CSR basé sur l'adresse IP et le nom d'hôte qui sont reconnus par les interfaces réseau du système d'exploitation XClarity Administrator invité. Vous pouvez personnaliser, supprimer ou ajouter ces valeurs SAN.

Le nom que vous spécifiez doit être valide pour le type sélectionné :
- **directoryName** (par exemple, `cn=lxca-example,ou=dcg,dc=company,dc=com`)
- **dNSName** (par exemple, `lxca-example.dcg.company.com`)
- **ipAddress** (par exemple, `192.0.2.0`)
- **registeredID** (par exemple, `1.2.3.4.55.6.5.99`)
- **rfc822Name** (par exemple, `example@company.com`)
- **uniformResourceIdentifier** (par exemple, `https://lxca-dev.dcg.company.com/example`)

Remarque : Tous les réseaux SAN qui sont répertoriés dans le tableau sont validés, enregistrés et ajoutés au CSR uniquement après que vous générez le CSR à l'étape suivante.

f. Cliquez sur **Générer un fichier CSR**. Le certificat de serveur est affiché dans la boîte de dialogue Demande de signature de certificat.

g. Cliquez sur **Enregistrer dans un fichier** pour enregistrer le certificat du serveur sur le serveur hôte.

Etape 2. Fournissez la CSR à une autorité de certification sécurisée (CA). L'autorité de certification signe la CSR et répond par un certificat de serveur.

Etape 3. Téléchargez le certificat de serveur à signature externe sur XClarity Administrator. Le contenu du certificat doit être un ensemble contenant le certificat racine de l'autorité de certification, tous les certificats intermédiaires et le certificat du serveur.

a. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Sécurité** pour afficher la page Sécurité.

b. Cliquez sur **Certificat du serveur** dans la section Gestion des certificats.

c. Cliquez sur l'onglet **Télécharger le certificat**.

d. Cliquez sur **Télécharger le certificat** pour afficher la boîte de dialogue Télécharger le certificat.

e. Indiquez un fichier de groupe de certificats au format PEM, DER ou PKCS7, ou collez le groupe de certificats au format PEM.

f. Cliquez sur **Télécharger** pour télécharger le certificat du serveur et le stocker dans le fichier de clés certifiées XClarity Administrator.

Déploiement de certificats de serveur personnalisé sur des appareils gérés

Vous pouvez déployer des certificats de serveur personnalisés sur des appareils gérés en téléchargeant et en installant le groupe de certificats à signature externe à l'aide du module CMM et du contrôleur de gestion pour ces appareils.

Avant de commencer

Vérifiez que le dernier microprogramme est installé sur tous les appareils gérés (voir Mise à jour du microprogramme sur les appareils gérés).

Lors de la génération d'une demande de signature de certificat (CSR) pour les certificats personnalisés, veillez à sélectionner un nom commun correspondant à l'adresse IP ou au nom d'hôte utilisé pour identifier le dispositif. La sélection d'une valeur incorrecte peut engendrer des connexions non sécurisées.

Vérifiez que vous obtenez un groupe de certificats contenant toute la chaîne de signature, du certificat de serveur final au certificat racine (base) de l'autorité de certification de confiance, qui peut être utilisé pour vérifier toute la chaîne de certificats de confiance.

Ne modifiez pas le certificat du serveur Lenovo XClarity Administrator lorsqu'un dispositif géré est « Hors ligne. » Vous devez réparer la connexion avant de modifier Lenovo XClarity Administrator ; sinon, des étapes supplémentaires peuvent être requises pour réparer les problèmes de connectivité (voir Résolution d'un certificat du serveur non sécurisé).

À propos de cette tâche

Cette section fournit des recommandations pour assurer la communication réussie et continue entre Lenovo XClarity Administrator et les appareils gérés. Pour obtenir des instructions détaillées sur la manière de générer un CSR et d'importer un certificat signé, consultez la documentation de votre dispositif.

Si Lenovo XClarity Administrator gère un ou plusieurs châssis, serveurs racks et serveurs au format tour, et si les certificats signés en interne Lenovo XClarity Administrator par défaut sont actuellement installés sur Lenovo XClarity Administrator et les appareils gérés, vous pouvez déployer un certificat de serveur personnalisé.

Si le certificat de serveur à signature externe est installé sur le dispositif *avant* que vous ne tentiez de gérer le dispositif par Lenovo XClarity Administrator, aucune étape supplémentaire n'est nécessaire. Pour déployer un certificat de serveur personnalisé sur les appareils gérés sous Lenovo XClarity Administrator, vous devez effectuer l'une des étapes suivantes afin de vérifier la connectivité continue entre le serveur de gestion et les appareils gérés.

Procédure

Effectuez l'une des actions suivantes pour déployer le certificat du serveur personnalisé et à signature externe sur le châssis ou les serveurs gérés.

- Si Lenovo XClarity Administrator utilise un certificat signé par la même autorité de certification que les appareils gérés, effectuez les étapes décrites dans Déploiement de certificats de serveur personnalisé sur Lenovo XClarity Administrator *avant* d'installer les certificats sur les appareils gérés. L'installation de la chaîne de certificats Lenovo XClarity Administrator de la même autorité de certification permet de s'assurer que la chaîne de certificats se trouve dans le fichier de clés certifiées Lenovo XClarity Administrator et que Lenovo XClarity Administrator peut faire confiance aux dispositifs après l'installation des certificats externes signés.
- Ajoutez des certificats signés en externe dans les chaînes de signature de l'autorité de certification au fichier de clés certifiées Lenovo XClarity Administrator.

  Vous devez ajouter le certificat racine CA et tous les certificats intermédiaires, un par un, dans le fichier de clés certifiées Lenovo XClarity Administrator. L'ordre n'importe pas. Chaque certificat doit être installé une fois, de sorte que si tous les dispositifs utilisent les mêmes certificats de CA et intermédiaires, la CA et chaque certificat intermédiaire doivent être installés une fois dans le fichier de clés certifiées Lenovo XClarity Administrator. Si plusieurs autorités de certification ou une autorité de certification intermédiaire est utilisée, vérifiez que chaque certificat racine CA unique ou certificat intermédiaire utilisé dans la chaîne de signature d'un dispositif géré est importé suivant ces étapes.

  Remarque : N'ajoutez pas de certificats de serveur finaux et non émis par une CA lors de cette procédure.

  Procédez comme suit pour chaque certificat dans le module.

  1. Dans la barre de menu Lenovo XClarity Administrator, cliquez sur **Administration → Sécurité** pour afficher la page Sécurité.
  2. Cliquez sur **Certificats sécurisés** sous Gestion des certificats dans la navigation à gauche.
  3. Cliquez sur l'icône **Créer** ( ) pour afficher la boîte de dialogue Ajouter un certificat.
  4. Indiquez un fichier de certificat, au format PEM ou DER, ou collez le certificat au format PEM.
  5. Cliquez sur **Créer** pour créer le certificat.

  Une fois la chaîne de signature de l'autorité de certification installée, Lenovo XClarity Administrator sécurise des connexions aux serveurs CIM sur le module CMM et le contrôleur de gestion, sur lesquelles est installé le certificat du serveur à signature externe.
- Importez les certificats signés en externe dans les appareils gérés.

  Remarque : Si les certificats requis ne sont pas présents dans le fichier de clés certifiées Lenovo XClarity Administrator, la connectivité est perdue entre Lenovo XClarity Administrator et le dispositif géré. Effectuez les étapes décrites dans Résolution d'un certificat du serveur non sécurisé pour réparer la connexion.

Important : Cette option implique la perte temporaire de connectivité ; par conséquent, l'une des options précédentes est recommandée.

Régénération ou restauration du certificat de serveur auto-signé Lenovo XClarity Administrator

Vous pouvez générer une nouvelle autorité de certification ou un certificat de serveur pour remplacer les certificats auto-signés actuels ou pour rétablir un certificat généré par Lenovo XClarity Administrator si XClarity Administrator utilise actuellement un certificat de serveur à signature externe personnalisé. Le nouveau certificat de serveur auto-signé est ensuite utilisé par les serveurs d'authentification, HTTPS et CIM sur XClarity Administrator. Il est aussi automatiquement fourni à tous les appareils gérés.

Avant de commencer

Lorsque vous regénérez ou téléchargez certificatXClarity Administrator, XClarity Administrator est redémarré.

Si un nouveau certificat de CA est généré, le nouveau certificat de CA est automatiquement déployé sur le fichier de clés certifiées dans chaque module CMM et le contrôleur de gestion de la carte mère dans tous les châssis gérés, les serveurs rack et les serveurs au format tour pour maintenir des connexions de serveur d'authentification sécurisé. Si une erreur se produit lors du déploiement du certificat racine CA, téléchargez-le à partir de la page Autorité de certification et importez-le manuellement dans le fichier de clés certifiées de tous les appareils gérés sur lequel il n'a pas été correctement géré avant la génération d'un nouveau certificat de serveur.

Si vous prévoyez de regénérer le certificat de CA, prévoyez du temps pour regénérer la CA, corriger toutes les erreurs de distribution et regénérer le certificat du serveur sous un court délai.

Après avoir généré un nouveau certificat racine CA, des erreurs de communication peuvent se produire ou vous risquez de ne pas pouvoir vous connecter à un dispositif avant la régénération et la signature du certificat du serveur.

Important : Pour XClarity Administrator v1.1.1 et versions antérieures, vous devez importer le certificat racine CA dans le fichier de clés certifiées de chaque module CMM et le contrôleur de gestion. Voir la documentation du module CMM et du contrôleur de gestion pour plus d'informations sur l'importation du certificat racine CA

Procédure

Procédez comme suit pour restaurer un certificat de serveur auto-signé sur XClarity Administrator.

Remarque : Le certificat de serveur qui est en cours d'utilisation sur XClarity Administrator, qu'il soit auto-signé ou à signature externe, reste en service jusqu'à ce que le nouveau certificat de serveur soit regénéré et signé.

Etape 1. **Facultatif :** générez un nouveau certificat racine CA.

a. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Sécurité** pour afficher la page Sécurité.

b. Cliquez sur **Autorité de certification** dans la section Gestion des certificats.

c. Cliquez sur **Regénérer le certificat racine de l'autorité de certification**.

Si la clé et le certificat de CA sont correctement regénérés, une boîte de dialogue s'affiche et présente l'état des travaux pour distribuer ce certificat en tant que certificat sécurisé LDAP à tous les CMM et contrôleurs de gestion (pour les serveurs Converged, NeXtScale, et System x). Cette boîte de dialogue, ainsi que la page de surveillance de la tâche, affiche la réussite ou l'échec de chacun de ces travaux de distribution.

Si l'un des travaux de distribution échoue, procédez comme suit pour télécharger le certificat racine CA, puis importer manuellement le certificat racine en tant que certificat LDAP sécurisé dans n'importe quel dispositif pour lequel le travail a échoué.

Etape 2. **Facultatif :** téléchargez le certificat racine CA vers le système hôte et importez-le dans votre navigateur Web.

a. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Sécurité** pour afficher la page Sécurité.

b. Cliquez sur **Autorité de certification** dans la section Gestion des certificats.

c. Cliquez sur **Télécharger le certificat racine de l'autorité de certification**. Le certificat racine CA actuel s'affiche dans la boîte de dialogue Certificat racine de l'autorité de certification.

d. Cliquez sur **Enregistrer dans un fichier** pour enregistrer le certificat racine CA sur le système hôte.

e. Suivez les instructions de votre navigateur Web et du navigateur Web d'autres utilisateurs qui accéderont à XClarity Administrator pour importer le certificat en tant qu'autorité racine sécurisée.

Etape 3. Régénérez un nouveau certificat de serveur et signez le certificat avec le nouveau certificat racine CA.

a. À partir de la page Sécurité, cliquez sur **Certificat du serveur** dans la section Gestion des certificats.

b. Cliquez sur l'onglet **Regénérer le certificat du serveur**.

c. Renseignez les zones sur la page Regénérer le certificat du serveur :
- Pays ou région
- État ou Province
- Ville ou localité
- Organisation
- Unité organisationnelle
- Nom commun
- Date de début de validité.
- Heure de début de validité.
- Date de fin de validité.
- Heure de fin de validité.

d. Cliquez sur **Regénérer un certificat**.

e. Si vous régénérez des certificats autosignés sur les modules CMM gérés et les contrôleurs de gestion (pour les serveurs Converged, NeXtScale, ThinkSystem et System x), après avoir régénéré le certificat sur chaque dispositif, importez le nouveau certificat de dispositif dans le XClarity Administrator fichier de clés certifiées (voir Résolution d'un certificat du serveur non sécurisé). Sinon, vous pouvez télécharger manuellement le certificat à partir de l'appareil et l'importer dans XClarity Administrator sur la page Certificats sécurisés.

Pour XClarity Administrator v1.1.0 et versions antérieures, le serveur Web redémarre et arrête automatiquement toutes les sessions de navigateur après avoir regénéré un certificat. Pour XClarity Administrator v1.1.1 et versions ultérieures, XClarity Administrator démarre en utilisant le nouveau certificat sans arrêter les sessions existantes. De nouvelles sessions sont établies avec le nouveau certificat. Pour afficher le nouveau certificat en cours d'utilisation, redémarrez votre navigateur Web.

Etape 4. Si vous régénérez des certificats autosignés sur les modules CMM gérés et les contrôleurs de gestion (pour les serveurs Converged, NeXtScale, ThinkSystem et System x), après avoir régénéré le certificat sur chaque dispositif, importez le nouveau certificat de dispositif dans le XClarity Administrator fichier de clés certifiées (voir Résolution d'un certificat du serveur non sécurisé).

Sinon, vous pouvez télécharger manuellement le certificat à partir de l'appareil et l'importer dans XClarity Administrator sur la page Certificats sécurisés.

Résolution d'un certificat du serveur non sécurisé

Le certificat de serveur utilisé pour établir une connexion sécurisée à un dispositif géré peut être non sécurisé. Si le problème est dû à une version de niveau précédent du certificat racine CA du dispositif ou du certificat autosigné du dispositif dans le fichier de clés certifiées Lenovo XClarity Administrator, XClarity Administrator peut résoudre le certificat de serveur non sécurisé.

À propos de cette tâche

Si un dispositif géré devient non sécurisé, XClarity Administrator empêche la communication avec ce dispositif, ce qui vous empêche d'effectuer des opérations de gestion ou d'inventaire sur ce dispositif.

Procédure

Pour résoudre un certificat de serveur non sécurisé pour un dispositif géré, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel**, puis cliquez sur le type de dispositif (**Châssis**, **Serveur**, **Stockage** ou **Commutateur**). Une page s'affiche avec une vue tabulaire de tous les appareils gérés de ce type.

Etape 2. Sélectionnez un dispositif spécifique dans l'état « Hors ligne ».

Etape 3. Cliquez sur **Toutes les actions → Sécurité → Résoudre les certificats non sécurisés**.

Etape 4. Cliquez sur **Installer le certificat**.

XClarity Administrator extrait le certificat en cours de l'appareil cible. Si ce certificat est différent du certificat sécurisé de cet appareil dans le fichier de clés certifiées de XClarity Administrator, le nouveau certificat est placé dans le fichier de clés certifiées de XClarity Administrator, ce qui remplace le certificat précédent de cet appareil.

Si cela ne résout pas le problème, assurez-vous que la connectivité réseau est opérationnelle entre XClarity Administrator et l'appareil.

Téléchargement du certificat du serveur

Vous pouvez télécharger une copie du certificat du serveur en cours, au format PEM ou DER, sur votre système local. Vous pouvez ensuite importer le certificat dans votre navigateur Web ou dans d'autres applications (par exemple Lenovo XClarity Mobile ou Lenovo XClarity Integrator).

Procédure

Procédez comme suit pour télécharger le certificat du serveur.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Administration → Sécurité** pour afficher la page Sécurité.

Etape 2. Cliquez sur **Certificat du serveur** dans la section Gestion des certificats. La page Certificat du serveur s'affiche.

Etape 3. Cliquez sur l'onglet **Télécharger le certificat**.

Etape 4. Cliquez sur **Télécharger le certificat**.

Etape 5. Cliquez sur **Enregistrer sous der** ou **Enregistrer sous pem** pour enregistrer le certificat du serveur en tant que fichier DER ou PEM sur votre système local.

Importation du certificat de l'autorité de certification dans un navigateur Web

Pour éviter les messages d'avertissement de sécurité à partir de votre navigateur Web lorsque vous accédez à Lenovo XClarity Administrator, vous pouvez télécharger une copie du certificat de l'autorité de certification

(CA), au format PEM ou DER, sur votre système local, puis importer ce certificat dans la liste de certificats sécurisés de votre navigateur Web.

À propos de cette tâche

XClarity Administrator prend en charge les signatures de certificat RSA-3072/SHA-384, RSA-2048/SHA-256 et ECDSA p256/SHA-256. D'autres algorithmes tels que SHA-1 de niveau supérieur ou des hachages SHA peuvent être pris en charge selon votre configuration. Tenez compte du mode cryptographique sélectionné dans XClarity Administrator (voir Configuration des paramètres cryptographiques sur le serveur de gestion), des paramètres de sécurité sélectionnés pour les serveurs gérés (Configuration des paramètres de sécurité pour un serveur géré) et des fonctionnalités des autres logiciels et dispositifs de votre environnement. Les certificats ECDSA qui sont basés sur certaines courbes elliptiques (y compris p256), mais pas sur toutes les courbes elliptiques, sont pris en charge sur la page Certificats sécurisés et dans la chaîne de signature du certificat XClarity Administrator mais *ne sont pas* actuellement prise en charge pour une utilisation par le certificat du serveur XClarity Administrator.

Remarque : XClarity Administrator utilise les signatures de certificat RSA- 3072/SHA-384 pour les serveurs avec XCC2 en mode Strict.

Procédure

Pour télécharger le certificat du serveur, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Sécurité** pour afficher la page Sécurité.

Etape 2. Cliquez sur **Autorité de certification** dans la section Gestion des certificats. La page Autorité de certification s'affiche.

Etape 3. Cliquez sur **Télécharger le certificat racine de l'autorité de certification**.

Etape 4. Cliquez sur **Enregistrer sous der** ou **Enregistrer sous pem** pour enregistrer le certificat du serveur en tant que fichier DER ou PEM sur votre système local.

Etape 5. Importez le certificat téléchargé dans la liste des certificats d'autorité racine de confiance pour votre navigateur.

- **Firefox :**
  1. Ouvrez le navigateur, puis cliquez sur **Outils → Options → Avancé**.
  2. Cliquez sur l'onglet **Certificats**.
  3. Cliquez sur **Afficher les certificats**.
  4. Cliquez sur **Importer** et accédez à l'emplacement où le certificat a été téléchargé.
  5. Sélectionnez le certificat, puis cliquez sur **Ouvrir**.
- **Internet Explorer :**
  1. Ouvrez le navigateur, puis cliquez sur **Outils → Options Internet → Contenu**.
  2. Cliquez sur **Certificats** pour afficher la liste de tous les certificats qui sont actuellement sécurisés.
  3. Cliquez sur **Importer** pour afficher l'Assistant d'importation de certificat.
  4. Exécutez l'assistant pour importer le certificat.

Ajout et remplacement d'une liste de révocation de certificat

Une *liste de révocation de certificat est une liste des certificats qui ont été révoqués et ne sont plus sécurisés.* Un certificat peut être révoqué s'il n'a pas été correctement généré par l'autorité de certification ou si la clé est compromise, perdue ou volée.

Procédure

Procédez comme suit pour ajouter une nouvelle liste de révocation de certificat ou en remplacer une existante.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Administration → Sécurité** pour afficher la page Sécurité.

Etape 2. Cliquez sur **Listes de révocation de certificat** sous Gestion des certificats dans la navigation à gauche. La page Listes de révocation de certificat s'affiche avec une liste de toutes les listes de révocation de certificat.

Etape 3. Cliquez sur **Ajouter / Remplacer CLR** pour ajouter une liste de révocation de certificat, ou sélectionnez-en une et cliquez sur **Ajouter / Remplacer CLR** pour remplacer le CLR.

Etape 4. Indiquez un fichier de liste de révocation de certificat, au format PEM ou DER, ou collez le certificat au format PEM.

Etape 5. Cliquez sur **Créer** pour créer la liste de révocation de certificat.

Activation de l'encapsulage

Lorsque vous gérez les châssis et les serveurs Lenovo dans Lenovo XClarity Administrator, vous pouvez configurer Lenovo XClarity Administrator pour modifier les règles de pare-feu des appareils afin que les demandes entrantes soient acceptées uniquement à partir de Lenovo XClarity Administrator. Cette procédure est appelée *encapsulage*. Vous pouvez également activer ou désactiver l'encapsulage sur les châssis et les serveurs qui sont déjà gérés par Lenovo XClarity Administrator.

Lorsque l'encapsulage est activé sur un appareil qui le prend en charge, Lenovo XClarity Administrator remplace la valeur du mode d'encapsulage d'appareil par « encapsulationLite » et modifie les règles de pare-feu sur l'appareil pour limiter les demandes entrantes à celles provenant de Lenovo XClarity Administrator.

Une fois l'encapsulage désactivé, le mode d'encapsulage prend la valeur « Normal ». Si l'encapsulage était précédemment activé sur les appareils, les règles de pare-feu d'encapsulage sont retirées.

Vous pouvez activer ou désactiver l'encapsulage de manière globale pour tous les appareils lors du processus de gestion en sélectionnant la case à cocher **Activer l'encapsulage de tous les appareils gérés ultérieurs** sur la page Reconnaître et gérer de nouveaux appareils. L'encapsulage est désactivé par défaut.

Vous pouvez également activer ou désactiver l'encapsulage de manière individuelle pour certains appareils gérés en accédant à tout moment à la page récapitulant les appareils, en sélectionnant l'appareil et en cliquant sur **Actions → Activer l'encapsulage** ou **Actions → Désactiver l'encapsulage**.

Attention : Si l'encapsulage est activé et que XClarity Administrator n'est plus disponible avant l'annulation de la gestion d'un dispositif, des mesures doivent être prises pour désactiver l'encapsulage afin d'établir la communication avec le dispositif. Pour les procédures de récupération, voir le fichier lenovoMgrAlert.mib et Reprise de la gestion avec un module CMM après une défaillance du serveur de gestion.

Remarque : L'encapsulage n'est pas pris en charge sur les commutateurs, les dispositifs de stockage et les châssis et serveurs non Lenovo.

Implémentation de la conformité avec la norme NIST SP 800-131A

Si vous devez respecter la norme NIST SP 800-131A, vous pouvez commencer par mettre en place un environnement intégralement conforme à l'aide de Lenovo XClarity Administrator.

À propos de cette tâche

La norme NIST SP 800-131A (National Institute of Standards and Technology Special Publication 800-131A) définit la façon dont les communications sécurisées doivent être gérées. Cette norme vient en renforcement

des algorithmes et augmente les longueurs de clés afin d'améliorer la sécurité. La norme NIST SP 800-131A requiert que les utilisateurs respectent une mise en application stricte de cette norme.

Remarques : Actuellement, les composants Flex System ne prennent pas en charge la norme NIST SP 800-131A. Les communications entre XClarity Administrator ou le module CMM et ces composants ne sont pas compatibles :
- Commutateur évolutif 10 Gb Flex System EN4023
- Commutateur Ethernet 40 Gb Flex System EN6131
- Commutateur SAN 8 Gb Flex System FC3171
- Commutateur évolutif SAN 16 Gb Flex System FC5022
- Commutateur Flex System IB6131 Infiniband

Remarque : Lorsqu'un fournisseur d'identité SAML est utilisé à des fins d'authentification, XClarity Administrator utilise SHA-1 pour apposer la signature dans les métadonnées. L'utilisation de l'algorithme SHA-1 pour les signatures numériques n'est pas compatible avec la norme NIST SP 800-131A.

Procédure

Pour implémenter la conformité avec la norme NIST SP 800-131A, procédez comme suit.

Etape 1. Assurez-vous que vos appareils respectent les critères suivants :

- Utilisation de SSL (Secure Sockets Layer) avec le protocole TLS v1.2.
- Utilisation de SHA-256 ou de fonctions de hachage plus fortes pour les signatures numériques et de SHA-1 ou de fonctions de hachage plus fortes pour les autres applications.
- Utilisation de RSA-2048 ou niveau supérieur ou de courbes elliptiques conformes à NIST de 224 bits ou plus.
- Utilisation d'un chiffrement symétrique conforme à NIST avec des clés d'au moins 128 bits de longueur.
- Utilisation de générateurs de nombres aléatoires conformes à NIST.
- Lorsque cela est possible, prise en charge de mécanismes d'échange de clés Diffie-Hellman ou Elliptic Curve Diffie-Hellman.

Etape 2. Configurez les paramètres cryptographiques sur Lenovo XClarity Administrator. Il existe deux paramètres relatifs à la conformité avec NIST SP 800-131A :

- Le *mode SSL/TLS* spécifie les protocoles à utiliser pour les communications sécurisées. XClarity Administrator prend en charge le paramètre **Serveur et client TLS 1.2** permettant de limiter le protocole cryptographique à TLS 1.2 sur XClarity Administrator et tous les appareils gérés.
- Si des communications sécurisées sont implémentées, le *mode cryptographique* définit les longueurs de clé de chiffrement à utiliser. Vous pouvez affecter la valeur **NIST SP 800-131A** au mode cryptographique. Cependant, vous ne pourrez peut-être pas déployer certains systèmes d'exploitation via XClarity Administrator car certains programmes d'installation de système d'exploitation ne prennent pas en charge les paramètres restreints. Pour permettre la prise en charge du déploiement de système d'exploitation, vous pouvez choisir d'autoriser une exception pour le déploiement du système d'exploitation.

Lorsque vous modifiez tous les paramètres cryptographiques, XClarity Administrator met à disposition les nouveaux paramètres pour tous les appareils gérés et tente de résoudre tous les nouveaux certificats sur ces dispositifs.

Remarque : Vous devez redémarrer XClarity Administrator manuellement après avoir modifié les paramètres cryptographiques de sorte que ces modifications prennent effet et que les services éventuellement perdus soient restaurés (voir Redémarrage de XClarity Administrator dans la documentation en ligne de).

Pour plus d'informations sur ces paramètres, voir Configuration des paramètres cryptographiques sur le serveur de gestion.

Etape 3. Utilisez un navigateur Web prenant en charge le protocole TLS1.2 et les fonctions de hachage SHA-256 et activez ces paramètres dans votre navigateur Web.

Remarque : Si vous utilisez ou souhaitez utiliser des certificats à signature externe ou personnalisés, tous les certificats présents dans la chaîne doivent être basés sur les fonctions de hachage SHA-256.

Etape 4. Utilisez des protocoles chiffrés pour toutes les communications. N'activez pas de protocoles non chiffrés, tels que Telnet, FTP et VNC, pour les communications distantes avec des appareils gérés par XClarity Administrator.

Utilisation de VMware Tools

Le module VMware Tools est installé sur le système d'exploitation invité de la machine virtuelle lorsque vous installez Lenovo XClarity Administrator dans des environnements VMware ESXi. Ce module fournit un sous-ensemble d'outils VMware qui prennent en charge la sauvegarde et la migration optimisées des dispositifs virtuels tout en conservant l'état et la continuité des applications.

Pour plus d'informations sur l'utilisation de VMware Tools, voir Site Web Utilisation de l'utilitaire de configuration des outils VMware dans le centre de documentation VMware vSphere.

Configuration de l'accès réseau

Lorsque vous configurez initialement Lenovo XClarity Administrator, vous configurez jusqu'à deux interfaces réseau. En outre, vous devez indiquer laquelle de ces interfaces doit être utilisée pour déployer des systèmes d'exploitation. Après la configuration initiale, vous pouvez modifier ces paramètres.

Avant de commencer

Attention :

- Le fait de modifier l'adresse IP de XClarity Administrator après avoir géré des appareils peut avoir pour effet de placer les appareils dans un état hors ligne dans XClarity Administrator. Vérifiez que la gestion de tous les appareils a été annulée avant de modifier l'adresse IP.
- Vous pouvez activer ou désactiver le contrôle des adresses IP en double dans le même sous-réseau en cliquant sur le bouton **Contrôle des adresses IP en double**. Ce contrôle est désactivé par défaut. Lorsqu'il est activé, XClarity Administrator déclenche une alerte si vous essayez de changer l'adresse IP de XClarity Administrator ou de gérer un appareil ayant la même adresse IP qu'un autre appareil en cours de gestion, ou qu'un autre appareil figurant sans le même sous-réseau.

  Remarque : Lorsque cette fonction est activée, XClarity Administrator exécute une analyse ARP pour rechercher les appareils IPv4 actifs sur le même sous-réseau. Pour empêcher l'analyse ARP, désactivez **Vérification des doublons d'adresse IP**.
- Lors de l'exécution de XClarity Administrator en tant que dispositif virtuel, si l'interface réseau pour le réseau de gestion est configurée pour utiliser Dynamic Host Configuration Protocol (DHCP), l'adresse IP de l'interface de gestion peut être modifiée lorsque le bail DHCP arrive à expiration. Si tel est le cas, vous devez annuler la gestion, puis activer de nouveau la gestion du châssis, de l'armoire et des serveurs au format tour. Pour éviter ce problème, vous pouvez remplacer l'interface de gestion par une adresse IP statique ou vérifier que la configuration du serveur DHCP est définie de telle sorte que l'adresse DHCP soit basée sur une adresse MAC ou que le crédit-bail n'expire pas.
- Si vous *ne souhaitez pas* utiliser XClarity Administrator pour déployer le système d'exploitation ou mettre à jour les pilotes de périphérique SE, vous pouvez désactiver les serveurs Samba et Apache en modifiant

l'interface réseau pour utiliser l'option **Reconnaître et gérer le matériel uniquement**. Notez que le serveur de gestion est redémarré après modification de l'interface réseau.

- Lors de l'exécution de XClarity Administrator en tant que conteneur.
  - Vous pouvez uniquement activer ou désactiver la vérification des doublons d'adresse IP, modifier les rôles de l'interface réseau ou les paramètres proxy. Tous les autres paramètres réseau (y compris l'adresse IP, la passerelle et le DNS) sont définis dans la configuration du conteneur.
  - Assurez-vous qu'un réseau macvlan est configuré sur le système hôte.

À propos de cette tâche

XClarity Administrator possède deux interfaces réseau distinctes que vous pouvez définir pour votre environnement en fonction de la topologie de réseau que vous mettez en place. Pour les dispositifs virtuels, ces réseaux sont nommés eth0 et eth1. Pour les conteneurs, vous pouvez choisir des noms personnalisés.

- Lorsque une seule interface réseau (eth0) est présente:
  - L'interface doit être configurée pour la prise en charge de la détection et la gestion des appareils (par exemple, la configuration de serveur et les mises à jour de microprogramme). Elle doit pouvoir communiquer avec les commutateurs CMM et Flex System sur chaque châssis géré, le contrôleur de gestion de la carte mère sur chaque serveur géré, et chaque commutateur RackSwitch.
  - Si vous prévoyez d'acquérir des mises à jour du microprogramme et des pilotes de périphérique à l'aide de XClarity Administrator, au moins l'une des interfaces réseau doit être connectée à Internet, de préférence via un pare-feu. Sinon, vous devez importer des mises à jour dans le référentiel.
  - Si vous souhaitez collecter des données de maintenance ou utiliser la notification de problèmes automatique (y compris l'Appel vers Lenovo et la fonction de téléchargement Lenovo), au moins l'une des interfaces réseau doit être connectée à Internet, de préférence via un pare-feu.
  - Si vous avez l'intention de déployer des images du système d'exploitation et de mettre à jour des pilotes de périphérique, l'interface réseau doit disposer d'une connectivité réseau IP à l'interface réseau du serveur qui est utilisée pour accéder au système d'exploitation hôte.

    Remarque : Si vous implémentiez un réseau distinct pour le déploiement SE et les mises à jour de pilote de périphérique SE, vous pouvez configurer la seconde interface réseau pour la connexion à ce réseau au lieu du réseau de données. Toutefois, si le système d'exploitation sur chaque serveur n'a pas accès au réseau de données, configurez une interface supplémentaire sur les serveurs pour assurer la connectivité entre le système d'exploitation hôte sur le serveur et le réseau de données pour le déploiement SE et les mises à jour de pilote de périphérique, si nécessaire.
- Lorsque deux interfaces réseau (eth0 et eth1) sont présentes:
  - La première interface réseau (généralement, l'interface Eth0) doit être connectée au réseau de gestion et configurée pour prendre en charge la détection et la gestion des appareils (y compris configuration de serveur et les mises à jour du microprogramme). Elle doit pouvoir communiquer avec les commutateurs CMM et Flex System sur chaque châssis géré, le contrôleur de gestion sur chaque serveur géré, et chaque commutateur RackSwitch.
  - La seconde interface réseau (généralement, l'interface eth1) peut être configurée pour communiquer avec un réseau de données interne, un réseau de données public ou les deux.
  - Si vous prévoyez d'acquérir des mises à jour du microprogramme et des pilotes de périphérique à l'aide de XClarity Administrator, au moins l'une des interfaces réseau doit être connectée à Internet, de préférence via un pare-feu. Sinon, vous devez importer des mises à jour dans le référentiel.
  - Si vous souhaitez collecter des données de maintenance ou utiliser la notification de problèmes automatique (y compris l'Appel vers Lenovo et la fonction de téléchargement Lenovo), au moins l'une des interfaces réseau doit être connectée à Internet, de préférence via un pare-feu.

– Si vous prévoyez de déployer des images de système d'exploitation et de mettre à jour des pilotes de périphérique, vous pouvez choisir d'utiliser l'interface eth0 ou eth1. Toutefois, l'interface que vous utilisez doit disposer d'une connectivité de réseau IP à l'interface réseau du serveur qui est utilisé pour accéder au système d'exploitation hôte.

  Remarque : Si vous implémentiez un réseau distinct pour le déploiement SE et les mises à jour de pilote de périphérique SE, vous pouvez configurer la seconde interface réseau pour la connexion à ce réseau au lieu du réseau de données. Toutefois, si le système d'exploitation sur chaque serveur n'a pas accès au réseau de données, configurez une interface supplémentaire sur les serveurs pour assurer la connectivité entre le système d'exploitation hôte sur le serveur et le réseau de données pour le déploiement SE et les mises à jour de pilote de périphérique, si nécessaire.

Le tableau suivant répertorie des configurations possibles pour les interfaces réseau de XClarity Administrator en fonction du type de topologie de réseau qui est implémenté dans votre environnement. Utilisez ce tableau pour déterminer comment définir chaque interfaces réseau.

Tableau 2. Rôle de chaque interfaces réseau en fonction de la topologie de réseau

Topologie de réseau	**Rôle de l'interface 1 (eth0)**	**Rôle de l'interface 2 (eth1)**
Réseau convergé (réseau de gestion et de données avec prise en charge pour le déploiement SE et les mises à jour du pilote de périphérique SE)	Réseau de gestion • Reconnaissance et gestion • Configuration du serveur • Mises à jour du microprogramme • Collecte des données de maintenance • Notification de problèmes automatique (par exemple, l'Appel Lenovo et la fonction de mise à jour Lenovo) • Récupération des données relatives à la garantie • Déploiement SE • Mises à jour de pilote de périphériques SE	Aucun
Réseau de gestion distinct avec prise en charge pour le déploiement SE et les mises à jour du pilote de périphérique et réseau de données	Réseau de gestion • Reconnaissance et gestion • Configuration du serveur • Mises à jour du microprogramme • Collecte des données de maintenance • Notification de problèmes automatique (par exemple, l'Appel Lenovo et la fonction de mise à jour Lenovo) • Récupération des données relatives à la garantie • Déploiement SE • Mises à jour de pilote de périphériques SE	Réseau de données • Aucun

Tableau 2. Rôle de chaque interfaces réseau en fonction de la topologie de réseau (suite)

Topologie de réseau	Rôle de l'interface 1 (eth0)	Rôle de l'interface 2 (eth1)
Réseau de gestion distinct et réseau de données avec prise en charge pour le déploiement SE et les mises à jour de pilote de périphérique	Réseau de gestion • Reconnaissance et gestion • Configuration du serveur • Mises à jour du microprogramme • Collecte des données de maintenance • Notification de problèmes automatique (par exemple, l'Appel Lenovo et la fonction de mise à jour Lenovo) • Récupération des données relatives à la garantie	Réseau de données • Déploiement SE • Mises à jour de pilote de périphériques SE
Réseau de gestion distinct et réseau de données sans prise en charge pour le déploiement SE et les mises à jour de pilote de périphérique	Réseau de gestion • Reconnaissance et gestion • Configuration du serveur • Mises à jour du microprogramme • Collecte des données de maintenance • Notification de problèmes automatique (par exemple, l'Appel Lenovo et la fonction de mise à jour Lenovo) • Récupération des données relatives à la garantie	Réseau de données • Aucun
Réseau de gestion uniquement (le déploiement SE et les mises à jour de pilote de périphérique ne sont pas pris en charge)	Réseau de gestion • Reconnaissance et gestion • Configuration du serveur • Mises à jour du microprogramme • Collecte des données de maintenance • Notification de problèmes automatique (par exemple, l'Appel Lenovo et la fonction de mise à jour Lenovo) • Récupération des données relatives à la garantie	Aucun

Pour plus d'informations sur les interfaces réseau de XClarity Administrator, y compris les limitations d'adresse IPv6, voir Remarques sur le réseau dans la documentation en ligne de XClarity Administrator.

Procédure

Pour configurer un accès réseau, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Accès réseau**. Les paramètres réseau actuels sont affichés.

Etape 2. De manière facultative, vous pouvez activer la vérification des doublons d'adresses IP dans le même sous-réseau en cliquant sur le bouton **Vérification des doublons d'adresse IP**.

Lorsqu'il est activé, XClarity Administrator déclenche une alerte si vous essayez de changer l'adresse IP de XClarity Administrator ou de gérer un appareil ayant la même adresse IP qu'un autre appareil en cours de gestion, ou qu'un autre appareil figurant sans le même sous-réseau.

Etape 3. Cliquez sur **Éditer l'accès réseau** pour afficher la page Éditer l'accès réseau.

Etape 4. Si vous prévoyez de déployer des systèmes d'exploitation et de mettre à jour des pilotes de périphérique SE avec XClarity Administrator, choisissez l'interface réseau à utiliser pour la gestion des systèmes d'exploitation.

- Si une seule interface est définie pour XClarity Administrator, choisissez si cette interface doit être utilisée pour reconnaître et gérer le matériel uniquement, ou si elle doit également être utilisée pour gérer les systèmes d'exploitation.
- Si deux interfaces sont définies pour XClarity Administrator (Eth0 et Eth1), déterminez l'interface à utiliser pour gérer les systèmes d'exploitation. Si vous choisissez « Aucune », vous *ne pouvez pas* déployer des images du système d'exploitation ou mettre à jour des pilotes de périphérique SE sur des serveurs gérés à partir de XClarity Administrator.

Etape 5. (XClarity Administrator en tant que dispositif virtuel uniquement) Modifiez les paramètres IP.

a. Pour la première interface, indiquez l'adresse IPv4, l'adresse IPv6 ou les deux.

- **IPv4**. Vous devez attribuer une adresse IPv4 à l'interface. Vous pouvez choisir d'utiliser une adresse IP attribuée de manière statique ou obtenir une adresse IP à partir d'un serveur DHCP.
- **IPv6**. Si vous le souhaitez, vous pouvez affecter une adresse IPv6 à l'interface à l'aide de l'une des méthodes d'affectation suivantes :
  - Utiliser l'adresse IP affectée de manière statique
  - Utiliser la configuration d'adresse avec état (DHCPv6)
  - Utiliser la configuration automatique d'adresse sans état

  Remarque : Pour plus d'informations sur les limitations d'adresse IPv6, voir Limitations de la configuration IPv6 dans la documentation en ligne de XClarity Administrator.

b. Si une seconde interface est disponible, indiquez l'adresse IPv4, l'adresse IPv6 ou les deux.

  Remarque : Les adresses IP attribuées à cette interface doivent être sur un sous-réseau différent des adresses IP attribuées à la première interface. Si vous choisissez d'utiliser le DHCP pour attribuer des adresses IP pour les deux interfaces (Eth0 et Eth1), le serveur DHCP ne doit pas attribuer le même sous-réseau pour les adresses IP des deux interfaces.

- **IPv4**. Vous pouvez choisir d'utiliser une adresse IP attribuée de manière statique ou obtenir une adresse IP à partir d'un serveur DHCP.
- **IPv6**. Si vous le souhaitez, vous pouvez affecter une adresse IPv6 à l'interface à l'aide de l'une des méthodes d'affectation suivantes :
  - Utiliser l'adresse IP affectée de manière statique
  - Utiliser la configuration d'adresse avec état (DHCPv6)
  - Utiliser la configuration automatique d'adresse sans état

c. Indiquez la passerelle par défaut.

Si vous indiquez une passerelle par défaut, celle-ci doit être une adresse IP valide et utiliser le même masque de réseau (le même sous-réseau) que l'adresse IP de l'une des interfaces réseau (Eth0 ou Eth1). Si vous utilisez une interface unique, la passerelle par défaut doit se trouver sur le même sous-réseau que l'interface réseau.

Si l'une des interfaces utilise le protocole DHCP pour obtenir une adresse IP, la passerelle par défaut utilise également le DHCP. Pour saisir manuellement une adresse de passerelle par défaut qui remplace celle reçue du serveur DHCP, sélectionnez la case à cocher **Remplacer la passerelle**.

Astuces :

- Assurez-vous que la passerelle correspond à l'un des sous-réseaux des interfaces réseau. La passerelle par défaut est automatiquement définie via cette interface réseau.
- Pour revenir à une passerelle fournie par DHCP, désélectionnez **Remplacer la passerelle**.

ATTENTION :
Si vous choisissez de remplacer la passerelle, faites attention à saisir la bonne adresse de passerelle ; sinon, ce serveur de gestion ne sera pas accessible et il n'y aura aucun moyen de se connecter à distance pour la corriger.

d. Cliquez sur **Enregistrer les paramètres IP**.

Etape 6. (XClarity Administrator en tant que dispositif virtuel uniquement) De manière facultative, modifiez les paramètres avancés.

a. Cliquez sur l'onglet **Routage avancé**.

b. Spécifiez un ou plusieurs entrées de route dans la table **Paramètres de route avancés** à utiliser par cette interface.

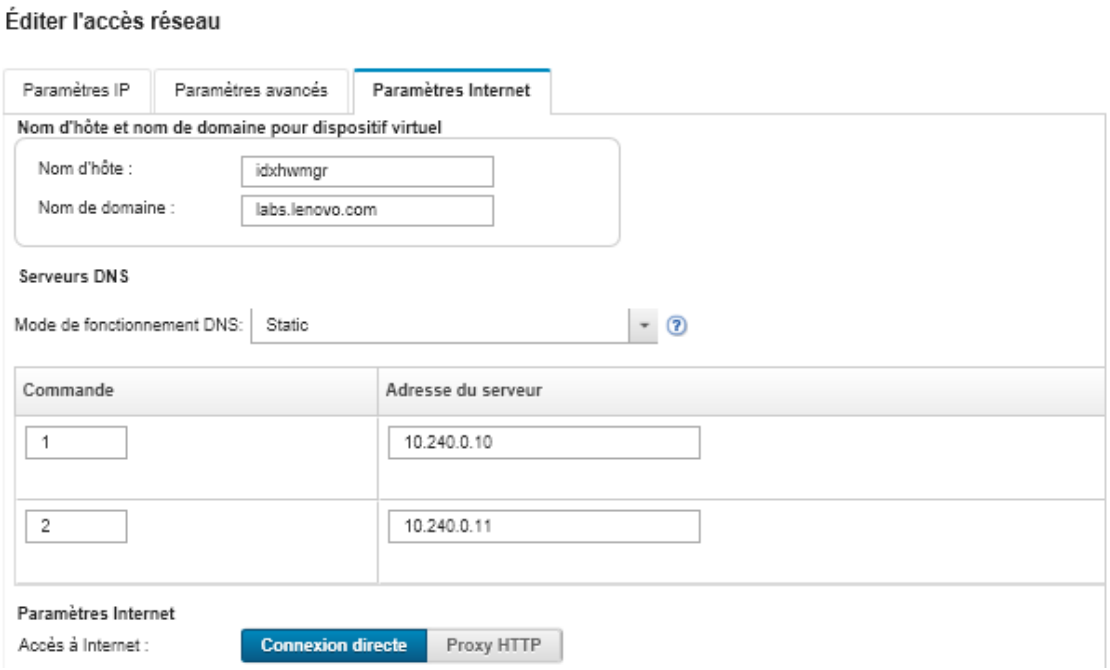
Pour définir une ou plusieurs entrées de route, procédez comme suit.
1. Sélectionnez l'interface.
2. Indiquez le type de route, qui peut être une route vers un autre hôte ou un réseau.
3. Indiquez l'hôte ou l'adresse réseau de destination auxquels vous envoyez la route.
4. Indiquez le masque de sous-réseau pour l'adresse de destination.
5. Indiquez l'adresse de passerelle à laquelle les modules doivent être adressés.

c. Cliquez sur **Enregistrer le routage avancé**.

Etape 7. Si vous le souhaitez, vous pouvez modifier les paramètres DNS et proxy.

Lorsque XClarity Administrator est défini comme conteneur, seuls les paramètres proxy peuvent être modifiés depuis l'interface Web. Les paramètres DNS sont définis dans le conteneur.

a. Cliquez sur l'onglet **DNS et proxy**.



b. Indiquez le nom d'hôte et le nom de domaine à utiliser pour XClarity Administrator.

c. Sélectionnez le mode de fonctionnement DNS. Les valeurs possibles sont **Statique** ou **DHCP**.

Attention : Vous devez redémarrer le serveur de gestion lorsque vous modifiez le mode de fonctionnement DNS.

Remarque : Si vous choisissez d'utiliser un serveur DHCP pour obtenir l'adresse IP, toutes les modifications que vous apportez aux champs **Serveur DNS** sont remplacées la fois suivante où XClarity Administrator renouvelle le bail DHCP.

d. Indiquez l'adresse IP d'un ou de plusieurs serveurs DNS (Domain Name System) à utiliser, ainsi que l'ordre de priorité de chacun.

e. Indiquez si l'accès à Internet est un proxy de connexion directe ou HTTP (si XClarity Administrator a accès à Internet).

Remarques : Si vous utilisez un proxy HTTP, vérifiez que les conditions suivantes sont remplies.
- Vérifiez que le serveur proxy est configuré pour utiliser l'authentification de base.
- Vérifiez que le serveur proxy est configuré en tant que proxy sans arrêt.
- Vérifiez que le serveur proxy est configuré en tant que proxy de transfert.
- Vérifiez que les dispositifs d'équilibrage de charge sont configurés pour conserver des sessions avec un serveur proxy et non pour basculer entre eux.

Si vous choisissez d'utiliser un proxy HTTP, remplissez les zones obligatoires :
1. Indiquez le nom d'hôte et le port du serveur proxy.

2. Indiquez si vous souhaitez utiliser l'authentification, et indiquez le nom d'utilisateur et le mot de passe si nécessaire.
3. Indiquez l'URL du test de proxy.
4. Cliquez sur **Proxy de texte** pour vérifier que les paramètres de proxy sont configurés et fonctionnent correctement.

f. Cliquez sur **Enregistrer DNS et proxy**.

g. Envoyez les informations de DNS et FQDN (nom de domaine pleinement qualifié) du serveur de gestion XClarity Administrator aux serveurs gérés avec IMM2, XCC et XCC2 pour que les serveurs gérés trouvent le serveur de gestion à l'aide de ces informations.

1. Cliquez sur **Envoyer FQDN / DNS vers BMC**.
2. Choisissez comment traiter les entrées DNS existantes dans le contrôleur de gestion de la carte mère.
   - Conservez les entrées DNS existantes, puis ajoutez les entrées DNS du serveur de gestion dans l'emplacement disponible suivant.
   - Remplacez toutes les entrées DNS existantes par les entrées DNS du serveur de gestion.
3. Tapez **OUI** dans le champ éditable.
4. Cliquez sur **Appliquer**.

Une travail est créé pour effectuer cette opération. Vous pouvez surveiller la progression du travail à partir de la carte **Surveillance → Travaux**. Si le travail n'est pas terminé, cliquez sur le lien travail pour afficher des détails sur le travail (voir).

Vous pouvez également supprimer les informations FQDN et DNS du serveur de gestion des serveurs gérés par IMM2, XCC et XCC2 en cliquant sur **Supprimer FQDN / DNS de BMC**. Vous pouvez choisir de conserver d'autres entrées DNS existantes, de supprimer toutes les entrées DNS ou de ne supprimer que les entrées qui correspondent aux informations du serveur de gestion.

Etape 8. Cliquez sur **Redémarrer** pour redémarrer le serveur de gestion.

Etape 9. Cliquez sur **Tester la connexion** pour vérifier les paramètres réseau.

Définition de la date et de l'heure

Vous pouvez régler la date et l'heure à utiliser pour Lenovo XClarity Administrator.

Avant de commencer

Vous devez utiliser au moins un (quatre maximum) serveur NTP (Network Time Protocol) afin de synchroniser les horodatages pour tous les événements reçus à partir d'appareils gérés avec XClarity Administrator.

Conseil : Le serveur NTP doit être accessible via le réseau de gestion (généralement, l'interface Eth0). Pensez à configurer le serveur NTP sur l'hôte sur lequel XClarity Administrator s'exécute.

Si vous modifiez l'heure sur le serveur NTP, un certain temps peut être nécessaire pour que XClarity Administrator se synchronise avec la nouvelle heure.

Attention : Le dispositif virtuel XClarity Administrator et son hôte doivent être définis pour une synchronisation avec la même source temporelle afin d'éviter toute synchronisation involontaire entre XClarity Administrator et son hôte. Généralement, l'hôte est configuré pour que les dispositifs virtuels se synchronisent avec lui. Si XClarity Administrator est défini pour se synchroniser sur une source différente de son hôte, vous devez désactiver la synchronisation des horloges de l'hôte entre les dispositifs virtuels XClarity Administrator et son hôte.

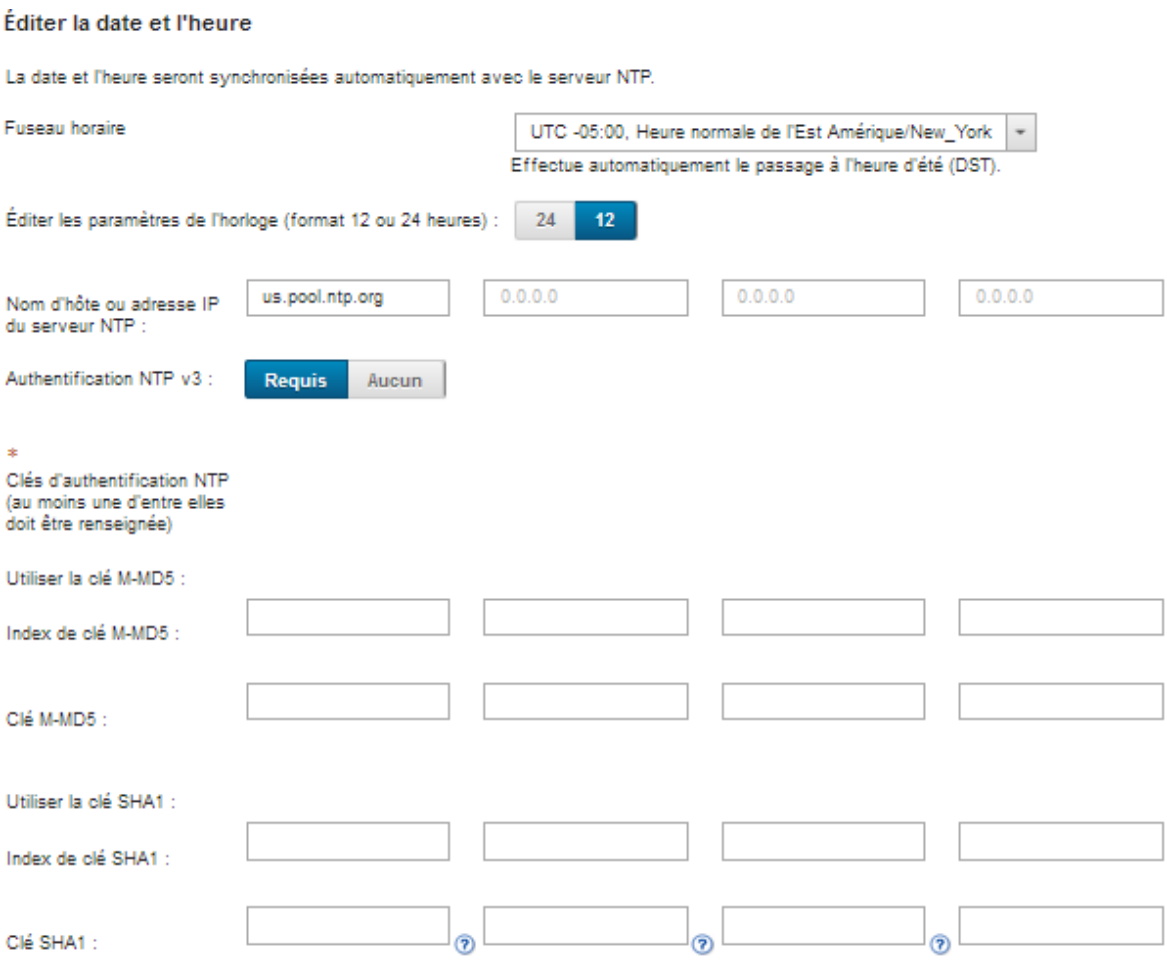
- Pour ESXi, suivez les instructions dans VMware – Page Web Désactivation de la synchronisation des horloges.
- Pour Hyper-V du Gestionnaire Hyper-V, cliquez avec le bouton droit sur la machine virtuelle XClarity Administrator, puis cliquez sur **Paramètres**. Dans la boîte de dialogue, cliquez sur **Gestion > Services d'intégration** dans le panneau de navigation, puis désélectionnez **Synchronisation des horloges**.

Procédure

Procédez comme suit pour définir la date et l'heure pour XClarity Administrator.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Date et heure**. La page Date et heure s'affiche. Cette page affiche les date et heure actuelles pour XClarity Administrator.

Etape 2. Cliquez sur **Éditer la date et l'heure** pour afficher la page Éditer la date et l'heure.



Etape 3. Renseignez la boîte de dialogue de date et d'heure.

1. Choisissez le fuseau horaire correspondant à l'hôte pour XClarity Administrator.

   Si le fuseau horaire sélectionné observe l'heure d'été (DST), l'heure est automatiquement ajustée en fonction.
2. Choisissez d'utiliser une horloge 12 heures ou 24 heures.
3. Indiquez le nom d'hôte ou l'adresse IP pour chaque serveur NTP dans votre réseau. Vous pouvez définir jusqu'à quatre serveurs NTP.

4. Sélectionnez **Requis** pour activer l'authentification NTP v3, ou bien sélectionnez **Aucun** pour utiliser l'authentification NTP v1 entre XClarity Administrator et les serveurs NTP au sein de votre réseau.

   Vous pouvez utiliser l'authentification v3 si les modules CMM Flex System gérés et les contrôleurs de gestion de la carte mère disposent d'un microprogramme qui requiert une authentification v3 et si l'authentification NTP v3 est requise entre XClarity Administrator et un ou plusieurs serveur NTP au sein de votre réseau

5. Si vous avez activé l'authentification NTP v3, vous devez définir la clé d'authentification et l'index pour chaque serveur NTP applicable. Vous pouvez spécifier une clé M-MD5, SHA1 ou les deux. Si des clés M-MD5 ou SHA1 sont spécifiées, XClarity Administrator transmet une clé M-MD5 ou SHA1 aux modules CMM Flex System et aux contrôleurs de gestion qui les prennent en charge. Le XClarity Administrator utilisera la clé pour vous authentifier auprès du serveur NTP

   - Pour la clé M-MD5, spécifiez une chaîne ASCII comprenant uniquement des lettres majuscules et minuscules (a-z, A-Z), des chiffres (0-9) et les caractères spéciaux @#.
   - Pour la clé SHA1, spécifiez une chaîne ASCII de 40 caractères, comprenant uniquement des caractères dans les plages 0-9 et a-f.
   - L'index de clé et la clé d'authentification spécifiés doivent correspondre aux valeurs key ID et password qui sont définies sur le serveur NTP. Par exemple, si l'index de clé de la clé SHA1 entrée dans le serveur NTP est 5, l'index de clé spécifié de la clé SHA1 de XClarity Administrator est également 5. Pour plus d'informations sur la configuration de l'ID et du mot de passe de clé, voir la documentation de votre serveur NTP.
   - Vous devez spécifier la clé pour chaque serveur NTP utilisant l'authentification v3, même si deux serveurs NTP ou plus utilisent la même clé.
   - Si vous avez activé l'authentification v3, mais que vous ne fournissez pas de clé d'authentification et d'index pour un serveur NTP, l'authentification v1 est utilisée par défaut.
   - Si vous avez spécifié plusieurs serveurs NTP, les serveurs NTP doivent être tous authentifiés selon l'authentification v3 ou tous selon l'authentification v1. Une combinaison de serveurs NTP authentifiés selon les authentifications v3 et v1 ne sera pas prise en charge.
   - Si vous avez spécifié plusieurs serveurs NTP avec l'authentification v3, les indices de clés doivent être uniques si plusieurs clés sont utilisées. Par exemple, les serveurs NTP 1 et 2 ne peuvent pas disposer d'un indice de clé SHA 1 si les clés SHA1 diffèrent dans les serveurs NTP 1 et 2. Vous devez configurer l'un des serveurs NTP de sorte qu'il accepte la clé ayant un indice de clé différent de l'autre serveur NTP ; dans le cas contraire, la dernière clé définie associée à l'index de clé sera configurée pour tous les serveurs NTP ayant le même indice de clé.

Etape 4. Cliquez sur **Enregistrer**.

Définition des préférences d'inventaire

Vous pouvez définir vos préférences d'inventaire pour les appareils gérés, y compris la propriété à utiliser pour afficher le nom de l'appareil.

Procédure

Effectuez les étapes suivantes pour définir les préférences d'inventaire des appareils gérés.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Administration → Préférences de l'inventaire**. La page Préférences de l'inventaire s'affiche.

Etape 2. Sélectionnez la propriété à utiliser pour le nom d'appareil affiché dans l'interface utilisateur de Lenovo XClarity Administrator. Vous pouvez sélectionner l'une des propriétés suivantes :
- **Séquence prédéfinie (par défaut)**
- **Nom défini par l'utilisateur**
- **Nom d'hôte du module DNS**
- **Nom d'hôte**
- **Adresse IPv4**
- **Numéro de série**

Si l'option **Séquence prédéfinie** est sélectionnée, le nom d'appareil affiché est choisi en fonction de la séquence des propriétés de la liste précédente. Par exemple, si un appareil a un nom défini par l'utilisateur, ce nom s'affiche. Si un appareil n'a pas de nom défini par l'utilisateur, le nom d'hôte DNS s'affiche. Si un appareil n'a pas de nom défini par l'utilisateur ou de nom d'hôte DNS, le nom d'hôte s'affiche.

Remarque : Sélectionner une autre valeur que celle par défaut change le nom qui est affiché dans l'interface utilisateur de Lenovo XClarity Administrator pour tous les appareils à celui de la propriété sélectionnée. Le nom défini par l'utilisateur affecté à l'appareil ne change pas.

Etape 3. Cliquez éventuellement sur **Activer** pour choisir de trier les grilles (tableaux) avec la valeur sélectionnée pour le nom de l'appareil.

Etape 4. Sélectionnez la préférence d'ordre de numérotation d'armoire, de haut en bas (par exemple, 1 à 52) ou de bas en haut (par exemple, 52 à 1).

Remarque : La modification de la préférence d'ordre des nombres ne modifie pas l'emplacement d'un appareil dans l'armoire.

Etape 5. Cliquez sur **Appliquer**.

Après avoir terminé

Vous pouvez définir des préférences de seuil pour le déclenchement d'une alerte et d'un événement lorsqu'une certaine valeur, comme la durée de vie d'un disque SSD sur un serveur ThinkSystem ou ThinkServer dépasse un niveau d'avertissement ou critique (voir Définition des préférences de seuil pour la génération d'alertes et d'événements).

Définition des préférences de seuil pour la génération d'alertes et d'événements

Vous pouvez définir des préférences de seuil pour le déclenchement d'une alerte et d'un événement lorsqu'une certaine valeur, comme la durée de vie d'un disque SSD sur un serveur ThinkSystem ou ThinkServer dépasse un niveau d'avertissement ou critique.

Procédure

Procédez comme suit pour réexpédier des fichiers de maintenance spécifiques au prestataire de services.

Etape 1. Dans la barre de menus Lenovo XClarity Administrator, cliquez sur **Surveillance → Alertes** pour afficher la page Alertes.

Etape 2. Cliquez sur l'icône **Paramètres de seuil** () pour afficher la boîte de dialogue Paramètres de seuil.

Etape 3. Modifiez les seuils d'avertissement et critiques pour la durée de vie restante des disques SSD dans les serveurs ThinkSystem et ThinkServer.

La durée de vie restante des disques SSD est calculée à l'aide des compteurs SMART de fournisseur. Les valeurs par défaut sont de 30 % pour le seuil d'avertissement et de 20 % pour le seuil critique.

Etape 4. Sélectionnez la bascule **Activé** pour générer une alerte et un événement lorsque chaque seuil est atteint.

Etape 5. Cliquez sur **Appliquer**.

Configuration de la notification automatique de problème à l'Lenovo Support (Appel vers Lenovo)

Vous pouvez créer un réexpéditeur de service qui envoie automatiquement les données de maintenance d'un appareil géré au Lenovo Support à l'aide de l'Appel vers Lenovo quand certains événements réparables, comme une erreur de mémoire irrécupérable, sont reçus de la part d'un appareil géré spécifique, afin que le problème puisse être résolu. Ce service réexpédié est nommé « Par défaut Appel vers Lenovo. »

Lenovo s'engage sur la sécurité. Lorsque cette fonction est activée, Appel vers Lenovo Lenovo Centre de support lorsqu'un appareil signale une panne matérielle ou que vous choisissez d'initier manuellement un Appel vers Lenovo. Les données de maintenance que vous devez généralement télécharger manuellement vers le support Lenovo sont automatiquement envoyées au Lenovo Centre de support sur HTTPS via TLS 1.2 ou version ultérieure. Vos données d'entreprise ne sont jamais transmises. L'accès aux données de maintenance dans le Lenovo Centre de support est limité au personnel de maintenance autorisé.

Avant de commencer

Attention : Vous devez accepter le document suivant : Déclaration de confidentialité de Lenovo pour pouvoir transférer des données au support Lenovo.

Assurez-vous que tous les ports requis par Lenovo XClarity Administrator (y compris les ports requis pour Appel vers Lenovo) sont disponibles avant d'activer la fonction Appel vers Lenovo. Pour plus d'informations sur les ports, voir Disponibilité de port dans la documentation en ligne de XClarity Administrator.

Vérifiez qu'il existe une connexion aux adresses Internet qui sont requises par l'Appel vers Lenovo. Pour plus d'informations sur les pare-feu, voir Pare-feux et serveurs proxy dans la documentation en ligne de XClarity Administrator.

Si XClarity Administrator accède à Internet via un proxy HTTP, vérifiez que le serveur proxy est configuré pour utiliser l'authentification de base et est configuré en tant que proxy sans arrêt. Pour plus d'informations sur la configuration du proxy, voir Configuration de l'accès réseau Configuration de l'accès réseau dans la documentation en ligne de XClarity Administrator.

Une fois que vous aurez configuré Appel vers Lenovo, le réexpéditeur de service **Appel vers Lenovo par défaut** est ajouté à la page Réexpéditeurs de service. Vous pouvez éditer ce réexpéditeur afin de configurer d'autres paramètres, notamment les appareils associés à ce réexpéditeur. Tous les appareils sont par défaut mis en correspondance. Si aucun appareil n'est spécifié, Appel vers Lenovo n'enverra *pas* les notifications de problème au support Lenovo.

À propos de cette tâche

Un *réexpéditeur de service* définit des informations sur l'endroit auquel envoyer les fichiers de données de maintenance lorsqu'un événement réparable se produit. Vous pouvez définir jusqu'à 50 réexpéditeurs de service.

- **Si un Appel vers Lenovo réexpéditeur de service d' n'est pas configuré**, vous pouvez ouvrir manuellement un ticket de maintenance et envoyer des fichiers de maintenance au Lenovo Centre de

support en suivant les instructions fournies dans Page Web de nouvelle demande de service. Pour plus d'informations sur la collecte et le téléchargement des fichiers de maintenance, voir Téléchargement de fichiers de diagnostic XClarity Administrator et Collecte et téléchargement de fichiers de diagnostic pour un dispositif dans la documentation en ligne de XClarity Administrator.

- **Si un Appel vers Lenovo réexpéditeur de service est configuré mais pas activé**, vous pouvez ouvrir *manuellement* un ticket de maintenance à l'aide de la fonction Appel vers Lenovo pour collecter et transmettre des fichiers de données de maintenance au Lenovo Centre de support à tout moment. Pour plus d'informations, voir Ouverture d'un ticket de maintenance dans la documentation en ligne de XClarity Administrator.
- **Si un Appel vers Lenovo réexpéditeur de service est configuré et activé**, XClarity Administrator collecte *automatiquement* les données de maintenance, ouvre un ticket de maintenance et transfère les fichiers de service au Lenovo Centre de support lorsqu'un événement réparable se produit, de sorte que le problème puisse être résolu.

  Important : Lorsque vous activez un Appel vers Lenovo réexpéditeur de service dans Lenovo XClarity Administrator, Appel vers Lenovo est désactivé sur chaque appareil géré afin d'éviter de générer des enregistrements de problème en double. Si vous prévoyez de cesser d'utiliser XClarity Administrator pour gérer vos appareils ou de désactiver la fonction Appel vers Lenovo dans XClarity Administrator, vous pourrez ultérieurement réactiver la fonction Appel vers Lenovo sur tous les appareils gérés à partir de XClarity Administrator au lieu de réactiver la fonction Appel vers Lenovo pour chaque appareil géré ultérieurement. Pour plus d'informations sur la réactivation de l'Appel vers Lenovo sur tous les appareils gérés lorsque le réexpéditeur de service de l'Appel vers Lenovo est désactivé, voir Réactivation de l'appel vers Lenovo sur tous les appareils gérés dans la documentation en ligne de XClarity Administrator..Pour les serveurs équipés de XCC2, XClarity Administrator enregistre les données de maintenance dans deux fichiers dans le référentiel.

  – **Fichier de maintenance**. (.zip) Ce fichier contient les informations de maintenance et d'inventaire dans un format aisément lisible. Ce fichier est automatiquement envoyé au Lenovo Centre de support lorsqu'un événement réparable se produit.
  – **Fichier de débogage**. (.tzz) Ce fichier contient toutes les informations de maintenance, l'inventaire et les journaux de débogage utilisables par le support Lenovo. Vous pouvez envoyer manuellement ce fichier au support Lenovo si des informations supplémentaires sont nécessaires pour résoudre un problème.

  Pour les autres appareils, XClarity Administrator enregistre les données de maintenance (y compris les informations de maintenance, l'inventaire et les journaux de débogage) dans un fichier de maintenance unique dans le référentiel. Ce fichier est envoyé au Lenovo Centre de support lorsqu'un événement réparable se produit.

  Bien que XClarity Administrator prenne en charge Appel vers Lenovo pour les appareils ThinkAgile et ThinkSystem, le contrôleur de gestion de la carte mère pour certains de ceux-ci n'inclut pas la prise en charge de Appel vers Lenovo. Par conséquent, vous ne pouvez pas activer ou désactiver l'appel vers Lenovo sur ces appareils. L'appel vers Lenovo ne peut être activé que pour ces appareils au niveau XClarity Administrator.

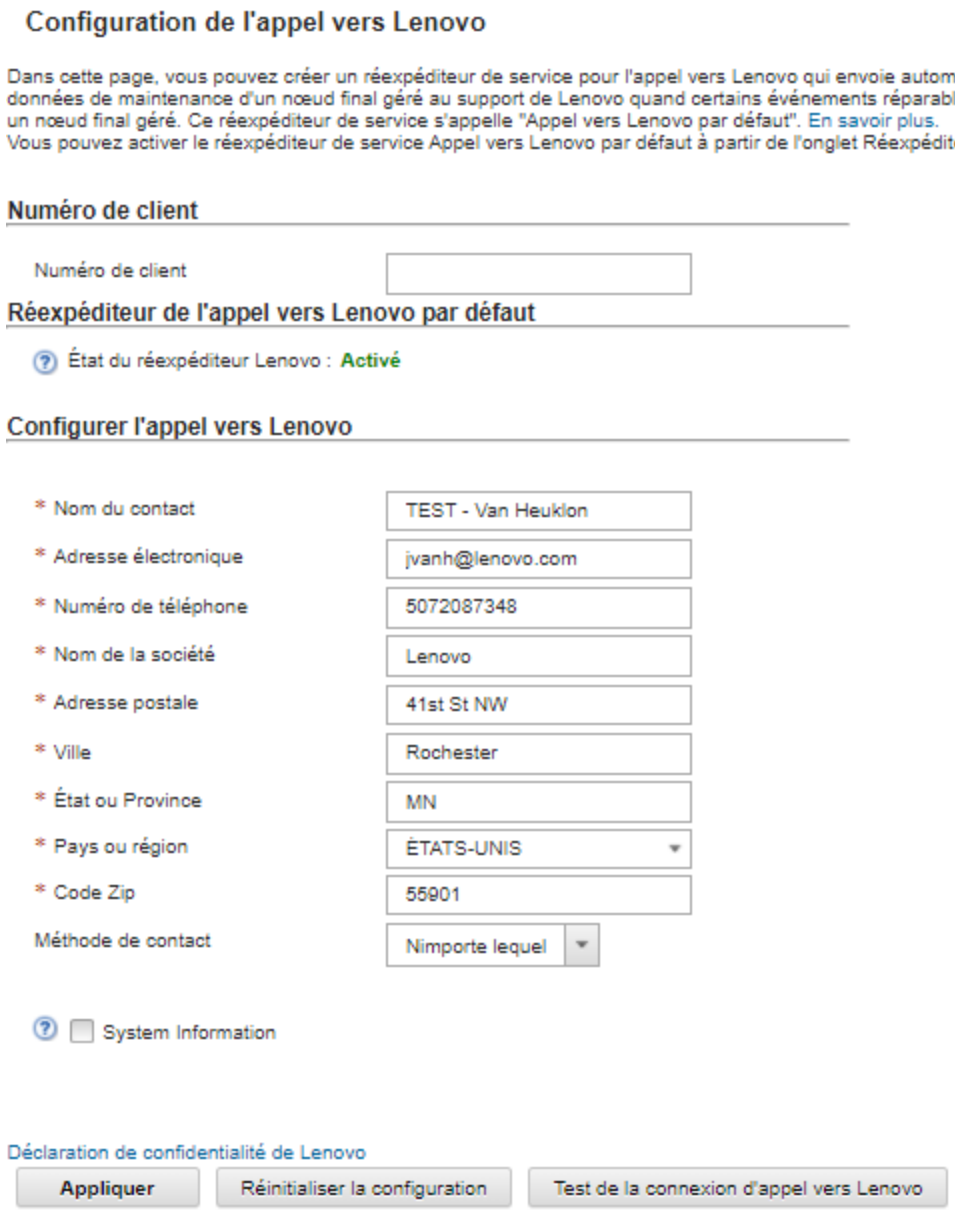
  L'appel vers Lenovo est supprimé pour les événements répétés de tout appareil si un ticket de maintenance est ouvert pour cet événement sur cet appareil. L'appel vers Lenovo est également supprimé pour les événements similaires de tout appareil ThinkAgile et ThinkSystem si un ticket de maintenance est ouvert pour un événement sur cet appareil. Les événements ThinkAgile et ThinkSystem sont des chaînes de 16 caractères au format suivant *xx<2_char_reading_type><2_char_sensor_type>xx<2_char_entity_ID>xxxxxx* (par exemple, `806F010D0401FFFF`). Les événements sont similaires s'ils ont le même type de lecture, le même type de détecteur et le même ID d'entité. Par exemple, si un ticket de maintenance est ouvert pour l'événement 806F010D0401FFFF sur un appareil ThinkAgile ou ThinkSystem spécifique, tous les événements qui se produisent sur cet appareil avec des ID d'événement tels que *xx*`6F01`*xx*`04`*xxxxxx*, où *x* est n'importe quel caractère alphanumérique, sont supprimés.

Pour plus d'informations sur l'affichage de tickets de maintenance qui ont été ouverts automatiquement par un réexpéditeur de service de l'Appel vers Lenovo, voir Affichage des tickets de maintenance et de l'état dans la documentation en ligne de XClarity Administrator.

Procédure

Procédez comme suit pour configurer un service réexpédié pour Appel vers Lenovo.

- Configurez l'Appel vers Lenovo pour tous les appareils gérés (actuels et futurs) :
  1. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Service et support**.
  2. Cliquez sur **Configuration de l'appel vers Lenovo** dans la navigation de gauche pour afficher la page Configuration de l'appel vers Lenovo.



  3. (Facultatif) Indiquez le numéro de client Lenovo par défaut à utiliser pour signaler des problèmes auprès de XClarity Administrator.

Astuce : Vous pouvez trouver le numéro de votre client dans l'e-mail de preuve d'achat que vous avez reçu lorsque de l'achat du Lenovo XClarity Pro.

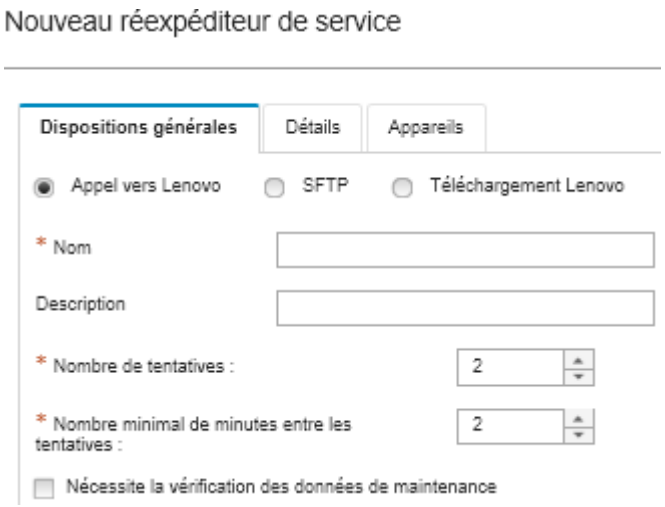
4. Indiquez les informations de contact et d'emplacement.
5. Sélectionnez la méthode de contact préférée du support Lenovo.
6. (Facultatif) Indiquez les informations système.
7. Cliquez sur **Appliquer**.

   Un réexpéditeur de service d'Appel vers Lenovo nommé « Appel vers Lenovo par défaut » est créé pour tous les appareils gérés avec les informations de contact spécifiées.
8. Activez et testez le réexpéditeur de service « Appel vers Lenovo par défaut ».
   a. Cliquez sur **Réexpéditeur de service** dans la navigation de gauche pour afficher la page Réexpéditeurs de service.
   b. Sélectionnez **Activer** dans la colonne **État** du réexpéditeur de service « Appel vers Lenovo par défaut ».
   c. Sélectionnez le réexpéditeur de service « Appel vers Lenovo par défaut », puis cliquez sur **Tester les réexpéditeurs de service** pour générer un événement de test pour le réexpéditeur de service et vérifier que XClarity Administrator peut communiquer avec Support Lenovo Center.

      Vous pouvez surveiller la progression du test en cliquant sur **Surveillance → Travaux** dans la barre de menus XClarity Administrator.

      Remarque : Le réexpéditeur de service doit être activé pour pouvoir être testé

- Configurez l'Appel vers Lenovo pour des appareils gérés spécifiques :
  1. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Service et support**.
  2. Cliquez sur **Réexpéditeurs de service** dans la navigation de gauche pour afficher la page Réexpéditeurs de service.
  3. Cliquez sur l'icône **Créer un réexpéditeur de service** ( ) pour afficher la boîte de dialogue Nouveau réexpéditeur de service.
  4. Cliquez sur l'onglet **General**.



   a. Sélectionnez **Appel vers Lenovo** comme réexpéditeur de service :
   b. Entrez le nom du réexpéditeur de service ainsi qu'une description.
   c. Indiquez le nombre de tentatives de notification automatique. La valeur par défaut est 2.
   d. Indiquez le nombre minimal de minutes entre les tentatives. La valeur par défaut est 2.

e. (Facultatif) Cliquez sur **Nécessite la vérification des données de maintenance** si vous souhaitez inspecter les fichiers de données de maintenance avant leur transfert, et indiquer éventuellement l'adresse électronique du contact à notifier lorsque les fichiers de données de maintenance doivent être inspectés.

5. Cliquez sur l'onglet **Spécifique**, puis indiquez les informations de contact et les informations système.

   Astuce : Pour utiliser les mêmes informations de contact et d'emplacement que celles configurées sur la page Configuration de l'appel vers Lenovo, sélectionnez **Configuration générale** dans le menu déroulant **Configuration**.

6. Cliquez sur l'onglet **Appareils** et sélectionnez les appareils gérés et les groupes de ressources pour lesquels vous souhaitez que ce réexpéditeur de service transfère les fichiers de maintenance.

   Astuce : Pour acheminer des fichiers de maintenance pour tous les appareils gérés (actuels et ultérieurs), cochez la case **Faire correspondre tous les appareils**.

7. Cliquez sur **Créer**. Le réexpéditeur de service est ajouté à la page Service et support.
8. Sur la page Réexpéditeurs de service, sélectionnez **Activer** dans la colonne **État** pour activer le réexpéditeur de service.
9. Sélectionnez le réexpéditeur de service et cliquez sur **Tester les réexpéditeurs de service** pour générer un événement de test pour le réexpéditeur de service et vérifier que XClarity Administrator peut communiquer avec Support Lenovo Center.

   Vous pouvez surveiller la progression du test en cliquant sur **Surveillance → Travaux** dans la barre de menus XClarity Administrator.

   Remarque : Le réexpéditeur de service doit être activé pour pouvoir être testé.

Après avoir terminé

Sur la page Service et support, vous pouvez également exécuter les actions suivantes :

- Si l'option **Nécessite la vérification des données de maintenance** est sélectionnée et qu'un événement réparable a été reçu de l'un des appareils gérés associés au réexpéditeur de service, vous devez inspecter les fichiers de maintenance avant qu'ils ne soient transférés au prestataire de services. Pour plus d'informations, voir Transfert de fichiers de diagnostic au support Lenovo dans la documentation en ligne de XClarity Administrator.
- Déterminez si Appel vers Lenovo est activé ou désactivé sur un appareil géré en cliquant sur **Actions de nœud final** dans la navigation de gauche et en vérifiant l'état dans la colonne **Appel vers Lenovo État**.

  Astuce Si « État inconnu » s'affiche dans la colonne **Appel vers LenovoEtat**, actualisez le navigateur Web pour afficher l'état correct.
- Définissez les informations de contact de support et d'emplacement pour un appareil géré spécifique en cliquant sur **Actions de nœud final** dans la navigation de gauche, puis en cliquant sur l'icône **Créer un profil de contact** ( ) ou l'icône **Éditer le profil de contact** ( ). Les informations de contact et d'emplacement pour l'appareil géré sont incluses dans le ticket de maintenance que Appel vers Lenovo envoie au Lenovo Centre de support. Si des informations de contact et d'emplacement uniques sont spécifiées pour un appareil géré, ces informations sont incluses dans le ticket de maintenance. Sinon, les informations générales spécifiées pour la configuration de XClarity Administrator Appel vers Lenovo (sur la page **Appel vers Lenovo Configuration** ou la page **Réexpéditeurs de service**) sont utilisées. Pour plus d'informations, voir Lenovo Centre de support. Pour plus d'informations, voir Définition des contacts de support pour un appareil dans la documentation en ligne de XClarity Administrator.
- Affichez les tickets de maintenance qui ont été envoyés au Lenovo Centre de support en cliquant sur **État du ticket de maintenance** dans la navigation de gauche. Cette page répertorie les tickets de

maintenance qui ont été ouverts automatiquement ou manuellement par un réexpéditeur de service de l'Appel vers Lenovo, l'état et les fichiers de maintenance qui ont été transmis au Lenovo Centre de support. Pour plus d'informations, voir Affichage des tickets de maintenance et de l'état dans la documentation en ligne de XClarity Administrator.

- Collectez des données de maintenance pour un appareil spécifique en cliquant sur **Actions de nœud final** dans la navigation de gauche, puis en cliquant sur l'icône **Collecter les données de maintenance** (). Pour plus d'informations, voir Collecte et téléchargement de fichiers de diagnostic pour un dispositif dans la documentation en ligne de XClarity Administrator.
- Ouvrez manuellement un ticket de maintenance dans le Lenovo Centre de support, collectez les données de maintenance pour un appareil spécifique, et envoyez ces fichiers au Lenovo Centre de support en cliquant sur **Actions de nœud final** dans la navigation de gauche, puis en cliquant sur **Toutes les actions → Effectuer un Appel vers Lenovo**.Si Lenovo Centre de support requiert des informations supplémentaires, Lenovo Support peut vous demander de collecter à nouveau des données de maintenance pour cet appareil ou un autre.

  Pour plus d'informations, voir Ouverture d'un ticket de maintenance dans la documentation en ligne de XClarity Administrator.
- Réactivez Appel vers Lenovo sur tous les appareils gérés en cliquant sur **Actions de nœud final** dans la navigation de gauche, puis en cliquant sur **Toutes les actions → Activer Appel vers Lenovo sur tous les appareils**.

  Lorsque vous activez un Appel vers Lenovo réexpéditeur de service dans Lenovo XClarity Administrator, Appel vers Lenovo est désactivé sur chaque appareil géré afin d'éviter de générer des enregistrements de problème en double. Si vous prévoyez de cesser d'utiliser XClarity Administrator pour gérer vos appareils ou de désactiver la fonction Appel vers Lenovo dans XClarity Administrator, vous pourrez ultérieurement réactiver la fonction Appel vers Lenovo sur tous les appareils gérés à partir de XClarity Administrator au lieu de réactiver la fonction Appel vers Lenovo pour chaque appareil géré ultérieurement.

  Pour plus d'informations, voir Réactivation de l'appel vers Lenovo sur tous les appareils gérés dans la documentation en ligne de XClarity Administrator.

Configuration de la notification de problème automatique pour un prestataire de services préféré

Vous pouvez configurer Lenovo XClarity Administrator pour envoyer automatiquement des fichiers de diagnostic d'un ensemble spécifique d'appareils gérés à votre prestataire de services préféré (notamment le support Lenovo à l'aide de l'Appel vers Lenovo) lorsque certains événements réparables sont reçus d'appareils gérés (par exemple une erreur de mémoire irrécupérable) afin que le problème puisse être résolu.

Avant de commencer

Attention : Vous devez accepter le document suivant : Déclaration de confidentialité de Lenovo pour pouvoir transférer des données au support Lenovo.

Assurez-vous que tous les ports requis par XClarity Administrator (y compris les ports requis pour l'appel vers Lenovo) sont disponibles avant de configurer un réexpéditeur de service. Pour plus d'informations sur les ports, voir Disponibilité de port dans la documentation en ligne de XClarity Administrator.

Vérifiez qu'il existe une connexion aux adresses Internet qui sont requises par le prestataire de services.

Si vous choisissez d'utiliser Lenovo Support, vérifiez qu'il existe une connexion aux adresses Internet qui sont requises par l'Appel vers Lenovo. Pour plus d'informations sur les pare-feu, voir Pare-feux et serveurs proxy dans la documentation en ligne de XClarity Administrator.

Si XClarity Administrator accède à Internet via un proxy HTTP, vérifiez que le serveur proxy est configuré en tant que proxy sans arrêt. Pour plus d'informations sur la configuration du proxy, voir Configuration de l'accès réseau Configuration de l'accès réseau dans la documentation en ligne de XClarity Administrator.

À propos de cette tâche

Un *réexpéditeur de service* définit des informations sur l'endroit auquel envoyer les fichiers de données de maintenance lorsqu'un événement réparable se produit. Vous pouvez définir jusqu'à 50 réexpéditeurs de service.

Pour chaque réexpéditeur de service, vous pouvez choisir de transférer automatiquement les données de maintenance au support Lenovo (appelé *Appel vers Lenovo*), à la fonction de téléchargement Lenovo ou à un autre prestataire de services à l'aide de SFTP. Pour plus d'informations sur la configuration d'un réexpéditeur de service pour Appel vers Lenovo, voir Configuration de la notification automatique de problème à l'Lenovo Support (Appel vers Lenovo) et Configuration de la notification de problème automatique pour un prestataire de services préféré. Pour plus d'informations sur la configuration d'un réexpéditeur de service pour la fonction de téléchargement Lenovo, voir Configuration de la notification automatique de problèmes à la fonction de téléchargement Lenovo dans la documentation en ligne de XClarity Administrator.

Si un réexpéditeur de service est configuré et activé pour le SFTP, XClarity Administrator transfère *automatiquement* les fichiers de données de maintenance au site SFTP spécifié pour votre prestataire de services préféré.

Pour les serveurs équipés de XCC2, XClarity Administrator enregistre les données de maintenance dans deux fichiers dans le référentiel.

- **Fichier de maintenance**. (.zip) Ce fichier contient les informations de maintenance et d'inventaire dans un format aisément lisible. Ce fichier est automatiquement envoyé à votre prestataire de services préféré lorsqu'un événement réparable se produit.
- **Fichier de débogage**. (.tzz) Ce fichier contient toutes les informations de maintenance, l'inventaire et les journaux de débogage utilisables par le support Lenovo. Vous pouvez envoyer manuellement ce fichier au support Lenovo si des informations supplémentaires sont nécessaires pour résoudre un problème.

Pour les autres appareils, XClarity Administrator enregistre les données de maintenance (y compris les informations de maintenance, l'inventaire et les journaux de débogage) dans un fichier de maintenance unique dans le référentiel. Ce fichier est envoyé à votre prestataire de services préféré lorsqu'un événement réparable se produit.

Remarque : Si plusieurs réexpéditeurs de service SFTP sont configurés pour le même appareil, seul l'un d'entre eux transfère des données de maintenance. L'adresse et le port utilisés dépendent du réexpéditeur de service déclenché en premier.

Procédure

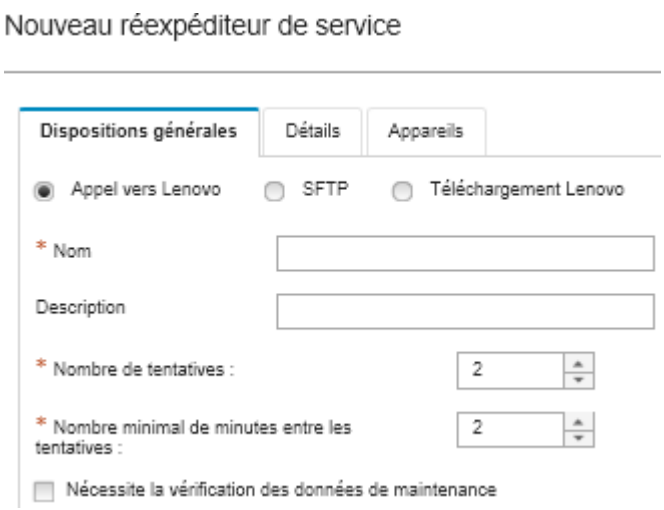
Procédez comme suit pour définir et activer un réexpéditeur de service.

Etape 1. Dans la barre de menus de XClarity Administratorcliquez sur **Administration → Service et support**. La page Service et support s'affiche.

Etape 2. Cliquez sur **Réexpéditeurs de service** dans la navigation de gauche pour afficher la page Réexpéditeurs de service.

Etape 3. Cliquez sur l'icône **Créer un réexpéditeur de service** ( ) pour afficher la boîte de dialogue Nouveau réexpéditeur de service.

Etape 4. Cliquez sur l'onglet **General**.



1. Sélectionnez **SFTP** comme réexpéditeur de service :
2. Entrez le nom du réexpéditeur de service ainsi qu'une description.
3. Indiquez le nombre de tentatives de notification automatique. La valeur par défaut est 2.
4. Indiquez le nombre minimal de minutes entre les tentatives. La valeur par défaut est 2.
5. (Facultatif) Cliquez sur **Nécessite la vérification des données de maintenance** si vous souhaitez inspecter les fichiers de maintenance avant leur transfert, et indiquer éventuellement l'adresse électronique du contact à notifier lorsque les fichiers de données de maintenance doivent être inspectés.

Etape 5. Cliquez sur l'onglet **Spécifique**, puis indiquez les informations suivantes :
- Adresse IP et numéro de port du serveur SFTP
- ID utilisateur et mot de passe pour l'authentification au serveur SFTP

Etape 6. Cliquez sur l'onglet **Appareil** et sélectionnez les appareils gérés et les groupes de ressources pour lesquels vous souhaitez que ce réexpéditeur de service transfère les données de maintenance.

Astuce : Pour acheminer des données de maintenance pour tous les appareils gérés (actuels et ultérieurs), cochez la case **Faire correspondre tous les appareils**.

Etape 7. Cliquez sur **Créer**. Le réexpéditeur de service est ajouté à la page Service et support

Etape 8. Sur la page Service et support, sélectionnez **Activer** dans la colonne **État** pour activer le réexpéditeur de service.

Etape 9. Pour empêcher les événements réparables qui figurent dans la liste des événements exclus d'ouvrir automatiquement des rapports d'incidents, sélectionnez **Non** à la question **Voulez-vous que des événements exclus ouvrent des rapports d'incidents ?**.

Etape 10. Sélectionnez le réexpéditeur de service et cliquez sur **Tester les réexpéditeurs de service** pour générer un événement de test pour le réexpéditeur de service et vérifier que XClarity Administrator peut communiquer avec le prestataire de services.

Remarque : Le réexpéditeur de service doit être activé pour pouvoir être testé.

Après avoir terminé

Sur la page Service et support, vous pouvez également exécuter les actions suivantes :

- Si l'option **Nécessite la vérification des données de maintenance** est sélectionnée et qu'un événement réparable a été reçu de l'un des appareils gérés associés au réexpéditeur de service, vous devez inspecter et gérer les fichiers avant qu'ils ne soient transférés au prestataire de services. Pour plus

d'informations, voir Examen de fichiers de diagnostic dans la documentation en ligne de XClarity Administrator.

- Modifiez les informations du réexpéditeur de service en cliquant sur **Réexpéditeurs de service** dans la navigation de gauche et en cliquant sur l'icône **Modifier le réexpéditeur de service** ( ).
- Activez ou désactivez un prestataire de services en cliquant sur **Réexpéditeurs de service** et en sélectionnant **Activer** ou **Désactiver** dans la colonne **État**.
- Supprimez le prestataire de services en cliquant sur **Réexpéditeurs de service** et en cliquant sur l'icône **Supprimer le réexpéditeur de service** ( ).
- Définissez les informations de contact de support et d'emplacement pour un appareil géré spécifique en cliquant sur **Actions de nœud final** dans la navigation de gauche, puis en cliquant sur l'icône **Créer un profil de contact** ( ) ou l'icône **Éditer le profil de contact** ( ). Les informations de contact et d'emplacement pour l'appareil géré sont incluses dans l'enregistrement de problème que l'appel vers Lenovo crée dans le Lenovo Centre de support. Si des informations de contact et d'emplacement uniques sont spécifiées pour un appareil géré, ces informations sont incluses dans l'enregistrement de problème. Sinon, les informations générales spécifiées pour la configuration de l'appel vers Lenovo de XClarity Administrator (sur la page **Configuration de l'appel vers Lenovo** ou sur la page **Réexpéditeurs de service**) sont utilisées. Pour plus d'informations, voir Définition des contacts de support pour un appareil dans la documentation en ligne de XClarity Administrator.
- Collectez des données de maintenance pour un appareil spécifique en cliquant sur **Actions de nœud final**, en sélectionnant l'appareil, puis en cliquant sur l'icône **Collecter les données de maintenance** ( ). Pour plus d'informations, voir Collecte et téléchargement de fichiers de diagnostic pour un dispositif dans la documentation en ligne de XClarity Administrator.

Pour plus d'informations sur ces tâches de service et support, voir Utilisation du service et support dans la documentation en ligne de XClarity Administrator.

Connexion de XClarity Administrator en tant que concentrateur au portail TruScale

Vous pouvez connecter Lenovo XClarity Administrator en tant que concentrateur de gestion au portail Lenovo TruScale.

Avant de commencer

Attention : Ces étapes de configuration sont destinées uniquement aux représentants de service Lenovo.

Procédure

Procédez comme suit pour connecter XClarity Administrator au portail TruScale.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Configuration du concentrateur** pour afficher la page Configuration du concentrateur.

Etape 2. Créez une clé d'inscription en cliquant sur **Générer une demande d'inscription**. La boîte de dialogue Générer une demande d'inscription s'affiche.

Etape 3. Cliquez sur **Copier dans le presse-papiers** pour copier la clé d'inscription, puis fermez la boîte de dialogue.

Etape 4. Cliquez sur **Installer une clé d'inscription** pour afficher la boîte de dialogue Installer une clé d'inscription.

Etape 5. Collez la clé d'inscription dans la zone **Clé d'inscription**.

Etape 6. Cliquez sur **Soumettre**.

Après avoir terminé

Vous pouvez désinstaller la clé d'inscription en cliquant sur **Réinitialiser la configuration**.

Sauvegarde, restauration et migration des données des paramètres système

Vous pouvez utiliser Lenovo XClarity Administrator pour sauvegarder et restaurer les données et paramètres système, ainsi que les fichiers importés, tels que des images du système d'exploitation, des mises à jour de microprogramme et des pilotes de périphérique SE.

Sauvegarde de Lenovo XClarity Administrator

Si vous avez déjà des procédures de sauvegarde mises en place pour les hôtes virtuels, vérifiez qu'elles incluent Lenovo XClarity Administrator.

Avant de commencer

Attention : Vérifiez que vous informez tous les utilisateurs actifs avant de lancer la procédure de sauvegarde. XClarity Administrator est mis au repos lors de la procédure pour empêcher la modification des données. Par conséquent, vous ne pouvez pas accéder à XClarity Administrator pendant l'exécution de la procédure de sauvegarde.

Vérifiez que le certificat d'autorité de certification a été téléchargé depuis le dispositif virtuel XClarity Administrator et importé dans votre navigateur Web (voir Importation du certificat de l'autorité de certification dans un navigateur Web).

Vérifiez que tous les travaux en cours d'exécution sont terminés, et qu'il n'existe pas de travaux en cours. Si des travaux sont en cours d'exécution, vous pouvez choisir d'arrêter les travaux en cours d'exécution et de poursuivre la création de la sauvegarde.

Assurez-vous que les serveurs DNS sont correctement configurés, sinon il se peut que SMTP et NTP ne fonctionnent pas correctement une fois la sauvegarde restaurée.

Vérifiez qu'il y a suffisamment d'espace disque sur le serveur de gestion pour la sauvegarde. Sinon, libérez de l'espace disque en supprimant des ressources, XClarity Administrator y compris des sauvegardes précédentes, qui ne sont plus nécessaires (voir Gestion de l'espace disque, ou créez une nouvelle sauvegarde sans inclure les images de système d'exploitation, les mises à jour du microprogramme et les pilotes de périphérique SE.

Assurez-vous que le déploiement du SE est configuré sur l'interface réseau appropriée, eth1 ou eth0, si vous souhaitez sauvegarder des images du SE (voir Configuration de l'accès réseau).

À propos de cette tâche

Sauvegardez toujours XClarity Administrator après avoir effectué la configuration initiale et après avoir apporté des modifications de configuration importantes, notamment :
- Avant de mettre à jour XClarity Administrator
- Lorsque vous gérez de nouveaux châssis ou de nouveaux serveurs rack
- Lorsque vous ajoutez des utilisateurs à XClarity Administrator
- Lorsque vous créez et déployez de nouveaux modèles de configuration

Assurez-vous de sauvegarder XClarity Administrator régulièrement.

Il est recommandé de télécharger les sauvegardes sur votre système local. Si le système d'exploitation hôte s'arrête inopinément, vous risquez de ne pas pouvoir vous authentifier auprès de XClarity Administrator après le redémarrage du système d'exploitation hôte. Pour résoudre ce problème, restaurez XClarity Administrator à partir de la dernière sauvegarde sur votre système local (voir Restauration de Lenovo XClarity Administrator).

Procédure

Procédez comme suit pour sauvegarder XClarity Administrator.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Sauvegarder et restaurer les données**. La page Sauvegarder et restaurer les données s'affiche.

Etape 2. Cliquez sur l'icône **Sauvegarder** (). La boîte de dialogue Sauvegarder et restaurer les données s'affiche.

Etape 3. Entrez une description pour cette sauvegarde.

Etape 4. Choisissez l'emplacement où créer la sauvegarde. Il peut s'agir du référentiel local ou d'un partage distant.

La sauvegarde est créée dans le référentiel local par défaut. Vous pouvez copier une sauvegarde à partir du référentiel local sur un partage distant en cliquant sur l'icône **Copier sauvegarde** ().

Si vous choisissez un partage distant, la sauvegarde est d'abord créée dans le référentiel local. Ensuite, la sauvegarde est copiée sur le partage distant sélectionné et la copie locale est supprimée. Pour plus d'informations, voir Gestion de partages distants.

Etape 5. Choisissez éventuellement d'inclure des images du système d'exploitation, les mises à jour de microprogramme, et des pilotes de périphérique SE.

Etape 6. Spécifiez l'expression de passe de chiffrement pour la sauvegarde.

Attention : Notez l'expression de passe de chiffrement. L'expression de passe est nécessaire pour restaurer la sauvegarde sur cette instance ou sur une autre instance de XClarity Administrator. Si vous oubliez l'expression de passe, il n'est pas possible de la récupérer.

Etape 7. Cliquez sur **Sauvegarder** pour sauvegarder les données et les paramètres immédiatement, ou cliquez sur **Planning** afin de planifier cette sauvegarde à une période ultérieure.

Attention : Si vous choisissez d'effectuer une sauvegarde immédiatement, ne fermez ni n'actualisez le navigateur Web ou la fenêtre avant que le processus ne soit terminé Sinon, la sauvegarde peut ne pas être générée.

La génération de la sauvegarde peut durer un moment. Une barre de progression affiche l'état du travail.

Si vous avez choisi de créer la sauvegarde sur un partage distant, vous pouvez surveiller la progression depuis la page Travaux (voir Surveillance des travaux).

Si vous planifiez une sauvegarde, le serveur de gestion est arrêté temporairement pendant le processus de sauvegarde. Dès que le serveur de gestion est de nouveau en ligne, vous pouvez surveiller l'état du processus de sauvegarde à partir de la page Travaux.

Etape 8. Connectez-vous à XClarity Administrator pour continuer à gérer vos appareils.

Après avoir terminé

Depuis la page Sauvegarder et restaurer les données, vous pouvez effectuer les actions suivantes :

- Copiez des sauvegardes XClarity Administrator vers ou depuis un partage distant en cliquant sur l'icône **Copie sauvegarde** ().
- Supprimez des sauvegardes sélectionnées du référentiel local ou de partages distants qui ne sont plus nécessaires en cliquant sur l'icône **Supprimer la sauvegarde** ().
- Restaurer des données et des paramètre système sur ce serveur de gestion (voir Restauration de Lenovo XClarity Administrator).
- Importer et exporter des sauvegardes à partir du système local en cliquant sur l'icône **Importer la sauvegarde** () ou sur l'icône **Exporter la sauvegarde** (), respectivement.
- Envoyez la sauvegarde sélectionnée vers une nouvelle instance de XClarity Administrator (voir Migration des données du système et paramètres vers une autre instance de XClarity Administrator).

Restauration de Lenovo XClarity Administrator

Vous pouvez utiliser les paramètres et les données sauvegardées pour restaurer Lenovo XClarity Administrator à un état antérieur.

Avant de commencer

Attention : Vérifiez que vous informez tous les utilisateurs actifs avant de lancer la procédure de sauvegarde. XClarity Administrator est mis au repos lors de la procédure pour empêcher la modification des données. Par conséquent, vous ne pouvez pas accéder à XClarity Administrator pendant l'exécution de la procédure de sauvegarde

Téléchargez le certificat d'autorité de certification depuis le dispositif virtuel XClarity Administrator et importez le certificat dans votre navigateur Web (voir Importation du certificat de l'autorité de certification dans un navigateur Web).

Vérifiez que tous les travaux en cours d'exécution sont terminés, et qu'il n'existe pas de travaux en cours.

Vous pouvez restaurer une sauvegarde uniquement vers la même version de XClarity Administrator que celle utilisée pour créer la sauvegarde.

À propos de cette tâche

Attention :

- Toutes les modifications apportées depuis la création de la sauvegarde seront perdues.
- Pour restaurer les données, le dispositif virtuel est réinitialisé à son état d'origine. Tous les paramètres en cours, l'inventaire des dispositifs et les fichiers (images du système d'exploitation, mises à jour de microprogramme, et les pilotes de périphérique SE) sont supprimés avant la restauration des données de la sauvegarde. Les données et paramètres de la sauvegarde ne sont pas mélangés avec les données et paramètres en cours du dispositif virtuel. Si vous choisissez de ne pas restaurer l'inventaire des dispositifs, les images de système d'exploitation, les mises à jour de microprogramme et les pilotes de périphérique SE, seules les données par défaut de XClarity Administrator sont présentes une fois la restauration terminée.

La restauration d'une sauvegarde ne supprime pas les sauvegardes de l'instance de XClarity Administrator.

La restauration d'une sauvegarde ne modifie pas les données ou les paramètres sur les appareils gérés. Par exemple, si vous annulez la gestion d'un appareil puis restaurez une sauvegarde précédente alors que l'appareil était encore géré sur XClarity Administrator, vous rencontrerez peut-être des problèmes de connectivité à cet appareil une fois la restauration terminée. De même, si vous gérez un appareil puis restaurez une sauvegarde précédente alors que l'appareil n'était pas encore géré, vous devrez peut-être

modifier manuellement la configuration de l'appareil pour annuler l'état géré, ou utiliser l'option **Force** lorsque vous tenterez de gérer XClarity Administrator à nouveau.

Procédure

Procédez comme suit pour restaurer XClarity Administrator.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Sauvegarder et restaurer les données**. La page Sauvegarder et restaurer les données s'affiche.

Etape 2. Si vous avez exporté le module de sauvegarde sur votre système local puis l'avez supprimé de XClarity Administrator, procédez comme suit.

a. Depuis la page Sauvegarder et restaurer les données, cliquez sur l'icône **Importer la sauvegarde** () pour afficher la boîte de dialogue Importer la sauvegarde.

b. Cliquez sur **Parcourir** pour trouver la sauvegarde que vous avez exporté depuis une instance de XClarity Administrator.

c. Cliquez sur **Importer** pour télécharger la sauvegarde vers XClarity Administrator.

L'importation de la sauvegarde peut durer un moment. Une barre de progression affiche l'état du travail.

Attention : Si vous fermez ou actualisez l'onglet du navigateur Web ou la fenêtre avant que le chargement ne soit terminé, le processus pourrait échouer.

d. Une fois l'importation terminée, indiquez l'expression de passe de chiffrement pour la sauvegarde.

Remarque : Si vous ne connaissez pas l'expression de passe de chiffrement, vous devez créer une nouvelle sauvegarde sur la version source de XClarity Administrator (voir Sauvegarde de Lenovo XClarity Administrator).

Etape 3. Sélectionnez la sauvegarde à restaurer, puis cliquez sur l'icône **Restaurer la sauvegarde** (). La boîte de dialogue Restaurer les données s'affiche.

Etape 4. Spécifiez l'expression de passe de chiffrement pour la sauvegarde.

Etape 5. Cliquez sur **Confirmer**.

Etape 6. Dans la boîte de dialogue Confirmer la restauration des données, vérifiez que toutes les informations sont correctes.

Etape 7. Dans la boîte de dialogue Options de restauration, vous pouvez éventuellement choisir d'importer des images du système d'exploitation, des mises à jour de microprogramme, des pilotes de périphérique SE, des paramètres réseau et inventaire de dispositifs.

Attention : Lisez attentivement tous les avertissements qui sont affichés dans cette boîte de dialogue.

Etape 8. Cliquez sur **Confirmer** pour commencer la restauration de données.

La restauration des données et des paramètres peut être longue. Une barre de progression affiche l'état du travail.

Lorsque le processus de restauration est terminé, vous êtes redirigé vers la page de connexion.

Attention : Si vous fermez ou actualisez l'onglet du navigateur Web ou la fenêtre avant que le processus ne soit terminé, le processus pourrait échouer.

Etape 9. Connectez-vous à XClarity Administrator pour continuer à gérer vos appareils.

Migration des données du système et paramètres vers une autre instance de XClarity Administrator

Vous pouvez migrer les données et les paramètres système sauvegardés vers une nouvelle instance de Lenovo XClarity Administrator qui se trouve sur le même réseau ou sur un réseau différent.

Avant de commencer

Le serveur de gestion cible doit être une *nouvelle* instance XClarity Administrator avec la même version que le serveur de gestion utilisé pour créer la sauvegarde. Il doit être dans l'Assistant de configuration initiale, avec aucune étape terminée. Pour plus d'informations, voir Installation et configuration de XClarity Administrator dans la documentation en ligne de XClarity Administrator.

Vérifiez que vous informez tous les utilisateurs actifs avant de lancer la procédure de sauvegarde. XClarity Administrator est mis au repos lors de la procédure pour empêcher la modification des données. Par conséquent, vous ne pouvez pas accéder à XClarity Administrator pendant l'exécution de la procédure de sauvegarde.

Téléchargez le certificat d'autorité de certification depuis XClarity Administrator et importez le certificat dans votre navigateur Web (voir Gestion de l'espace disque dans la documentation en ligne de XClarity Administrator).

Les sauvegardes dans le référentiel de sauvegarde du serveur de gestion source ne sont pas migrées vers le serveur de gestion cible. Avant de migrer des données et des paramètres, exportez les sauvegardes dont vous pouvez avoir besoin sur votre système local.

À propos de cette tâche

Les modifications apportées sur le serveur de gestion source après création de la sauvegarde ne sont pas migrées vers le serveur de gestion cible.

La restauration d'une sauvegarde ne modifie pas les données ou les paramètres sur les appareils gérés. Par exemple, si vous annulez la gestion d'un appareil puis restaurez une sauvegarde précédente alors que l'appareil était encore géré sur XClarity Administrator, vous rencontrerez peut-être des problèmes de connectivité à cet appareil une fois la restauration terminée. De même, si vous gérez un appareil puis restaurez une sauvegarde précédente alors que l'appareil n'était pas encore géré, vous devrez peut-être modifier manuellement la configuration de l'appareil pour annuler l'état géré, ou utiliser l'option **Force** lorsque vous tenterez de gérer XClarity Administrator à nouveau.

Remarques : Lors de l'exécution de XClarity Administrator en tant que conteneur, les volumes créés sur l'hôte pour ce conteneur peuvent être utilisés comme volumes pour un autre conteneur. Une fois les volumes liés au nouveau conteneur (cible), ils ne peuvent plus être utilisés par le conteneur initial (source).

1. Configuration du fichier `docker-compose.yml` pour le conteneur cible en vue d'utiliser la même adresse IP et le nom de conteneur du conteneur source.
2. Arrêtez le conteneur source à l'aide de la commande suivante.
   `docker-compose -p ${CONTAINER_NAME} down`
3. Démarrez le conteneur cible à l'aide de la commande suivante, <*env_filename*> étant le nom du fichier des variables d'environnement. Une fois le conteneur cible démarré, les volumes sont liés au conteneur XClarity Administrator cible. XClarity Administrator utilise les données système et les paramètres de ces volumes.
   COMPOSE_HTTP_TIMEOUT=300 `docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d`

Procédure

Procédez comme suit pour restaurer XClarity Administrator.

Etape 1. Si les versions source et cible de XClarity Administrator se trouvent sur le même réseau, procédez comme suit.

a. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Sauvegarder et restaurer les données**. La page Sauvegarder et restaurer les données s'affiche.

b. Cliquez sur l'icône **Envoyer la sauvegarde** () pour afficher la boîte de dialogue Envoyer les données.

c. Entrez l'adresse IP actuelle de la version cible de XClarity Administrator.

d. Cliquez sur **Continuer** pour télécharger la sauvegarde vers la version cible de XClarity Administrator.

Le téléchargement de la sauvegarde peut durer un moment. Une barre de progression affiche l'état du travail.

Attention : Si vous fermez ou actualisez l'onglet du navigateur Web ou la fenêtre avant que le téléchargement ne soit terminé, le module peut ne pas être téléchargé.

Etape 2. Si les versions source et cible de XClarity Administrator ne se trouvent *pas* sur le même réseau, procédez comme suit

a. Dans la barre de menus de la version source de XClarity Administrator, cliquez sur **Administration → Sauvegarder et restaurer les données**. Dans la page Sauvegarder et restaurer les données, cliquez sur l'icône **Exporter la sauvegarde** () pour exporter la sauvegarde sur le système local.

L'exportation de la sauvegarde peut durer un moment.

b. Copiez la sauvegarde exportée à partir du serveur de gestion source sur un système dans le même réseau que le serveur de gestion cible

c. Depuis la page de l'assistant sur la version cible de XClarity Administrator, cliquez sur l'icône **Importer la sauvegarde** () pour afficher la boîte de dialogue Importer le module de données.

d. Cliquez sur **Parcourir** pour trouver la sauvegarde que vous avez exporté depuis la version source de XClarity Administrator.

e. Cliquez sur **Charger** pour importer la sauvegarde vers la version cible de XClarity Administrator.

L'importation de la sauvegarde peut durer un moment. Une barre de progression affiche l'état du travail.

Attention : Si vous fermez ou actualisez l'onglet du navigateur Web ou la fenêtre avant que le chargement ne soit terminé, le processus pourrait échouer.

Etape 3. Une fois l'importation terminée, indiquez l'expression de passe de chiffrement pour la sauvegarde.

Remarque : Si vous ne connaissez pas l'expression de passe de chiffrement, vous devez créer une nouvelle sauvegarde sur la version source de XClarity Administrator (voir Sauvegarde de Lenovo XClarity Administrator.

Etape 4. Dans la boîte de dialogue Confirmation de la restauration des données, vérifiez que toutes les informations sont correctes.

Etape 5. Cliquez sur **Confirmer** pour lancer le chargement des données et paramètres système.

Etape 6. Dans la boîte de dialogue Options de restauration, vous pouvez éventuellement choisir d'importer des images du système d'exploitation, des mises à jour de microprogramme, des pilotes de périphérique SE, des paramètres réseau et inventaire de dispositifs.

Attention : Lisez attentivement tous les avertissements qui sont affichés dans cette boîte de dialogue.

Etape 7. Si vous avez choisi d'importer les paramètres réseau ou l'inventaire des dispositifs, arrêter le serveur de gestion source depuis la version source de XClarity Administrator en cliquant sur **Administration → Arrêter le serveur de gestion → Arrêter**.

Confirmez que le dispositif virtuel source est arrêté avant de continuer

Etape 8. Sur la version cible de XClarity Administrator, cliquez sur **Confirmer** pour lancer le chargement des données et des paramètres depuis le module

Si vous avez choisi d'importer les paramètres réseau, une fois la migration terminée, les adresses IP de la version source de XClarity Administrator sont réaffectées à la version cible de XClarity Administrator.

Attention : Si la version source de XClarity Administrator utilise le protocole DHCP, vous devez établir une liaison entre les adresses MAC de la version cible de XClarity Administrator et les adresses IP de la version source correspondante de XClarity Administrator sur le serveur DHCP. Patientez au moins 15 minutes après la modification du serveur DHCP avant de continuer.

Etape 9. Attendez que la barre de progression de chargement des données et des paramètres du module soit terminée.

Lorsque la migration des données est terminée, vous êtes redirigé vers la page de connexion.

Attention : Si vous fermez ou actualisez l'onglet du navigateur Web ou la fenêtre avant que le chargement ne soit terminé, le processus pourrait échouer.

Etape 10. Connectez-vous à la version cible de XClarity Administrator pour continuer à gérer vos appareils.

Gestion de l'espace disque

Vous pouvez gérer la quantité d'espace disque qui est utilisée par Lenovo XClarity Administrator en déplaçant des fichiers de données volumineux qui ne sont pas immédiatement nécessaires vers un partage distant ou en supprimant des ressources qui ne sont plus nécessaires.

À propos de cette tâche

Pour déterminer la quantité d'espace disque actuellement utilisée, cliquez sur **Tableau de bord** dans la barre de menus de XClarity Administrator. L'utilisation de l'espace disque sur le référentiel et les partages distants est répertoriée dans la section Activité de XClarity Administrator.

Procédure

Effectuez une ou plusieurs des étapes suivantes pour libérer de l'espace disque en déplaçant les fichiers sur un partage distant et en supprimant les ressources non nécessaires.

- **Supprimer des ressources non nécessaires**

  Vous pouvez rapidement supprimer des fichiers du référentiel local qui ne sont plus nécessaires en procédant comme suit.

  1. Dans la barre de menus XClarity Administrator, cliquez sur **Administration → Nettoyage de disque** pour afficher la page Nettoyage de disque.

2. Sélectionnez les fichiers que vous souhaitez supprimer. L'en-tête de section identifie la quantité d'espace qui sera libérée lorsque les fichiers seront supprimés.
   - **Fichiers du système d'exploitation**

     Vous pouvez supprimer des images SE, des fichiers d'options d'amorçage et des fichiers logiciels.
   - **Mises à jour du microprogramme**

     Vous pouvez supprimer des fichiers de contenu pour tous les pilotes de périphérique SE associés à des UpdateXpress System Packs (UXSPs) et des pilotes de périphérique individuels qui indiquent l'état Téléchargé.

     Vous pouvez aussi supprimer des fichiers de contenu pour les mises à jour de microprogramme individuelles indiquant l'état Téléchargé et qui ne sont pas utilisés dans une stratégie de conformité du microprogramme.

     Vous pouvez supprimer les fichiers de contenu des mises à jour du serveur de gestion qui sont à l'état Téléchargé.

     Remarque : Lorsque le référentiel des mises à jour de microprogramme se trouve sur un partage distant, vous ne pouvez pas utiliser la fonction de nettoyage de disque pour supprimer des mises à jour de microprogramme et des modules UXSP individuels.
   - **Fichiers de données de maintenance**

     Lorsqu'un événement de maintenance se produit sur un appareil, les données de maintenance sont collectées automatiquement pour cet appareil. Les données de maintenance sont automatiquement collectées pour le serveur de gestion, chaque fois qu'une exception se produit dans XClarity Administrator. Il est recommandé de supprimer régulièrement ces archives si XClarity Administrator et les appareils gérés s'exécutent normalement.

     Lorsque les mises à jour du serveur de gestion sont correctement appliqués, les fichiers de mise à jour sont automatiquement retirés du référentiel.
3. Cliquez sur **Supprimer la sélection**.
4. Consultez la liste des fichiers que vous avez sélectionnés, puis cliquez sur **Supprimer**.

- **Déplacer des modules de mise à jour de microprogramme vers un référentiel distant**

  By default, Lenovo XClarity Administrator utilise un référentiel local (interne) pour le stockage des mises à jour de microprogramme. Vous pouvez libérer de l'espace disque disponible pour le référentiel local XClarity Administrator à l'aide d'un partage distant monté sur un système de fichier SSH (SSHFS) comme référentiel distant. Vous pouvez ensuite utiliser des fichiers de mise à jour de microprogramme directement depuis le référentiel distant pour maintenir la conformité du microprogramme sur vos appareils. Pour plus d'informations, voir Utilisation d'un référentiel distant pour les mises à jour de microprogramme.

  Lorsque vous modifiez l'emplacement du référentiel des mises à jour de microprogramme, vous pouvez choisir de copier toutes les mises à jour de microprogramme depuis le référentiel d'origine vers le nouveau référentiel.

  Les fichiers de mise à jour de microprogramme du référentiel d'origine *ne sont pas* automatiquement effacés après la modification d'emplacements.

  Astuce : le référentiel des mises à jour distant peut être partagé par plusieurs serveurs de gestion XClarity Administrator.

  Procédez comme suit pour déplacer les mises à jour de microprogramme vers un référentiel des mises à jour de microprogramme distant.

  1. Ajoutez un partage distant à XClarity Administrator (voir Gestion de partages distants).

2. Dans la barre de menus XClarity Administrator, cliquez sur **Distribution → Mises à jour de microprogramme : référentiel**. La page Référentiel des mises à jour de microprogramme s'affiche.
3. Cliquez sur **Toutes les actions → Modifier l'emplacement du référentiel** pour afficher la boîte de dialogue Modifier l'emplacement du référentiel.
4. Sélectionnez le partage distant nouvellement créé depuis la liste déroulante **Emplacement du référentiel**.
5. Sélectionnez **Copier les modules de mise à jour du référentiel actuel vers le nouveau référentiel** pour copier les fichiers de mise à jour de microprogramme vers le nouvel emplacement du référentiel avant de modifier l'emplacement du référentiel.
6. Cliquez sur **OK**.

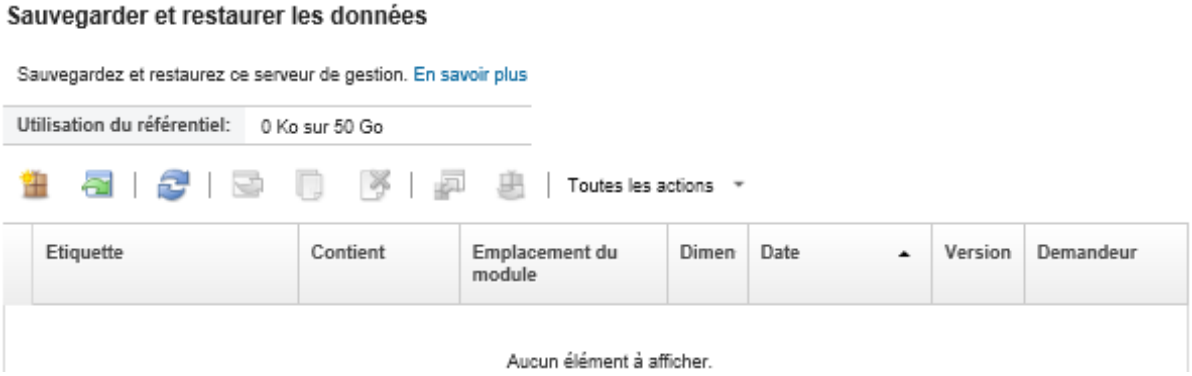
   Un travail est créé pour copier les modules de mise à jour de microprogramme vers le nouveau référentiel. Vous pouvez surveiller la progression du travail en cliquant sur **Surveillance → Travaux** dans la barre de menus XClarity Administrator.
7. Effacez les fichiers de mise à jour de microprogramme dans le référentiel local.
   a. Modifiez l'emplacement vers le référentiel local en cliquant sur **Toutes les actions → Modifier l'emplacement du référentiel**, sélectionnez **Référentiel local** pour l'emplacement du référentiel, puis cliquez sur **OK**.
   b. Cliquez sur l'onglet **Mises à jour individuelles**, cliquez sur la case Tout sélectionner dans le tableau pour sélectionner toutes les mises à jour de microprogramme. Enfin, cliquez sur l'icône **Supprimer entièrement les modules de mise à jour** ( )
   c. Cliquez sur l'onglet **UpdateXpress System Pack (UXSP)**, cochez la case Tout sélectionner du tableau pour sélectionner tous les modules UXSP, puis cliquez sur l'icône **Supprimer le module UXSP et la stratégie associée** ( )
   d. Modifiez l'emplacement de nouveau vers le référentiel distant en cliquant sur **Toutes les actions → Modifier l'emplacement du référentiel**, sélectionnez le nouveau référentiel distant pour l'emplacement du référentiel, puis cliquez sur **OK**.

- **Déplacez les sauvegardes XClarity Administrator vers un partage distant**

  Vous pouvez libérer de l'espace disque qui est disponible dans le référentiel local de XClarity Administrator en déplaçant des sauvegardes XClarity Administrator vers un partage distant. Toutefois, vous ne pouvez pas utiliser des fichiers directement sur le partage distant. Pour utiliser les fichiers, vous devez les déplacer vers le référentiel local XClarity Administrator. Pour plus d'informations sur partages distants, voir la section Gestion de partages distants.

  Important : Il est recommandé de télécharger les sauvegardes sur votre système local ou de copier les sauvegardes sur un partage distant avant de les supprimer dans XClarity Administrator.

  1. À partir de la barre de menus de XClarity Administrator, cliquez sur **Administration → Sauvegarder et restaurer les données** pour afficher la page Sauvegarder et restaurer les données.



La colonne **Emplacement de package** identifie si la sauvegarde est stockée, en local dans le référentiel local de XClarity Administrator ou sur un partage distant.

2. Sélectionnez la sauvegarde, puis cliquez sur l'icône **Copier la sauvegarde** ( ) pour afficher la boîte de dialogue Copier sauvegarde.
3. Choisissez le partage distant pour stocker la sauvegarde.
4. Cliquez sur **Copier**.
5. Surveiller la progression de la copie sur la page Travaux. Lorsque la copie est terminée, sélectionnez de nouveau la sauvegarde, puis cliquez sur l'icône **Supprimer la sauvegarde** ( ) pour afficher la boîte de dialogue Supprimer la sauvegarde.
6. Sélectionnez « Local » comme emplacement.
7. Cliquez sur **Supprimer**.

Gestion de partages distants

Vous pouvez monter partages distants et ensuite déplacer des fichiers plus volumineux, comme des sauvegardes Lenovo XClarity Administrator et des mises à jour de microprogramme, du référentiel local vers le partage distant pour gérer l'espace disque disponible pour le serveur de gestion.

Avant de commencer

Lors de l'exécution de XClarity Administrator en tant que conteneur, les partages distants sont montés sur le conteneur à l'aide du fichier yml lors de l'installation (voir Installation de XClarity Administrator dans les environnements basés sur VMware ESXi dans la documentation en ligne de XClarity Administrator).

Lors de l'exécution de XClarity Administrator en tant que dispositif virtuel, vous devez disposer de droits **lxc-supervisor** pour monter ou démonter un partage distant.

Vérifiez que vous disposez d'un réseau stable et rapide entre le serveur de fichier et XClarity Administrator.

Les partages distants ne sont pas pris en charge lors de l'exécution de XClarity Administrator en tant que conteneur.

À propos de cette tâche

Vous devez utiliser des partages distants distincts pour stocker les sauvegardes XClarity Administrator et les mises à jour de microprogramme.

Vous ne pouvez pas utiliser les fichiers de sauvegarde XClarity Administrator directement depuis le partage distant. Pour utiliser les fichiers de sauvegarde, vous devez les déplacer vers le référentiel local.

Actuellement, seul le système SSHFS est pris en charge.

Procédure

Pour ajouter un partage distant lors de l'exécution de XClarity Administrator en tant que dispositif virtuel, procédez comme suit.

1. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Partage distant**. La page Partage distant s'affiche.
2. Cliquez sur l'icône **Créer** ( ) pour créer un partage distant. La boîte de dialogue Créer un partage distant s'affiche.

3. Indiquez l’adresse IP du serveur fichier hébergeant le partage distant.
4. Indiquez les données d’identification stockées à utiliser pour accéder au partage distant.

   Astuce : Pour créer des données d'identification stockées, voir Gestion de données d'identification stockées.
5. Indiquez le point de montage (répertoire local) sur le serveur de gestion à utiliser pour le montage du partage distant.

   Important : Le chemin d'accès doit commencer par « /mnt ».
6. Indiquez le répertoire partagé (chemin de serveur distant) à monter comme partage distant sur le serveur de gestion.
7. Cliquez sur **Créer**.

Après avoir terminé

- Démontez le partage distant en sélectionnant le partage distant, puis en cliquant sur l’icône **Supprimer** ( ).
- Déplacez les fichiers de sauvegarde XClarity Administrator vers et depuis un partage distant (voir Gestion de l'espace disque).
- Configurez XClarity Administrator pour utiliser un partage distant comme référentiel des mises à jour de microprogramme (voir Utilisation d’un référentiel distant pour les mises à jour de microprogramme).

Modification de la langue de l'interface utilisateur

Vous pouvez modifier la langue de l'interface utilisateur une fois que vous êtes connecté.

Procédure

Dans la barre de titre de Lenovo XClarity Administrator, cliquez sur le menu d'action utilisateur (ADMIN_USER), puis cliquez sur **Modifier la langue**. Sélectionnez la langue que vous voulez afficher, puis cliquez sur **Fermer**.

Remarque : Le système d'aide s'affiche dans la langue définie dans l'interface utilisateur.

Arrêter XClarity Administrator

Lorsque Lenovo XClarity Administrator s'arrête, la connectivité à Lenovo XClarity Administrator est perdue.

Avant de commencer

Vous devez disposer des droits **lxc-supervisor** ou **lxc-admin** pour arrêter un dispositif virtuel XClarity Administrator.

Assurez-vous qu'aucun travail n'est en cours d'exécution. Tous les travaux en cours d'exécution ont été annulés lors du processus d'arrêt. Pour afficher le journal des travaux, consultez Surveillance des travaux.

Procédure

Procédez comme suit pour arrêter Lenovo XClarity Administrator.

- **Conteneurs**

  Exécutez les commandes ci-après pour arrêter le conteneur.

```
docker-compose -p ${CONTAINER_NAME} down
```

- **Dispositifs virtuels**
  1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Administration → Arrêter le serveur de gestion**.

     Une boîte de dialogue de confirmation est affichée avec une liste de travaux en cours d'exécution. Lorsque vous arrêtez XClarity Administrator, les travaux sont arrêtés.
  2. Cliquez sur **Arrêter**.

Après avoir terminé

Pour redémarrer XClarity Administrator après un arrêt, consultez Redémarrage de XClarity Administrator.

Redémarrage de XClarity Administrator

Vous pouvez redémarrer Lenovo XClarity Administrator depuis l'interface Web ou depuis l'hyperviseur après un arrêt.

Avant de commencer

Vous devez disposer de droits **lxc-supervisor** ou **lxc-admin** pour redémarrer XClarity Administrator.

Assurez-vous qu'aucun travail n'est en cours d'exécution. Tous les travaux en cours d'exécution ont été annulés lors du processus de redémarrage. Pour afficher le journal des travaux, consultez Surveillance des travaux.

À propos de cette tâche

Certaines situations nécessitent de redémarrer Lenovo XClarity Administrator :
- Lors de la régénération d'un certificat de serveur
- Lors du téléchargement d'un nouveau certificat de serveur

Procédure

Effectuez l'une des procédures suivantes pour redémarrer Lenovo XClarity Administrator.

- **Conteneurs**

  Exécutez les commandes ci-après pour arrêter, puis démarrer le conteneur, <*env_filename*> étant le nom du fichier des variables d'environnement.
  ```
  docker-compose -p ${CONTAINER_NAME} down
  COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d
  ```
- **Dispositifs virtuels**
  - Redémarrez Lenovo XClarity Administrator depuis l'interface Web :
    1. Dans la barre de menuLenovo XClarity Administrator, cliquez sur **Administration → Arrêter le serveur de gestion**.

       Une boîte de dialogue de confirmation est affichée avec une liste de travaux en cours d'exécution. Lorsque vous redémarrez Lenovo XClarity Administrator, les travaux sont arrêtés.
    2. Cliquez sur **Redémarrer**.

       Lorsque Lenovo XClarity Administrator s'arrête, la connectivité à Lenovo XClarity Administrator est perdue.

3. Patientez quelques minutes le temps que Lenovo XClarity Administrator redémarre, puis connectez-vous à nouveau.

– Redémarrez Lenovo XClarity Administrator depuis l'hyperviseur après un arrêt :
  – Microsoft Hyper-V
    1. Dans le tableau de bord de Server Manager, cliquez sur **Hyper-V**.
    2. Cliquez avec le bouton droit sur le serveur, puis cliquez sur **Gestionnaire Hyper-V**.
    3. Cliquez avec le bouton droit de la souris sur la machine virtuelle, puis cliquez sur **Démarrer**. Lorsque la machine virtuelle est démarrée, les adresses IPv4 et IPv6 sont répertoriées pour chaque interface, comme illustré dans l'exemple suivant.

       Le port de gestion eth0 XClarity Administrator utilise une adresse IP DHCP par défaut. À la fin du processus d'amorçage de XClarity Administrator, vous pouvez choisir de définir une adresse IP statique pour le port de gestion eth0 en saisissant 1 lorsque vous y êtes invité, comme illustré dans l'exemple ci-dessous. L'invite est disponible pendant 150 secondes, jusqu'à ce que l'invite de connexion s'affiche. Pour passer immédiatement à l'invite de connexion, entrez x à l'invite.

       Important :

       - Lorsque vous modifiez les paramètres d'adresse IP statique, vous avez au maximum 60 secondes pour entrer les nouveaux paramètres. Vérifiez que vous disposez des informations IP requises avant de continuer.
         – Pour les paramètres IPv4, vous devez disposer de l'adresse IP, du masque de sous-réseau et de l'adresse IP de passerelle
         – Pour les paramètres IPv6, vous devez disposer l'adresse IP et de la longueur du préfixe
       - Si vous n'utilisez pas de serveur DHCP, vous pouvez utiliser un fichier de configuration pour spécifier les paramètres IP du port de gestion eth0 de XClarity Administrator que vous souhaitez utiliser pour accéder à XClarity Administrator. Pour plus d'informations, voir la section « Étape suivante » ci-dessous.
       - Si vous modifiez les paramètres d'adresse IP à partir de la console, XClarity Administrator est redémarré de manière à appliquer les nouveaux paramètres.
       - Aucune action n'est requise pour la connexion. Ignorez le message de connexion à la console. L'interface de console n'est pas destinée aux clients.
       - Le message suivant peut s'afficher : `TCP: eth0: Driver has suspect GRO implementation, TCP performance may be compromised` sur la console. Cela n'affecte pas les performances de la machine virtuelle, et vous pouvez ignorer cet avertissement.

       Attention : Le fait de modifier l'adresse IP du port de gestion de XClarity Administrator après avoir géré des appareils peut avoir pour effet de placer les appareils dans un état hors ligne dans XClarity Administrator. Si vous choisissez de modifier l'adresse IP une fois que XClarity Administrator est opérationnel, vérifiez qu'aucun appareil n'est géré avant de modifier l'adresse IP.

```
----------------------------------------
Lenovo XClarity Administrator  Version x.x.x
----------------------------------------

eth0   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.10  netmask 255.255.255.0  broadcast 192.0.2.55
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64   scopeid 0x20<link>
         ether 00:15:5d:0c:d1:92    txqueuelen 1000 (Ethernet)
         RX errors 0  dropped 0  overruns 0  frame 0

eth1   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.20  netmask 255.255.255.0  broadcast 192.0.2.130
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64  scopeid 0x20<link>
```

```
================================================================================
================================================================================

You have 150 seconds to change IP settings. Enter one of the following:
  1. To set a static IP address for Lenovo XClarity virtual appliance eth0 port
  2. To use a DHCP address for Lenovo XClarity virtual appliance eth0 port
  x. To continue without changing IP settings
  … …
```

4. Connectez-vous à Lenovo XClarity Administrator (voir Connexion à XClarity Administrator).

– VMware ESXi

1. Connectez-vous à l'hôte via VMware vSphere Client.
2. Cliquez avec le bouton droit sur la machine virtuelle, puis cliquez sur **Alimentation → Mise sous tension**.
3. Cliquez sur l'onglet **Console**. Lorsque la machine virtuelle est démarrée, les adresses IPv4 et IPv6 sont répertoriées pour chaque interface, comme illustré dans l'exemple suivant.

   Le port de gestion eth0 XClarity Administrator utilise une adresse IP DHCP par défaut. À la fin du processus d'amorçage de XClarity Administrator, vous pouvez choisir de définir une adresse IP statique pour le port de gestion eth0 en saisissant 1 lorsque vous y êtes invité, comme illustré dans l'exemple ci-dessous. L'invite est disponible pendant 150 secondes, jusqu'à ce que l'invite de connexion s'affiche. Pour passer immédiatement à l'invite de connexion, entrez x à l'invite.

   Important :

   - Lorsque vous modifiez les paramètres d'adresse IP statique, vous avez au maximum 60 secondes pour entrer les nouveaux paramètres. Vérifiez que vous disposez des informations IP requises avant de continuer.
     – Pour les paramètres IPv4, vous devez disposer de l'adresse IP, du masque de sous-réseau et de l'adresse IP de passerelle
     – Pour les paramètres IPv6, vous devez disposer l'adresse IP et de la longueur du préfixe
   - Si vous n'utilisez pas de serveur DHCP, vous pouvez utiliser un fichier de configuration pour spécifier les paramètres IP du port de gestion eth0 de XClarity Administrator que vous souhaitez utiliser pour accéder à XClarity Administrator. Pour plus d'informations, voir la section « Étape suivante » ci-dessous.
   - Si vous modifiez les paramètres d'adresse IP à partir de la console, XClarity Administrator est redémarré de manière à appliquer les nouveaux paramètres.
   - Aucune action n'est requise pour la connexion. Ignorez le message de connexion à la console. L'interface de console n'est pas destinée aux clients.
   - Le message suivant peut s'afficher : `TCP: eth0: Driver has suspect GRO implementation, TCP performance may be compromised` sur la console. Cela n'affecte pas les performances de la machine virtuelle, et vous pouvez ignorer cet avertissement.

   Attention : Le fait de modifier l'adresse IP du port de gestion de XClarity Administrator après avoir géré des appareils peut avoir pour effet de placer les appareils dans un état hors ligne dans XClarity Administrator. Si vous choisissez de modifier l'adresse IP une fois que XClarity Administrator est opérationnel, vérifiez qu'aucun appareil n'est géré avant de modifier l'adresse IP.

```
------------------------------------------
Lenovo XClarity Administrator  Version x.x.x
------------------------------------------

eth0   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.10  netmask 255.255.255.0  broadcast 192.0.2.55
```

```
          inet6 2001:db8:56ff:fe80:bea3  prefixlen 64   scopeid 0x20<link>
          ether 00:15:5d:0c:d1:92    txqueuelen 1000 (Ethernet)
          RX errors 0  dropped 0  overruns 0  frame 0

eth1   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
          inet 192.0.2.20  netmask 255.255.255.0  broadcast 192.0.2.130
          inet6 2001:db8:56ff:fe80:bea3  prefixlen 64  scopeid 0x20<link>

================================================================================
================================================================================

You have 150 seconds to change IP settings. Enter one of the following:
  1. To set a static IP address for Lenovo XClarity virtual appliance eth0 port
  2. To use a DHCP address for Lenovo XClarity virtual appliance eth0 port
  x. To continue without changing IP settings
  … …
```

4. Connectez-vous à Lenovo XClarity Administrator (voir Connexion à XClarity Administrator).

Après avoir terminé

Lorsque Lenovo XClarity Administrator redémarre, il collecte à nouveau l'inventaire de chaque appareil géré. Attendez environ 30 à 45 minutes, en fonction du nombre d'appareils gérés, avant de tenter une mise à jour de microprogramme, un déploiement de modèle de configuration ou un déploiement de système d'exploitation.

Chapitre 3. Appareils et activités de surveillance

Vous pouvez surveiller vos appareils et activités via le tableau de bord, les alertes, les journaux d'audit et les journaux de travaux.

Affichage d'un récapitulatif de votre environnement

Le tableau de bord affiche l'état de tous les appareils gérés, une présentation de toutes les liées à la distribution des tâche, ainsi que des informations sur les ressources et les activités de Lenovo XClarity Administrator.

En savoir plus :  XClarity Administrator : Surveillance

Procédure

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Tableau de bord**.

Etape 2. Développez la section relative à l'état du matériel, à l'état de la distribution, ou encore à l'activité de l'administrateur, afin d'afficher des informations supplémentaires sur chacun de ces domaines.

Affichage d'un récapitulatif de l'état de votre matériel

La zone État du matériel affiche l'état de tous les appareils gérés.

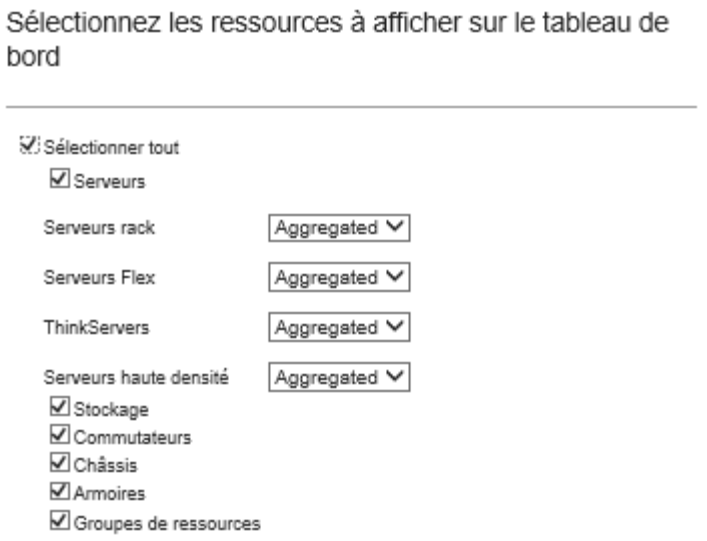
Procédure

Pour plus d'informations sur tous les appareils de ce type, cliquez sur le numéro indiqué au-dessous du type d'appareil.

Pour afficher des informations supplémentaires sur uniquement les appareils de ce type et l'état, cliquez sur l'icône ou le numéro figurant en regard de chaque icône d'état.

- **Serveurs**. Affiche le nombre total de serveurs (nœuds de traitement, serveurs rack, et serveurs au format tour) gérés par XClarity Administrator, ainsi que le nombre de serveurs à l'état normal, avertissement et critique. Pour plus d'informations, voir Affichage de l'état d'un serveur géré.
- **Stockage**. Affiche le nombre total de dispositifs de stockage gérés par XClarity Administrator, ainsi que le nombre de dispositifs de stockage à l'état normal, avertissement et critique. Pour plus d'informations, voir Affichage de l'état des dispositifs de stockage.
- **Commutateurs**. Affiche le nombre total de commutateurs RackSwitch et Flex System gérés par XClarity Administrator, ainsi que le nombre de commutateurs à l'état normal, avertissement et critique. Pour plus d'informations, voir Affichage de l'état de commutateurs
- **Châssis**. Affiche le nombre total de châssis Flex gérés par XClarity Administrator, ainsi que le nombre de châssis Flex à l'état normal, avertissement et critique. Pour plus d'informations, voir Affichage de l'état de châssis gérés.
- **Armoires**. Affiche le nombre d'armoires qui sont créées dans XClarity Administrator, ainsi que le nombre d'armoires comportant des appareils dont l'état le plus élevé est normal, avertissement et critique. Pour plus d'informations, voir Affichage de l'état des appareils présents dans une armoire.
- **Groupes de ressources**. Affiche le nombre de groupes de ressources qui sont gérées par XClarity Administrator, ainsi que le nombre de groupes de ressources comportant des appareils présentant le statut le plus élevé Normal, Avertissement et Critique. Pour plus d'informations, voir Affichage de l'état des appareils présents dans un groupe de ressources.

Pour personnaliser les ressources matérielles qui s'affichent dans le tableau de bord, cliquez sur l'icône **Personnaliser** (voir ). Vous pouvez choisir les types d'appareil que vous souhaitez afficher ou masquer. Vous pouvez également choisir d'agréger les serveurs dans un seul récapitulatif, d'afficher des récapitulatifs distincts pour chaque type de serveur (rack et au format tour, Flex System, NeXtScale et ThinkServer) ou omettre des types de serveurs spécifiques.



Affichage d'un récapitulatif de l'état de votre distribution

La zone État de la distribution fournit un récapitulatif de toutes les tâches qui sont associées aux dispositifs de distribution.

Procédure

- **Modèles de configuration**. Affiche des détails sur le nombre de serveurs comportant des profils, notamment les statistiques suivantes :

Remarque : Si le serveur de gestion n'est pas compatible avec les licences, toutes les valeurs sont définies sur 0 (voir Installation de la licence d'activation de l'ensemble des fonctionnalités dans la documentation en ligne de XClarity Administrator).

- Le nombre de serveurs conformes à leur profil de serveur. Vous pouvez cliquer sur ce nombre pour afficher la page Modèles de configuration : Profils de serveur avec la liste des serveurs conformes.
- Le nombre de serveurs non conformes à leur profil de serveur. Vous pouvez cliquer sur ce nombre pour afficher la page Modèles de configuration : Profils de serveur avec la liste des serveurs non conformes.
- Le nombre d'appareils pour lesquels l'état de conformité est inconnu. Vous pouvez cliquer sur ce nombre pour afficher la page Modèles de configuration : Profils de serveur avec la liste des serveurs dont la conformité est inconnue.

  Remarque : L'état de conformité est inconnu, généralement après le déploiement d'un profil partiel, lorsque Lenovo XClarity Administrator n'a pas collecté les informations de configuration du serveur. Actualisez l'inventaire de serveur ou revisitez la page de détails de profil de serveur afin de forcer la collecte des informations de configuration du serveur.
- Le nombre de serveurs auxquels un profil de serveur est attribué. Vous pouvez cliquer sur ce nombre pour afficher la page Modèles de configuration : Profils de serveur avec la liste des serveurs auxquels un profil est attribué.
- Le nombre de serveurs auxquels aucun profil de serveur n'est attribué. Vous pouvez cliquer sur ce nombre pour afficher la page Modèles de configuration : Modèles de serveur avec la liste des modèles de serveur qui peuvent être déployés sur les serveurs sans profils.
- Le nombre de modèles de serveur actuellement en cours de déploiement.

Pour afficher les données de tendances pour les modèles de configuration, cliquez sur **Afficher les données de tendances** (voir Surveillance des tendances dans l'état de la distribution).

Pour plus d'informations sur les modèles de configuration et les profils de serveur, voir Configuration des serveurs à l'aide de modèles de configuration.

- **Images du système d'exploitation**. Affiche des détails sur les déploiements de système d'exploitation, notamment les statistiques suivantes :

  Remarque : Si le serveur de gestion n'est pas compatible avec les licences, toutes les valeurs sont définies sur 0 (voir Installation de la licence d'activation de l'ensemble des fonctionnalités dans la documentation en ligne de XClarity Administrator).

  - Le nombre d'images SE dans le référentiel. Vous pouvez cliquer sur le nombre pour afficher la page Déployer des systèmes d'exploitation : gérer des images SE, avec une liste de systèmes d'exploitation.
  - Le nombre de déploiements SE actuellement en cours. Vous pouvez cliquer sur le nombre pour afficher la page Déployer des systèmes d'exploitation : déployer des images SE, avec une liste des appareils pour lesquels un système d'exploitation est en cours d'installation.
- **Mises à jour du microprogramme**. Affiche des détails sur les mises à jour du microprogramme, notamment les statistiques suivantes :
  - Le nombre d'appareils conformes. Vous pouvez cliquer sur le nombre pour afficher la page Mises à jour de microprogramme : Appliquer/Activer qui comporte une liste des appareils conformes.
  - Nombre d'appareils non compatibles. Vous pouvez cliquer sur le nombre pour afficher la page Mises à jour de microprogramme : Appliquer/Activer qui comporte une liste des appareils non conformes.
  - Nombre d'appareils auxquels n'est pas affectée une stratégie de conformité du microprogramme. Vous pouvez cliquer sur le nombre pour afficher la page Mises à jour de microprogramme : Appliquer/Activer qui comporte une liste des appareils sans stratégie de conformité.

    Depuis cette page, vous pouvez affecter à chaque appareil une stratégie de conformité du microprogramme en sélectionnant une stratégie dans la colonne **Stratégie de conformité affectée**.

- Nombre d’appareils pour lesquels les mises à jour ne sont pas prises en charge. Vous pouvez cliquer sur le nombre pour afficher la page Mises à jour de microprogramme : Appliquer/Activer qui comporte une liste des appareils pour lesquels les mises à jour ne sont pas prises en charge.
- Nombre de mises à jour qui sont en cours.
- Le nombre d'appareils en attente du microprogramme. Vous pouvez cliquer sur le nombre pour afficher la page Mises à jour de microprogramme : Appliquer/Activer qui comporte une liste des appareils dont l'activation est en attente.

Pour afficher les données de tendances pour les mises à jour de microprogramme, cliquez sur **Afficher les données de tendances** (voir Surveillance des tendances dans l'état de la distribution).

Pour plus d'informations sur les mises à jour de microprogramme et les stratégies de conformité, voir Mise à jour du microprogramme sur les appareils gérés.

Affichage d'un récapitulatif de l'activité de Lenovo XClarity Administrator

La zone Activité de XClarity Administrator affiche des informations sur les travaux actifs, les sessions actives et les ressources système dans XClarity Administrator.

Procédure

- **Travaux**. Affiche le nombre de travaux actifs actuellement en cours. Pour plus d'informations sur les travaux, voir Surveillance des travaux.
- **Sessions actives**. Affiche l'ID utilisateur et l'adresse IP de chaque session active XClarity Administrator. Pour plus d'informations sur les utilisateurs, voir Gestion des comptes utilisateur.
- **Utilisation de ressources**. Affiche l'utilisation du processeur, l'utilisation de la mémoire, la capacité de disque sur le système hôte et les partages de fichiers à distance. Pour plus d'informations à propos des ressources système, voir Surveillance des ressources système.

Surveillance des ressources système

Vous pouvez déterminer l'utilisation du processeur, l'utilisation de la mémoire, la capacité de disque sur le système hôte depuis la page Tableau de bord.

Avant de commencer

Les *exigences minimales* suivantes doivent être satisfaites pour XClarity Administrator. Selon la taille de votre environnement et la façon dont vous utilisez Modèles de configuration, des ressources supplémentaires peuvent s'avérer nécessaires afin d'optimiser les performances.

- Deux microprocesseurs virtuels
- 8 Go de mémoire
- 192 Go de stockage à utiliser par le dispositif virtuel XClarity Administrator.
- Afficher avec une résolution minimale de 1 024 pixels en largeur (XGA)

Le tableau suivant répertorie les configurations minimales recommandées pour un certain nombre d’appareils. Gardez à l’esprit que si vous exécutez la configuration minimale, vous risquez de constater des temps d'achèvement plus longs que prévus pour les tâches de gestion. Pour les tâches d’approvisionnement telles que le déploiement du système d’exploitation, les mises à jour de microprogramme et la configuration du serveur, vous devrez peut-être augmenter temporairement les ressources.

Nombre d'appareils gérés	Configuration UC virtuelle/mémoire
0 - 100 appareils	2 UC virtuelles, 8 Go RAM
100 - 200 appareils	4 UC virtuelles, 10 Go RAM
200 - 400 appareils	6 UC virtuelles, 12 Go RAM
400 - 600 appareils	8 UC virtuelles, 16 Go RAM
600 - 800 appareils	10 UC virtuelles, 20 Go RAM
800 – 1 000 appareils	12 UC virtuelles, 24 Go RAM

Remarques :

- Une instance XClarity Administrator unique peut prendre en charge jusqu'à 1 000 appareils.
- Pour les dernières recommandations et des remarques concernant des performances supplémentaires, voir le Guide des performances de XClarity Administrator (Livre blanc).
- Selon la taille de votre environnement géré et du modèle d'utilisation dans votre installation vous devrez peut-être ajouter des ressources pour maintenir des performances acceptables. Si vous voyez souvent que l'utilisation du processeur dans le tableau de bord de ressources système indique des valeurs élevées ou très élevées, envisagez d'ajouter 1 à 2 cœurs de processeur virtuels. Si l'utilisation de votre mémoire est toujours supérieure à 80 % en mode inactif, envisagez d'ajouter 1 ou 2 Go de RAM. Si votre système est sensible à une configuration, telle que définie dans le tableau, pensez à lancer la machine virtuelle pendant une plus longue période afin d'évaluer les performances du système.
- Pour plus d'informations sur la manière de libérer de l'espace disque en supprimant des ressources XClarity Administrator devenues inutiles, voir Gestion de l'espace disque.

Procédure

Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Tableau de bord**.

L'utilisation des ressources du système hôte est répertoriée dans la section Activité de XClarity Administrator.

Processeur

La mesure d'utilisation indique le nombre de processus XClarity Administrator qui accèdent simultanément aux processeurs sur l'hôte.

Astuce : La mesure d'utilisation peut afficher de temps en temps un pic d'utilisation Élevé ou Très élevé. Si l'utilisation demeure à ces niveaux pendant plus de 30 minutes, consultez le journal des travaux pour voir si des travaux à exécution longue sont en cours (voir Surveillance des travaux).

La mesure de capacité totale indique le nombre de processeurs disponibles sur l'hôte.

Mémoire

La mesure d'utilisation indique la quantité de mémoire qui est en cours de utilisation par XClarity Administrator.

La mesure de capacité totale indique la quantité de mémoire totale disponible sur l'hôte.

Données utilisateur

La mesure d'utilisation indique la quantité d'espace disque qui est en cours de utilisation par XClarity Administrator sur le système hôte.

La mesure de capacité totale indique la quantité totale d'espace (utilisé et non utilisé) qui est affectée pour les données utilisateur, par exemple, les systèmes d'exploitation et les mises à jour de microprogramme.

Pour plus d'informations sur la gestion de l'espace disque, voir Gestion de l'espace disque.

Attention : Si les ressources affectées sont insuffisantes pour gérer le nombre actuel d'appareils gérés avec des performances satisfaisantes, augmentez l'allocation de ressources. Pour plus d'informations sur le matériel requis en fonction du nombre d'appareils gérés présents dans votre environnement, voir Systèmes hôtes pris en charge dans la documentation en ligne de XClarity Administrator.

Surveillance des tendances dans l'état de la distribution

Lenovo XClarity Administrator collecte régulièrement l'état de la distribution, y compris la conformité et les travaux actifs pour les mises à jour de microprogramme et les modèles de configuration, pour tous les appareils gérés, de sorte que vous puissiez surveiller les tendances sur une période de temps.

À propos de cette tâche

Vous devez disposer de droits **lxc_admin** ou **lxc-supervisor** pour afficher les données de tendance.

Les données suivantes sont collectées :

- **Mises à jour du microprogramme**
  - **Appareils conformes**. Nombre d'appareils qui sont conformes à la stratégie de conformité du microprogramme qui leur est affectée
  - **Appareils non conformes** Nombre d'appareils qui ne sont pas conformes à la stratégie de conformité du microprogramme qui leur est affectée
  - **Appareils sans stratégies** Nombre d'appareils auxquels n'est affectée aucune stratégie de conformité du microprogramme
  - **Appareils non pris en charge pour les mises à jour** Nombre d'appareils pour lesquels les mises à jour de microprogramme ne sont pas prises en charge
  - **Mises à jour en cours**. Nombre d'appareils pour lesquels les mises à jour de microprogramme sont en cours
- **Modèles de configuration**
  - **Serveurs avec profils**. Nombre d'appareils auxquels est affecté un profil de serveur.
  - **Serveurs sans profils**. Nombre d'appareils auxquels n'est affecté aucun profil de serveur
  - **Conformes aux serveurs**. Nombre d'appareils qui sont conformes au profil de serveur qui leur est affecté

- **Non conformes aux serveurs**. Nombre d'appareils qui ne sont pas conformes au profil de serveur qui leur est affecté
- **Modèles de serveur en cours**. Nombre d'appareils pour lesquels des mises à jour de modèle de configuration sont en cours

Procédure

Procédez comme suit pour afficher les tendances dans l'état de la distribution.

Etape 1. Dans la barre de menus XClarity Administrator, cliquez sur **Tableau de bord** pour afficher la page Tableau de bord.

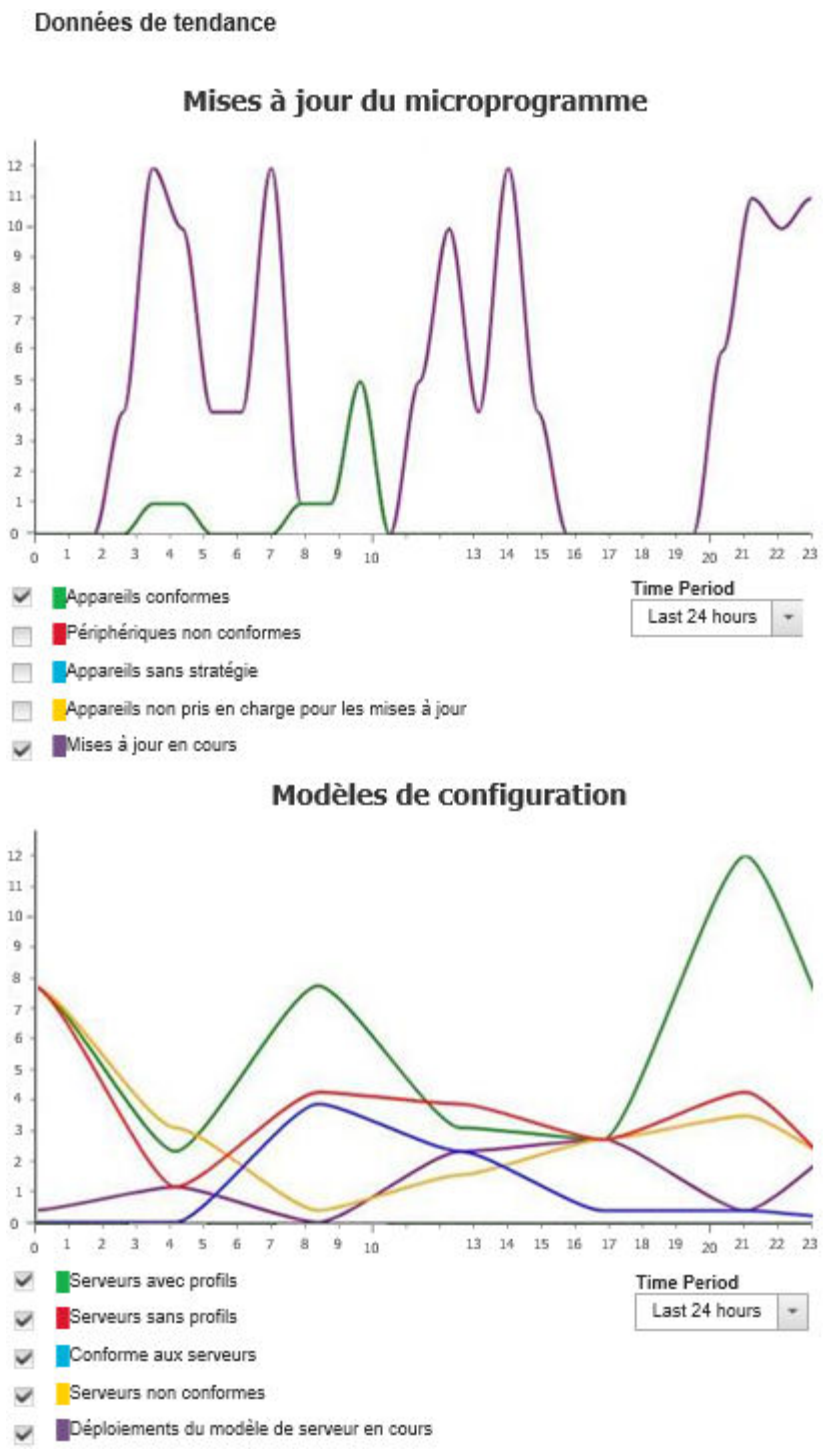
Etape 2. Cliquez sur le lien **Données de tendance** pour afficher la boîte de dialogue Paramètres du seuil.

Etape 3. Désélectionnez ou sélectionnez les données à afficher.

Etape 4. Sélectionnez la période à afficher.

- **24 heures**. Affiche des données des dernières 24 heures. Chaque point de données est une moyenne sur une période de 1 heure.
- **1 mois**. Affiche des données des 30 derniers jours. Chaque point de données est une moyenne sur une période de 24 heures.

Les données de tendance sont affichées sous forme de graphique sur la période sélectionnée.



Surveillance des mesures historiques

Lenovo XClarity Administrator collecte régulièrement des données de mesure pour les appareils ThinkSystem et ThinkAgile gérés, en vue d'analyser l'état actuel de votre environnement.

Avant de commencer

Les mesures historiques sont prises en charge uniquement pour les serveurs ThinkSystem (à l'exception de SR635, SR645, SR655 et SR665).

Seuls les disques SSD des serveurs ThinkSystem et ThinkAgile (à l'exception de SR635 et SR655) exécutant le microprogramme XCC avec une date de sortie ultérieure à avril 2019 sont pris en charge.

Les pilotes SATA intégrés ne sont pas pris en charge.

Les disques NVMe doivent prendre en charge la spécification NVMe-MI (NVMe Management Interface)

À propos de cette tâche

Les mesures suivantes sont collectées.

- **Surveillance des SSD** La carte de rapport comprend les statistiques et graphiques suivants.
  - Nombre total de disques SSD dans les appareils gérés (selon la portée).
  - Nombre de disques SSD ayant été analysés
  - Nombre de disques SSD non éligibles à une analyse
  - Un graphique circulaire représentant le nombre d'appareils dotés de disques SSD ayant une durée de vie restante dans une plage spécifique.
    - Durée de vie restante <= 10 %. Nombre de disques SSD ayant une durée de vie restante de 10 % ou moins
    - Durée de vie restante 11 à 50 %. Nombre de disques SSD ayant une durée de vie restante de 11 à 50 %
    - Durée de vie restante 51 à 100 %. Nombre de disques SSD ayant une durée de vie restante de plus de 50 %
- **Utilisation du système** La carte de rapport comprend les statistiques et graphiques suivants.
  - L'utilisation actuelle du processeur, exprimée en pourcentage
  - L'utilisation actuelle de la mémoire, exprimée en pourcentage
  - Un graphique linéaire affichant l'utilisation du processeur et de la mémoire dans le temps
- **Consommation électrique** La carte de rapport comprend les statistiques et graphiques suivants.
  - L'entrée d'énergie totale actuelle pour toutes les alimentations, en watts
  - Un graphique linéaire qui affiche l'entrée d'énergie totale au fil du temps
- **Température de l'appareil** La carte de rapport comprend les statistiques et graphiques suivants.
  - La température maximale actuelle de l'air en entrée, en Celsius
  - Un graphique linéaire qui affiche la température maximale au fil du temps

Afin d'obtenir plus d'informations sur la mesure, vous pouvez pointer chaque ligne colorée du graphique circulaire, un point ou un autre du graphique linéaire, ou un numéro à côté de chaque mesure. Vous pouvez afficher ou masquer les mesures dans le graphique en cliquant sur l'icône de couleur dans la légende. Vous pouvez également cliquer sur le numéro ou l'option lié(e) dans l'icône **Paramètres** () dans le coin supérieur droit de la carte afin d'afficher une liste de tous les appareils ayant des mesures qui répondent aux critères sélectionnés.

Procédure

Procédez comme suit pour afficher l'organigramme d'une activité spécifique.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Surveillance → Mesures historiques** pour afficher la page Mesures historiques avec des cartes de rapport pour chaque type de mesure.

Etape 2. Définissez la portée de tous les appareils ou d'un groupe spécifique.

Placement des appareils en mode de maintenance

Lorsqu'un appareil est en mode de maintenance, Lenovo XClarity Administrator exclut tous les événements et alertes de cet appareil de toutes les pages sur lesquelles des événements et des alertes sont affichés. Les alertes exclues sont toujours consignées, mais masquées dans la vue.

À propos de cette tâche

Seuls sont exclus les événements et alertes générés pour un appareil pendant que celui-ci est en mode de maintenance. Des événements et des alertes s'affichent, lesquels ont été générés avant que l'appareil ne soit placé en mode de maintenance.

Le fait de placer un appareil géré en maintenance, puis de nouveau en service peut entraîner l'obsolescence de l'inventaire de cet appareil. Si vous constatez des anomalies, actualisez manuellement l'inventaire à partir de la page de l'appareil en sélectionnant l'appareil, puis en cliquant sur **Toutes les actions → Inventaire → Actualiser l'inventaire**.

Procédure

Pour placer un appareil en mode maintenance, procédez de l'une des manières suivantes :

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Administration → Service et support**. La page Service et support s'affiche.

Etape 2. Cliquez sur **Actions de nœud final** dans la navigation de gauche pour afficher la page Actions de nœud final.

Etape 3. Sélectionnez au moins un appareil à placer en mode de maintenance.

Etape 4. Cliquez sur **Actions → Maintenance** pour afficher la boîte de dialogue Mode de maintenance.

Etape 5. Sélectionnez la date et l'heure de sortie de l'appareil du mode de maintenance et de sa remise en service.

Sélectionnez **Indéfiniment** si vous ne souhaitez pas que l'appareil soit remis en service.

Etape 6. Cliquez sur **Confirmer**. La colonne maintenance du tableau affiche la valeur Oui pour cet appareil.

Après avoir terminé

Lorsque vous avez terminé la maintenance sur l'appareil, vous pouvez remettre l'appareil en service en sélectionnant l'appareil, puis en cliquant sur **Actions → Maintenance**, puis sur **Désactiver la maintenance** dans la boîte de dialogue. Si vous ne remettez pas manuellement l'appareil en service, il est mis en service automatiquement après l'expiration de la date et de l'heure de fin spécifiées.

Utilisation des alertes

Les *alertes* sont des conditions de matériel ou de gestion nécessitant une recherche et une action utilisateur. Lenovo XClarity Administrator interroge les appareils gérés de manière asynchrone et affiche les alertes qui sont reçues de ces appareils.

En savoir plus : XClarity Administrator : Surveillance

À propos de cette tâche

Généralement, quand une alerte est reçue, un événement correspondant est stocké dans le journal des événements. Il est possible d'avoir une alerte sans événement correspondant dans le journal des

événements (même si le journal est en boucle). Par exemple, les événements qui se produisent avant que vous procédiez à la gestion d'un châssis ne s'affichent dans le journal des événements. Toutefois, les alertes du châssis s'affichent dans le journal des alertes, car Lenovo XClarity Administrator interroge le module CMM une fois la gestion du châssis terminée.

Affichage des alertes actives

Vous pouvez afficher la liste de toutes les alertes de matériel et de gestion actives.

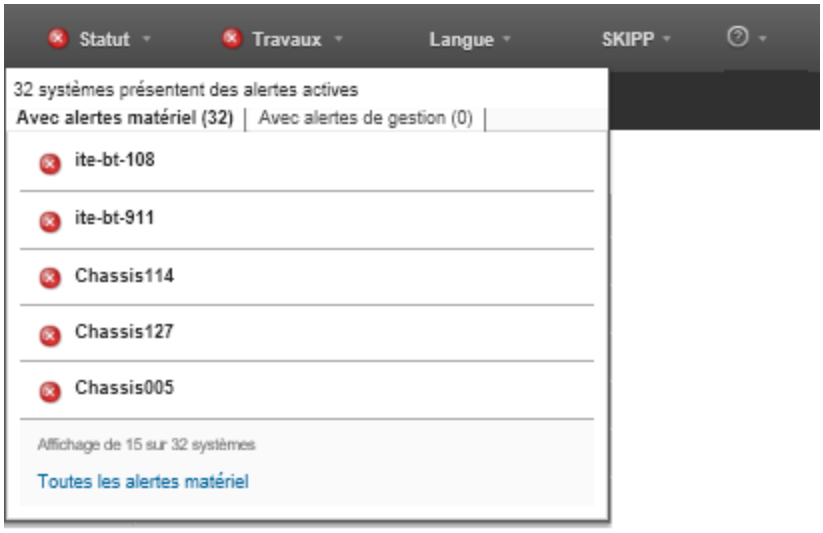
À propos de cette tâche

Remarque : Les alertes pour les dispositifs Lenovo Storage sont présentées uniquement en anglais, même lorsque les paramètres régionaux pour Lenovo XClarity Administrator sont définis sur une autre langue. Utilisez un système de traduction externe pour traduire les messages manuellement, si nécessaire.

Procédure

Suivez l'une des procédures suivantes pour afficher les alertes actives.

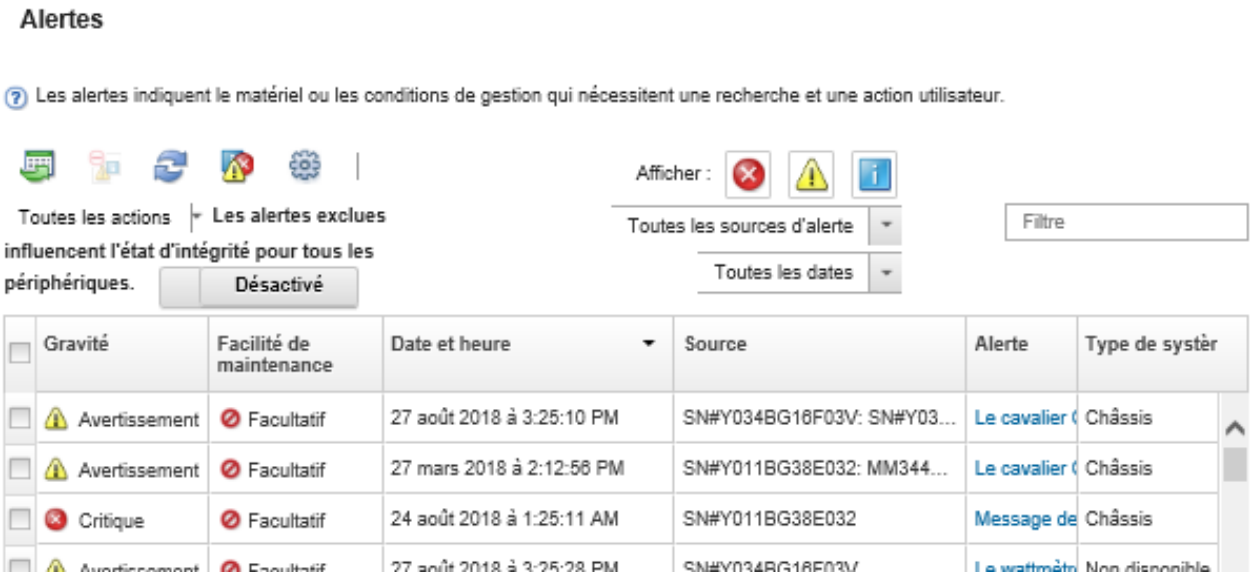
- Pour afficher uniquement les alertes pour les appareils gérés (appelées *alertes de matériel) :*
  1. Dans la barre de titre de XClarity Administrator, cliquez sur le menu déroulant **État** pour afficher un récapitulatif des alertes de matériel et de gestion.
  2. Cliquez sur l'onglet **Avec alertes matériel** pour afficher un récapitulatif des alertes pour chaque appareil géré.



  3. Passez le curseur au-dessus d'un appareil répertorié sous cet onglet pour afficher la liste des alertes pour cet appareil.
  4. Cliquez sur le lien **Toutes les alertes matériel** pour afficher la page Alertes avec une liste filtrée de toutes les alertes de matériel.
- Pour afficher uniquement les alertes de XClarity Administrator (appelées *alertes de gestion) :*
  1. Dans la barre de titre de XClarity Administrator, cliquez sur le menu déroulant **État** pour afficher un récapitulatif des alertes de matériel et de gestion.
  2. Cliquez sur l'onglet **Avec alertes de gestion** pour afficher un récapitulatif de toutes les alertes CMM et XClarity Administrator.

3. Passez le curseur au-dessus d'un appareil répertorié sous cet onglet pour afficher la liste des alertes pour cet appareil.
4. Cliquez sur le lien **Toutes les alertes de gestion** pour afficher la page Alertes avec une liste filtrée de toutes les alertes CMM et XClarity Administrator.

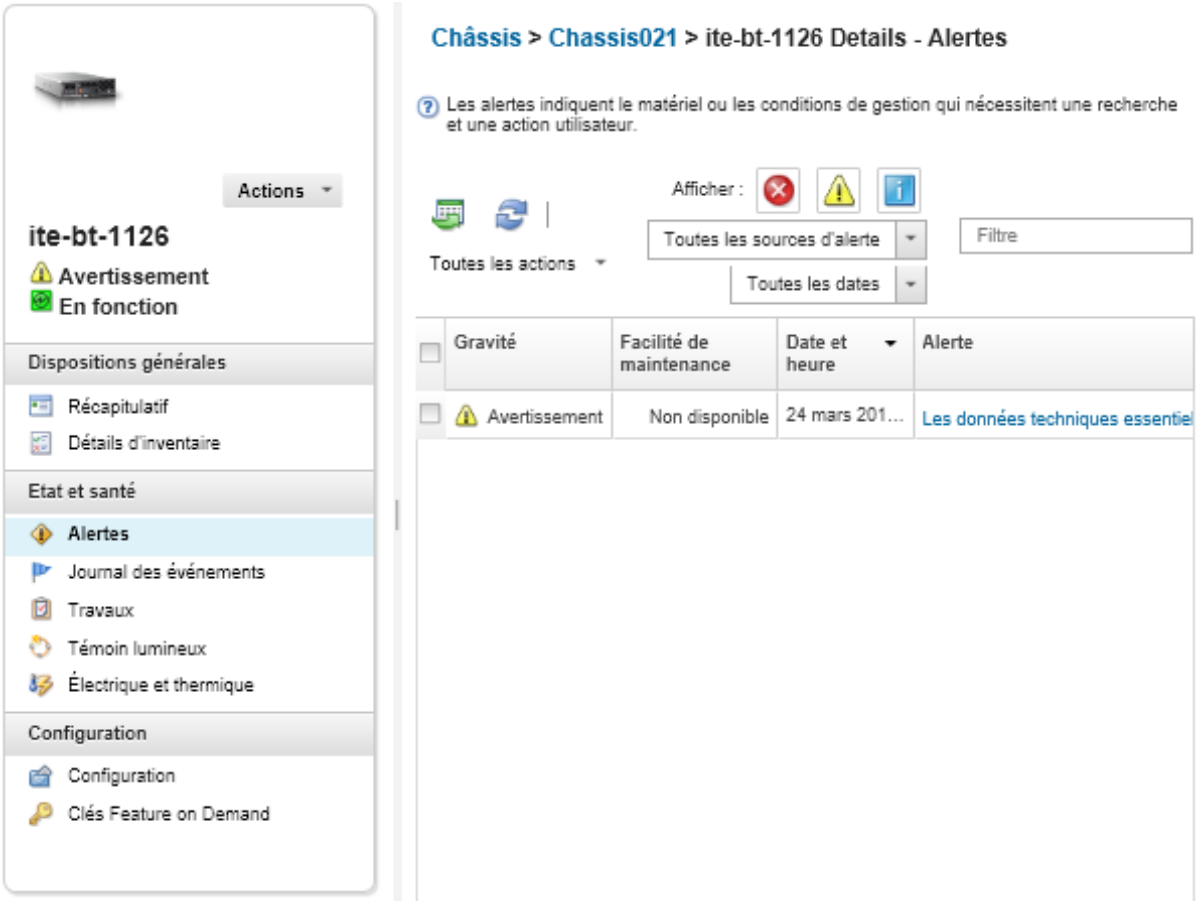
- Pour afficher toutes les alertes dans XClarity Administrator, cliquez sur **Surveillance → Alertes** dans la barre de menus XClarity Administrator. La page Alertes s'affiche avec la liste de toutes les alertes actives.



- Pour afficher les alertes pour un appareil spécifique :
  1. Dans la barre de menus XClarity Administrator, cliquez sur **Matériel**, puis sur un type d'appareil. Une page s'affiche avec une vue tabulaire de tous les appareils gérés de ce type. Par exemple, cliquez sur **Matériel → Serveurs** pour afficher la page Serveurs.
  2. Cliquez sur un appareil spécifique pour afficher la page Récapitulatif correspondante.
  3. Sous État et santé, cliquez sur **Alertes** pour afficher la liste de toutes les alertes associées à cet appareil.

     Remarques : La colonne Facilité de maintenance peut afficher « Non disponible » si :

     – l'alerte sur l'appareil s'est produite avant que XClarity Administrator commence à le gérer
     – le journal des événements est en boucle, et que l'événement associé à cette alerte ne figure plus dans ce journal.



Résultats

Dans la page Alertes, vous pouvez effectuer les actions suivantes :

- Actualiser la liste des alertes en cliquant sur l'icône **Actualiser** ( ).

  Conseil : Si de nouvelles alertes sont détectées, le journal des alertes s'actualise automatiquement toutes les 30 secondes.
- Afficher des informations sur une alerte spécifique (notamment une explication et une actions utilisateur) et sur l'appareil qui est la source de l'alerte (telles que l'identificateur unique universel) en cliquant sur le lien figurant dans la colonne **Alerte**. Une boîte de dialogue contenant des informations sur les propriétés et les détails de l'alerte s'affiche.

  Remarque : Si l'explication et les actions de récupération spécifiées pour une alerte ne sont pas affichées sous l'onglet **Détails**, accédez à Documentation en ligne de Lenovo Flex System, puis recherchez l'ID de l'alerte (par exemple, `FQXHMSE0004G`). Le site Web fournit toujours les toutes dernières informations.
- Par défaut, les alertes exclues n'affectent pas l'état de santé des appareils gérés. Vous pouvez autoriser à les alertes exclues à influencer l'état d'intégrité des appareils gérés à partir de la page Alertes en cliquant sur le bouton permettant d'activer **Les alertes exclues influencent l'état d'intégrité de tous les appareils**.
- Vous pouvez définir des préférences de seuil pour le déclenchement d'une alerte et d'un événement lorsqu'une certaine valeur, comme la durée de vie d'un disque SSD sur un serveur ThinkSystem ou ThinkServer dépasse un niveau d'avertissement ou critique (voir Définition des préférences de seuil pour la génération d'alertes et d'événements).

- Exporter le journal des alertes en cliquant sur l'icône **Exporter au format CSV** ().

  Remarque : Les horodatages dans le journal exporté utilisent l'heure locale spécifiée par le navigateur Web.
- Exclure des alertes spécifiques de toutes les pages sur lesquelles des alertes s'affichent (voir Exclusion d'alertes).
- Restreindre la liste des alertes qui s'affichent sur la page actuelle :
  - Afficher ou masquer les alertes d'un niveau de gravité spécifique en cliquant sur les icônes suivantes :
    - L'icône **Alertes critiques** ()
    - L'icône **Alertes d'avertissements** ()
    - L'icône **Alertes d'information** ()
  - Afficher uniquement les alertes provenant de sources spécifiques. Vous pouvez choisir l'une des options suivantes dans la liste déroulante :
    - Toutes les sources d'alerte
    - Événements matériels
    - Événements de gestion
    - Événements du centre de maintenance
    - Événements client réparables
    - Événements non réparables
  - Afficher uniquement les alertes avec une date et une heure spécifiques. Vous pouvez choisir l'une des options suivantes dans la liste déroulante :
    - Toutes les dates
    - Deux heures précédentes
    - 24 heures précédentes
    - La semaine dernière
    - Le mois dernier
  - Répertorier uniquement les alertes qui contiennent un texte spécifique en indiquant le texte dans la zone **Filtre**.
  - Trier les alertes par colonne en cliquant sur un en-tête de colonne.

Exclusion d'alertes

Si certaines alertes ne vous intéressent pas, vous pouvez les exclure de toutes les pages sur lesquelles les alertes sont affichées. Les alertes exclues figurent toujours dans le journal, mais elles sont masquées sur toutes les pages sur lesquelles les alertes sont affichées, notamment les vues de journal et l'état de l'appareil.

À propos de cette tâche

Les alertes exclues sont masquées pour tous les utilisateurs, et non pas uniquement pour l'utilisateur qui a défini la configuration.

Vous pouvez placer les appareils en mode de maintenance, afin que tous les événements et alertes de ces appareils soient exclus (voir Placement des appareils en mode de maintenance).

Restriction : Seuls les utilisateurs disposant de droits d'administration peuvent exclure ou restaurer des alertes.

Important : Si vous excluez les alertes d'état, l'état de l'appareil sur les pages récapitulant les appareils et les détails ne change pas.

ProcédurePour exclure des alertes du journal des alertes, procédez comme suit.

Etape 1. Dans la barre de menus Lenovo XClarity Administrator, cliquez sur **Surveillance → Alertes**. La page Alertes s'affiche.

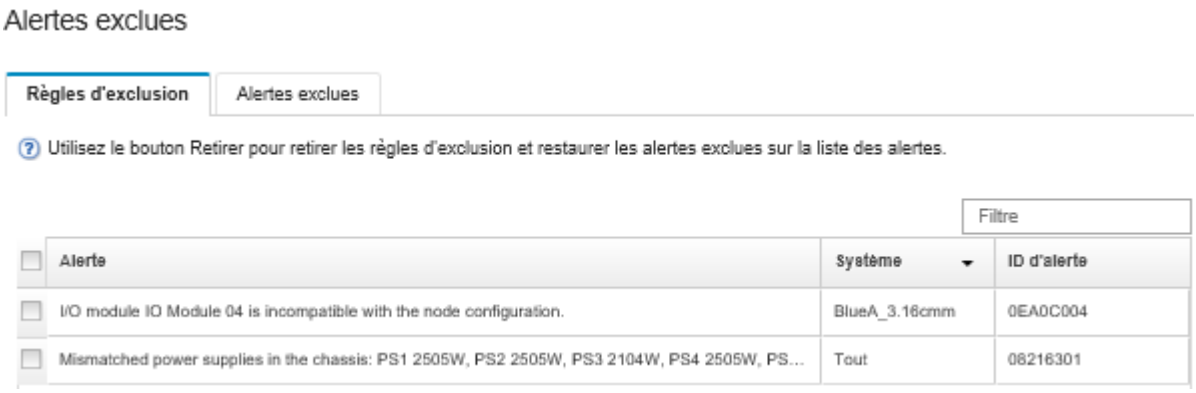
Etape 2. Sélectionnez les alertes à exclure, puis cliquez sur l'icône **Exclure des alertes** ( ). La boîte de dialogue Exclure des alertes s'affiche.

Etape 3. Sélectionnez l'une des options suivantes :
- **Exclure les alertes sélectionnées de tous les systèmes**. Permet d'exclure les alertes sélectionnées de tous les appareils gérés.
- **Exclure les alertes uniquement des systèmes dans le champ de l'instance sélectionnée**. Permet d'exclure les alertes sélectionnées des appareils gérés auxquels les alertes sélectionnées s'appliquent.

Etape 4. Cliquez sur **Enregistrer**.

Après avoir terminé

Lorsque vous excluez des alertes, Lenovo XClarity Administrator crée des règles d'exclusion à partir des informations que vous fournissez. Vous pouvez afficher une liste de règles d'exclusion et d'alertes exclues à la page Alertes en cliquant sur l'icône **Afficher les alertes exclues/enregistrées** ( ). Dans la boîte de dialogue Alertes exclues/enregistrées, cliquez sur l'onglet **Règles d'exclusion** pour afficher la liste des règles d'exclusion ou cliquez sur l'onglet **Alertes exclues** pour afficher la liste des alertes exclues.



Par défaut, les alertes exclues n'affectent pas l'état de santé des appareils gérés. Vous pouvez autoriser les alertes exclues à influencer l'état d'intégrité des appareils gérés à partir de la page Alertes en cliquant sur le bouton permettant d'activer **Afficher les alertes exclues/enregistrées**.

Vous pouvez restaurer des alertes qui ont été exclues dans le journal des alertes en retirant la règle d'exclusion appropriée. Pour retirer une règle d'exclusion, cliquez sur l'icône **Afficher les alertes exclues** ( ) pour afficher la boîte de dialogue Alertes exclues, sélectionnez les règles d'exclusion ou l'alerte exclue à restaurer, puis cliquez sur **Retirer**.

Résolution d'une alerte

Lenovo XClarity Administrator fournit des informations sur les actions appropriées à effectuer pour résoudre une alerte.

ProcédurePour résoudre une alerte, procédez comme suit.

Etape 1. Dans la barre de menus Lenovo XClarity Administrator, cliquez sur **Surveillance → Alertes** pour afficher la page Alertes.

Etape 2. Recherchez l'alerte dans le journal des alertes.

Etape 3. Cliquez sur le lien dans la colonne **Alerte** pour afficher des informations sur cette alerte (notamment une explication et des actions de récupération) et les propriétés de l'appareil qui est la source de l'alerte (telles que l'identificateur unique universel).

Etape 4. Exécutez les actions de récupération indiquées sous l'onglet **Détails** pour résoudre l'alerte. L'exemple suivant présente les actions de récupération pour un événement.

Modifiez le paramètre de stratégie de sécurité du châssis géré référencé pour qu'il corresponde à la stratégie de sécurité actuelle sur le serveur de gestion.

Pour modifier la stratégie de sécurité du châssis, ouvrez une session d'interface de ligne de commande sur le module Chassis Management Module (CMM), puis exécutez l'une des commandes suivantes :

- Pour définir le niveau de stratégie de sécurité sur `Secure` :
  ```
  security -p secure -T mm[p]
  ```
- Pour définir le niveau de stratégie de sécurité sur `Legacy` :
  ```
  security -p legacy -T mm[p]
  ```

Remarque : Si l'explication et les actions de récupération spécifiées pour une alerte ne sont pas affichées sous l'onglet **Détails**, accédez à Documentation en ligne de Lenovo Flex System, puis recherchez l'ID de l'alerte (par exemple, `FQXHMSE0004G`). Le site Web fournit toujours les toutes dernières informations.

Si vous suivez les actions recommandées et que le problème persiste, contactez le Lenovo Support.

Enregistrement d'alertes

Lorsqu'une alerte active est enregistrée, l'alerte est énumérée sur les pages dans lesquelles les alertes sont affichées, mais n'affecte pas le statut de gravité de l'appareil concerné.

Procédure

Pour enregistrer une alerte, procédez comme suit.

Etape 1. Dans la barre de menus Lenovo XClarity Administrator, cliquez sur **Surveillance → Alertes**. La page Alertes s'affiche.

Etape 2. Sélectionnez les alertes à enregistrer.

Etape 3. Cliquez sur l'icône **Enregistrer les alertes** ( ).

Après avoir terminé

- Vous pouvez afficher la liste des alertes enregistrées à la page Alertes en cliquant sur l'icône **Afficher les alertes exclues/enregistrées** ( ) pour afficher la boîte de dialogue Alertes exclues/enregistrées, puis en cliquant sur l'onglet **Alertes enregistrées**.
- Vous pouvez supprimer l'enregistrement d'une alerte active en cliquant sur l'icône **Afficher les alertes exclues/enregistrées** ( ) pour afficher la boîte de dialogue Alertes exclues/enregistrées, en cliquant sur l'onglet **Alertes enregistrées**, en sélectionnant les alertes, puis en cliquant sur l'icône **Supprimer l'enregistrement** ( ).

Utilisation des événements

Depuis Lenovo XClarity Administrator, vous avez accès à un journal des événements et un journal d'audit.

En savoir plus : XClarity Administrator : Surveillance

À propos de cette tâche

Le *journal des événements* fournit une liste historique de l'ensemble des événements de gestion et concernant le matériel.

Le *journal d'audit* fournit un enregistrement historique des actions utilisateur, comme la connexion à Lenovo XClarity Administrator, la création d'un utilisateur ou la modification d'un mot de passe utilisateur. Vous pouvez utiliser le journal d'audit pour suivre et consigner l'authentification et les commandes dans les systèmes informatiques.

Surveillance des événements dans le journal des événements

Le *journal des événements* fournit une liste historique de l'ensemble des événements de gestion et concernant le matériel.

À propos de cette tâche

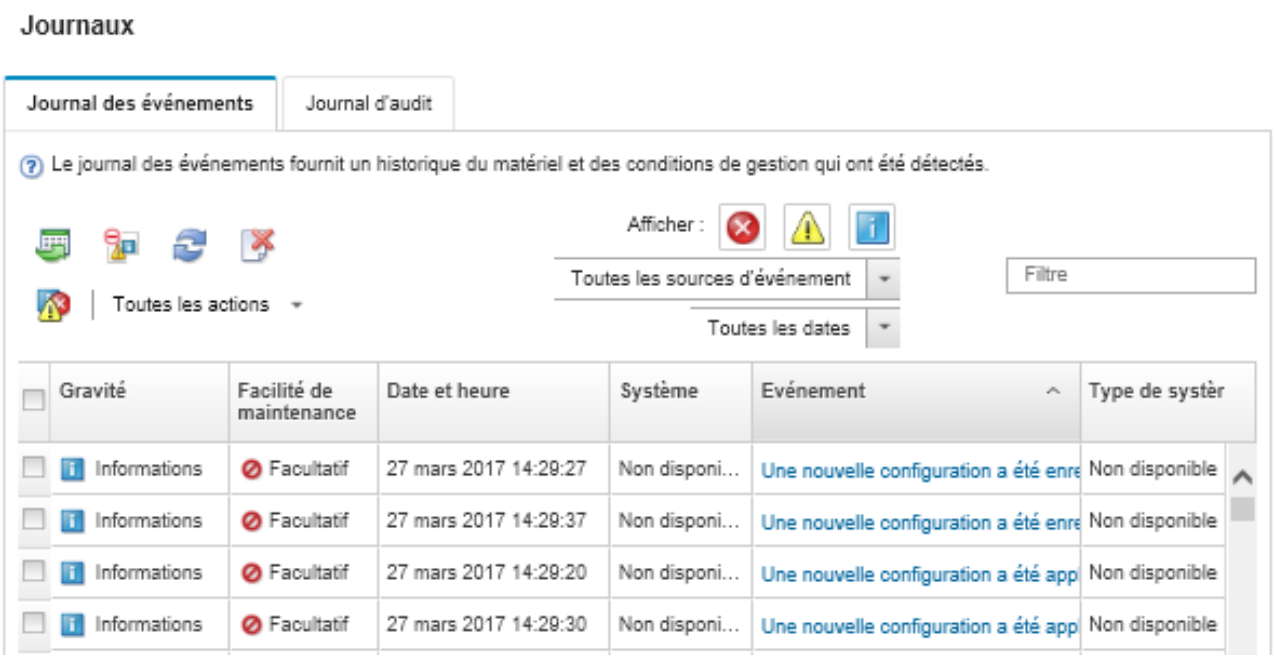
Le journal des événements contient des événements d'information et des événements autres que des événements d'information. Le nombre de chacun de ces événements varie jusqu'à atteindre le nombre maximum de 50 000 événements dans le journal des événements. À ce stade, il y a au maximum 25 000événements d'information et 25 000 événements autres que des événements d'information. Par exemple, il y a initialement 0 événement dans le journal des événements. Supposons que les événements suivants sont reçus : 20 000 événements d'information et 30 000 événements autres que des événements d'information. Lors de la réception d'un nouvel événement, l'événement d'information le plus ancien est supprimé même s'il existe un événement autre qu'un événement d'information plus ancien. À terme, le journal s'équilibre afin de contenir 25 000 événements de chaque type.

Lenovo XClarity Administrator envoie un événement lorsque le journal des événements atteint 80 % de la taille minimum et un autre événement lorsque la somme des entrées du journal des événements et du journal d'audit atteint 100 % de la taille maximum.

Astuce : Vous pouvez exporter le journal des événements pour être sûr de disposer d'un enregistrement complet de tous les événements matériel et de gestion. Pour exporter le journal des événements, cliquez sur l'icône **Exporter au format CSV** ( ).

Procédure

Pour afficher le journal des événements, cliquez sur **Surveillance → Journaux des événements** dans la barre de menus de Lenovo XClarity Administrator, puis cliquez sur l'onglet **Journal des événements**. La page Journal des événements s'affiche.



La colonne **Facilité de maintenance** indique si l'appareil a besoin d'une maintenance. Cette colonne peut contenir l'une des valeurs suivantes :

- **Non requis**. L'événement est de type Information et ne nécessite pas de maintenance.
- **Utilisateur**. Effectuez l'action de reprise appropriée afin de résoudre le problème.

  Pour afficher des informations sur un événement spécifique, cliquez sur le lien dans la colonne **Événement**. Une boîte de dialogue affiche des informations relatives aux propriétés de l'appareil qui a envoyé l'événement, des détails sur l'événement, ainsi que des actions de récupération.
- **Support**. Si l'Appel vers Lenovo est activé dans Lenovo XClarity Administrator, l'événement est généralement envoyé au Lenovo Centre de support à moins qu'un ticket de maintenance pour le même ID d'événement n'existe déjà pour l'appareil.

  Si l'Appel vers Lenovo n'est pas activé, il est recommandé d'ouvrir manuellement un ticket de maintenance pour résoudre le problème (voir Ouverture d'un ticket de maintenance dans la documentation en ligne de Lenovo XClarity Administrator).

Résultats

Dans la page Journal des événements, vous pouvez effectuer les actions suivantes :

- Affichez la source de l'événement en cliquant sur le lien dans la colonne **Source**.
- Actualiser la liste des événements en cliquant sur l'icône **Actualiser** ( ).

  Conseil : si de nouveaux événements sont détectés, le journal des événements s'actualise automatiquement toutes les 30 secondes.
- Effacez tous les événements dans le journal des événements en sélectionnant **Toutes les actions → Effacer le journal des événements**.
- Afficher des détails sur un événement spécifique en cliquant sur le lien de la colonne **Événement** puis sur l'onglet **Détails**.
- Exporter le journal des événements en cliquant sur l'icône **Exporter au format CSV** ( ).

Remarque : Les horodatages dans le journal exporté utilisent l'heure locale spécifiée par le navigateur Web.

- Excluez des événements spécifiques de toutes les pages sur lesquelles des événements s'affichent (voir Exclusion d'événements).
- Restreindre la liste des événements de gestion et concernant le matériel qui s'affichent sur la page actuelle :
  - Afficher ou masquer les événements d'un niveau de gravité spécifique en cliquant sur les icônes suivantes dans la liste déroulante :
    - Icône **Événements critiques** ()
    - Icône **Événements d'avertissement** ()
    - Icône **Événements d'information** ()
  - Afficher uniquement les événements provenant de sources spécifiques. Vous pouvez choisir l'une des options suivantes dans la liste déroulante :
    - Toutes les sources d'alerte
    - Événements matériels
    - Événements de gestion
    - Événements réparables
    - Événements client réparables
    - Événements non réparables
  - Afficher uniquement les événements avec une date et une heure spécifiques. Vous pouvez choisir l'une des options suivantes :
    - Toutes les dates
    - 2 heures précédentes
    - 24 heures précédentes
    - La semaine dernière
    - Le mois dernier
    - Custom

    Si vous sélectionnez **Personnalisé**, vous pouvez filtrer les événements de matériel et de gestion qui ont été générés entre une date de début personnalisée et la date actuelle.
  - Répertorier uniquement les événements qui contiennent un texte spécifique en indiquant le texte dans la zone **Filtre**.
  - Trier les événements par colonne en cliquant sur un en-tête de colonne.

Surveillance des événements dans le journal d'audit

Le *journal d'audit* fournit un enregistrement historique des actions utilisateur, comme la connexion à Lenovo XClarity Administrator, la création d'un utilisateur ou la modification d'un mot de passe utilisateur. Vous pouvez utiliser le journal d'audit pour suivre et consigner l'authentification et les commandes dans les systèmes informatiques.

À propos de cette tâche

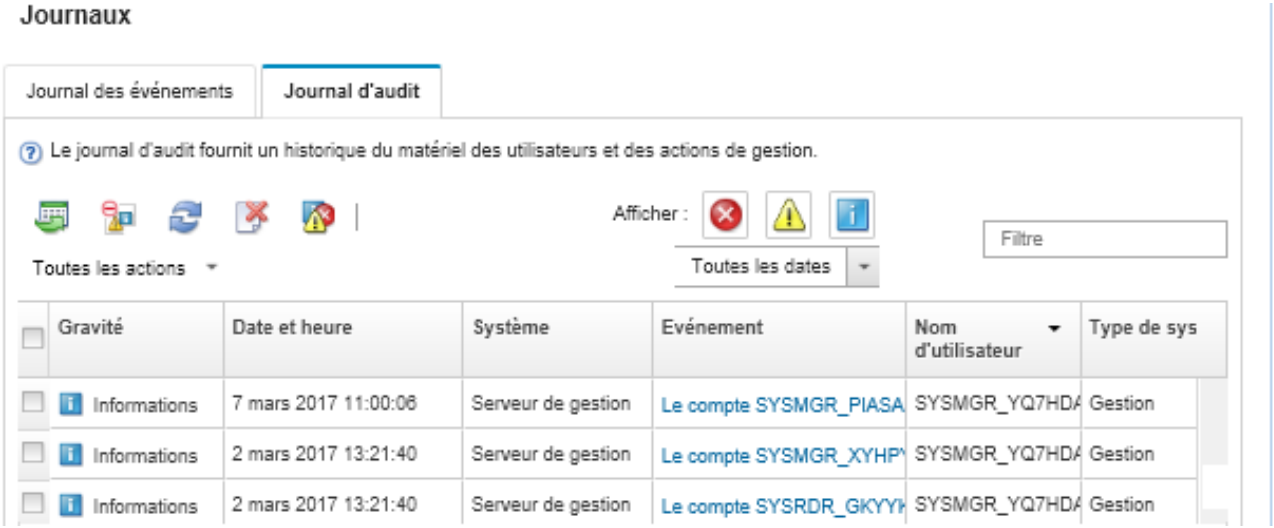
Le journal d'audit peut contenir au maximum 50 000 événements. Lorsque la taille maximum est atteinte, l'événement le plus ancien du journal est supprimé et le nouvel événement est ajouté au journal.

XClarity Administrator envoie un événement lorsque le journal d'audit atteint 80 % de la taille maximum et un autre événement lorsque la somme des entrées du journal des événements et du journal d'audit atteint 100 % de la taille maximum.

Astuce : vous pouvez exporter le journal d'audit pour être sûr de disposer d'un enregistrement complet de tous les événements d'audit. Pour exporter le journal d'audit, cliquez sur l'icône **Exporter au format CSV** ( ).

Procédure

Pour afficher le journal d'audit, cliquez sur **Surveillance → Journaux des événements** dans la barre de menus de XClarity Administrator, puis cliquez sur l'onglet **Journal d'audit**. La page Journal d'audit s'affiche.



Pour afficher des informations sur un événement d'audit spécifique, cliquez sur le lien dans la colonne **Événement**. Une boîte de dialogue affiche des informations relatives aux propriétés de l'appareil qui a envoyé l'événement, des détails sur l'événement, ainsi que des actions de récupération.

Résultats

Depuis cette page, vous pouvez effectuer les actions suivantes :

- Affichez la source de l'événement d'audit en cliquant sur le lien dans la colonne **Source**.
- Actualiser la liste des événements d'audit en cliquant sur l'icône **Actualiser** ( ).

  Conseil : si de nouveaux événements sont détectés, le journal des événements s'actualise automatiquement toutes les 30 secondes.
- Afficher des détails sur un événement d'audit spécifique en cliquant sur le lien de la colonne **Événement**, puis sur l'onglet **Détails**.
- Exporter le journal d'audit en cliquant sur l'icône **Exporter au format CSV** ( ).

  Remarque : Les horodatages dans le journal exporté utilisent l'heure locale spécifiée par le navigateur Web.
- Excluez des événements d'audit spécifiques de toutes les pages sur lesquelles des événements sont affichés (voir Exclusion d'événements).
- Restreindre la liste des événements d'audit qui s'affichent sur la page actuelle :
  - Afficher ou masquer les événements d'un niveau de gravité spécifique en cliquant sur les icônes suivantes :
    - Icône **Événements critiques** ( )

  - Icône **Événements d'avertissement** ()
  - Icône **Événements d'information** ()
- Afficher uniquement les événements avec une date et une heure spécifiques. Vous pouvez choisir l'une des options suivantes dans la liste déroulante :
  - Toutes les dates
  - 2 heures précédentes
  - 24 heures précédentes
  - La semaine dernière
  - Le mois dernier
  - Custom

  Si vous sélectionnez **Personnalisé**, vous pouvez filtrer les événements de matériel et de gestion qui ont été générés entre une date de début personnalisée et la date actuelle.
- Répertorier uniquement les événements qui contiennent un texte spécifique en indiquant le texte dans la zone **Filtre**.
- Trier les événements par colonne en cliquant sur un en-tête de colonne.

Résolution d'un événement

Lenovo XClarity Administrator fournit des informations sur les actions appropriées à effectuer pour résoudre un événement.

Procédure

Procédez comme suit pour résoudre un événement.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Surveillance → Journaux des événements** pour afficher la page Journaux.

Etape 2. Cliquez sur l'onglet **Journal des événements**.

Etape 3. Recherchez l'événement dans le journal des événements.

Etape 4. Cliquez sur le lien dans la colonne **Événement** pour afficher des informations sur cet événement (y compris une explication et les actions de reprise) et sur l'appareil qui est la source de l'événement.

Etape 5. Cliquez sur l'onglet **Détails**.

Etape 6. Exécutez les actions de reprise indiquées sous l'onglet **Détails** pour résoudre l'événement.

Remarque : Si l'explication et l'action de reprise d'un événement ne sont pas affichées, accédez au Documentation en ligne de Lenovo Flex System et effectuez une recherche sur le titre de l'événement. Le site Web fournit toujours les toutes dernières informations.

Si vous suivez les actions recommandées et que le problème persiste, contactez le Lenovo Support.

Exclusion d'événements

Si certains événements ne vous intéressent pas, vous pouvez les exclure de toutes les pages sur lesquelles les événements sont affichés. Les événements exclus figurent toujours dans le journal, mais ils sont masqués sur toutes les pages sur lesquelles les événements sont affichés.

À propos de cette tâche

Les événements exclus sont masqués pour tous les utilisateurs et non pas uniquement pour l'utilisateur qui a défini la configuration.

Vous pouvez placer les appareils en mode de maintenance, afin que tous les événements et alertes de ces appareils soient exclus (voir Placement des appareils en mode de maintenance).

Restriction : Seuls les utilisateurs disposant de droits d'administration peuvent exclure ou restaurer des événements.

Procédure

Procédez comme suit pour exclure des événements des journaux des événements.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Surveillance → Journaux des événements**, puis cliquez sur l'onglet **Journal des événements**. Le journal des événements s'affiche.

Etape 2. Sélectionnez les événements à exclure, puis cliquez sur l'icône **Exclure des événements** ( ). La boîte de dialogue Exclure des événements s'affiche.

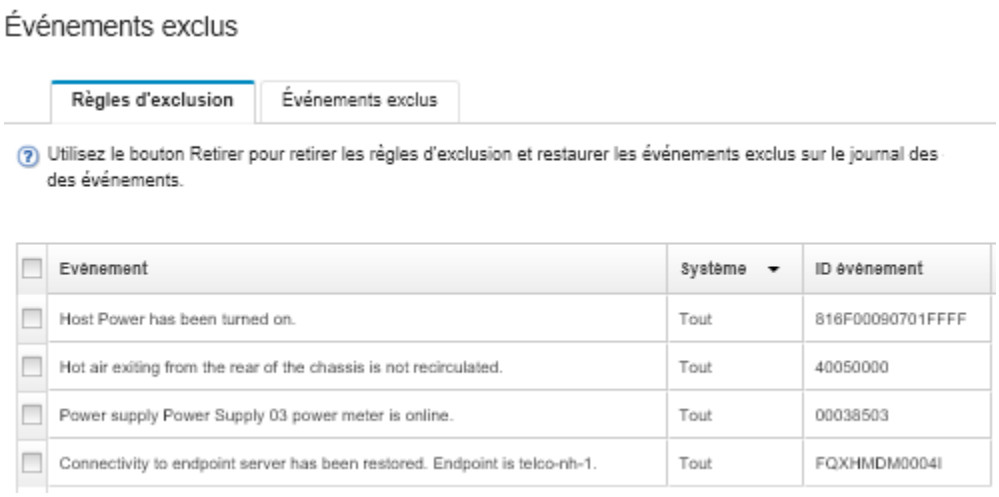
Etape 3. Sélectionnez l'une des options suivantes :
- **Exclure les événements sélectionnés de tous les systèmes**. Permet d'exclure les événements sélectionnés de tous les appareils gérés.
- **Exclure les événements uniquement des systèmes dans le champ de l'instance sélectionnée**. Permet d'exclure les événements sélectionnés des appareils gérés auxquels les événements sélectionnés s'appliquent.

Etape 4. Cliquez sur **Enregistrer**.

Après avoir terminé

Lorsque vous excluez des événements, Lenovo XClarity Administrator crée des règles d'exclusion à partir des informations que vous fournissez.

- Affichez une liste de règles d'exclusion et d'événements exclus à partir de la page Journaux en cliquant sur l'icône **Afficher les événements exclus** ( ). Dans la boîte de dialogue Événements exclus, cliquez sur l'onglet **Règles d'exclusion** pour afficher les règles d'exclusion ou cliquez sur l'onglet **Événements exclus** pour afficher les événements exclus.



- Restaurez des événements qui ont été exclus dans le journal des événements en retirant la règle d'exclusion appropriée. Pour retirer une règle d'exclusion, cliquez sur l'icône **Afficher les événements exclus** ( ) pour afficher la boîte de dialogue Événements exclus, sélectionnez les règles d'exclusion à restaurer, puis cliquez sur **Retirer les exclusions**.

- Empêchez les événements réparables qui figurent dans la liste des événements exclus d'ouvrir automatiquement des rapports d'incidents en cliquant sur **Administration → Service et support** dans la barre de menus Lenovo XClarity Administrator, en cliquant sur l'onglet **Réexpéditeurs de service**, puis en répondant **Non** à la question **Voulez-vous que des événements exclus ouvrent des rapports d'incidents ?**.

Acheminement des événements

Vous pouvez configurer Lenovo XClarity Administrator pour acheminer des événements vers des appareils mobiles et vers les applications connectées présentes dans votre environnement afin de regrouper et surveiller l'état du matériel et les problèmes d'exécution pour votre environnement matériel.

En savoir plus : XClarity Administrator : Surveillance

Acheminement des événements vers syslog, un gestionnaire SNMP distant, un e-mail et d'autres services d'événement

Vous pouvez configurer Lenovo XClarity Administrator pour acheminer des événements vers les applications connectées présentes dans votre environnement afin de regrouper et surveiller l'état du matériel et les problèmes d'exécution pour votre environnement matériel. Vous pouvez définir la portée des événements à acheminer en fonction des appareils, des classes d'événements, du niveau de gravité des événements et des composants.

À propos de cette tâche

Lenovo XClarity Administrator peut acheminer des événements vers un ou plusieurs appareils. Concernant les événements d'audit, vous pouvez choisir d'acheminer la totalité ou aucun des événements de ce type. Vous ne pouvez pas acheminer des événements d'audit spécifiques. Concernant les événements matériel et de gestion, vous pouvez choisir d'acheminer des événements liés à un ou plusieurs niveaux de gravité (Critique, Avertissement et Information) et à un ou plusieurs composants (par exemple, des unités de disque, des processeurs et des adaptateurs).

Lenovo XClarity Administrator utilise des systèmes d'acheminement d'événement pour acheminer les événements. Un *système d'acheminement d'événement* contient des informations sur le protocole à utiliser, le destinataire, les appareils à surveiller et les événements à acheminer. Après que vous avez créé et activé un système d'acheminement d'événement, Lenovo XClarity Administrator démarre la surveillance d'événements entrants selon des critères de filtrage. Lorsqu'une concordance est trouvée, le protocole associé est utilisé pour acheminer l'événement.

Les protocoles suivants sont pris en charge :

- **Analyse de journal Azure**. Lenovo XClarity Administrator achemine les événements surveillés via le réseau versAnalyse de journal Microsoft Azure.
- **E-mail**. Lenovo XClarity Administrator achemine les événements surveillés vers une ou plusieurs adresses e-mail à l'aide de SMTP. L'e-mail contient des informations sur l'événement, le nom d'hôte de l'appareil source, ainsi que des liens vers l'interface Web Lenovo XClarity Administrator et l'application Lenovo XClarity Mobile.
- **FTP**. Achemine les événements surveillés via le réseau vers un serveur FTP.
- **REST**. Lenovo XClarity Administrator achemine les événements surveillés via le réseau vers un site Web REST.
- **SNMP**. Lenovo XClarity Administrator achemine les événements surveillés via le réseau vers un gestionnaire SNMP distant. Les alertes SNMPv1 et SNMPv3 sont prises en charge.

Pour plus d'informations sur le fichier de base d'informations de gestion (MIB) qui décrit les alertes SNMP générées par Lenovo XClarity Administrator, voir le fichier lenovoMgrAlert.mibFichier lenovoMgrAlert.mib dans la documentation en ligne de Lenovo XClarity Administrator.

- **Syslog**. Lenovo XClarity Administrator achemine les événements surveillés via le réseau vers un serveur de journaux centralisé sur lequel des outils natifs peuvent être utilisés pour surveiller syslog.

Vous pouvez créer et activer jusqu'à 20 système d'acheminement d'événement pour l'envoi d'événements à des destinataires spécifiques.

Si XClarity Administrator est réamorcé après la configuration des systèmes d'acheminement d'événement, vous devez attendre que le serveur de gestion regénère des données internes pour que les événements soient correctement acheminés.

À compter de XClarity Administrator version 1.2.0, la zone **Commutateurs** est incluse sur l'onglet **Événements** dans les boîtes de dialogue Nouveau système d'acheminement d'événement et Modifier les systèmes d'acheminement d'événement. Si vous avez effectué une mise à niveau vers la version 1.2.0 ou une version ultérieure à partir d'une édition antérieure, pensez à mettre à jour vos systèmes d'acheminement d'événement de manière à inclure ou exclure les événements RackSwitch, le cas échéant. Cette action est nécessaire même si vous avez coché la case **Tous les systèmes** pour sélectionner tous les appareils.

Remarque : Les événements ne sont pas distribués si, par exemple, la connectivité entre Lenovo XClarity Administrator et le système d'acheminement d'événement est arrêtée ou si le port est bloqué.

Configuration de l'acheminement d'événement vers Analyse de journal Azure

Vous pouvez configurer Lenovo XClarity Administrator pour l'acheminement d'événements spécifiques vers Analyse de journal Azure.

À propos de cette tâche

Vous pouvez créer et activer jusqu'à 20 système d'acheminement d'événement pour l'envoi d'événements à des destinataires spécifiques.

Si XClarity Administrator est réamorcé après la configuration des systèmes d'acheminement d'événement, vous devez attendre que le serveur de gestion regénère des données internes pour que les événements soient correctement acheminés.

Remarque : À compter de XClarity Administrator version 1.2.0, la zone **Commutateurs** est incluse sur l'onglet **Événements** dans les boîtes de dialogue Nouveau système d'acheminement d'événement et Modifier les systèmes d'acheminement d'événement. Si vous avez effectué une mise à niveau vers la version 1.2.0 ou une version ultérieure à partir d'une édition antérieure, pensez à mettre à jour vos systèmes d'acheminement d'événement de manière à inclure ou exclure les événements RackSwitch, le cas échéant. Cette action est nécessaire même si vous avez coché la case **Tous les systèmes** pour sélectionner tous les appareils.

Procédure

Procédez comme suit pour créer un système d'acheminement d'événement pour Analyse de journal Azure.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez **Surveillance → Acheminement d'événement**. La page Acheminement d'événement s'affiche.

Etape 2. Cliquez sur l'onglet **Réexpéditeur d'événement**.

Etape 3. Cliquez sur l'icône **Créer** ( ). L'onglet **Général** de la boîte de dialogue Nouveau système d'acheminement d'événement s'affiche.

Etape 4. Sélectionnez **Analyse de journal Azure** comme type de système d'acheminement d'événement, puis indiquez les informations spécifiques au protocole :

- Entrez le nom et la description facultative du système d'acheminement d'événement.
- Entrez la clé principale de l'interface Analyse de journal Azure.
- Entrez le délai d'attente (en secondes) pour la demande. La valeur par défaut est 30 secondes.
- **Facultatif** : Si l'authentification est requise, sélectionnez l'un des types d'authentification suivants :
  - **Base**. Effectue l'authentification auprès du serveur spécifié à l'aide de l'ID utilisateur et du mot de passe spécifiés.
  - **Aucun**. Aucune authentification n'est utilisée.

Etape 5. Cliquez sur **Format de sortie** pour choisir le format de sortie des données d'événements à acheminer. Les informations varient pour chaque type de système d'acheminement d'événement.

L'exemple de format de sortie suivante est le format par défaut pour les destinataires Analyse de journal Azure. Tous les mots entre crochets doubles sont les variables qui sont remplacées par des valeurs réelles lors de l'acheminement d'un événement. Les variables disponibles pour les destinataires Analyse de journal Azure sont répertoriées dans la boîte de dialogue Format de sortie.

```
{\"Msg\":\"[[EventMessage]]\",\"EventID\":\"[[EventID]]\",\"Serialnum\":
\"[[EventSerialNumber]]\",\"SenderUUID\":\"[[EventSenderUUID]]\",\"Flags\":
\"[[EventFlags]]\",\"Userid\":\"[[EventUserName]]\",\"LocalLogID\":
\"[[EventLocalLogID]]\",\"DeviceName\":\"[[DeviceFullPathName]]\",\"SystemName\":
\"[[SystemName]]\",\"Action\":\"[[EventAction]]\",\"FailFRUs\":
\"[[EventFailFRUs]]\",\"Severity\":\"[[EventSeverity]]\",\"SourceID\":
\"[[EventSourceUUID]]\",\"SourceLogSequence\":[[EventSourceLogSequenceNumber]],
\"FailSNs\":\"[[EventFailSerialNumbers]]\",\"FailFRUUUIDs\":
\"[[EventFailFRUUUIDs]]\",\"EventClass\":\"[[EventClass]]\",\"ComponentID\":
\"[[EventComponentUUID]]\",\"Mtm\":\"[[EventMachineTypeModel]]\",\"MsgID\":
\"[[EventMessageID]]\",\"SequenceNumber\":\"[[EventSequenceID]]\",\"TimeStamp\":
\"[[EventTimeStamp]]\",\"Args\":[[EventMessageArguments]],\"Service\":
\"[[EventService]]\",\"CommonEventID\":\"[[CommonEventID]]\",\"EventDate\":
\"[[EventDate]]\",\"EventSource\":\"[[EventSource]]\",\"DeviceSerialNumber\":
\"[[DeviceSerialNumber]]\",\"DeviceIPAddress\":\"[[DeviceIPAddress]]\",
\"LXCA\":\"[[LXCA_IP]]\"}
```

Vous pouvez cliquer sur **Réinitialiser aux valeurs par défaut** pour rétablir le format de sortie dans les zones par défaut.

Etape 6. Cliquez sur le bouton **Autoriser les événements exclus** pour autoriser ou empêcher le transfert des événements exclus.

Etape 7. Sélectionnez **Activer ce réexpéditeur** pour activer l'acheminement d'événement pour ce système d'acheminement d'événement.

Etape 8. Cliquez sur **Suivant** pour afficher l'onglet **Appareils**.

Etape 9. Sélectionnez les appareils et les groupes que vous souhaitez surveiller pour ce système d'acheminement d'événement.

Astuce : Pour acheminer des événements pour tous les appareils gérés (actuels et ultérieurs), cochez la case **Faire correspondre tous les systèmes**.Si vous ne cochez pas la case **Faire correspondre tous les systèmes**, assurez-vous que la colonne UUID des appareils sélectionnés ne contient pas d'UUID factice. Un UUID factice est affecté aux appareils qui n'ont pas encore été récupérés après un redémarrage ou qui ne sont pas complètement reconnus par le serveur de gestion. Si vous sélectionnez un appareil doté d'un UUID factice, l'acheminement d'événement

fonctionne pour cet appareil jusqu'à ce que celui-ci soit complètement reconnu ou récupéré et que l'UUID factice soit remplacé par un UUID réel.

Etape 10. Cliquez sur **Suivant** pour afficher la page **Evénements**.

Etape 11. Sélectionnez les filtres à utiliser pour ce système d'acheminement d'événement.

- **Correspondance par catégorie d'événement**.
  1. Pour acheminer tous les événements d'audit, quel que soit le niveau de l'état, sélectionnez **Inclure tous les événements d'audit**.
  2. Pour acheminer tous les événements de garantie, sélectionnez **Inclure les événements de garantie**.
  3. Pour acheminer tous les événements de modification de l'état de santé, sélectionnez **Inclure les événements de changement d'état**.
  4. Pour acheminer tous les événements de mise à jour de l'état de santé, sélectionnez **Inclure les événements de mise à jour d'état**.
  5. Sélectionnez les classes d'événement et le niveau de facilité de maintenance à acheminer.
  6. Entrez les ID d'un ou de plusieurs événements à exclure de l'acheminement. Séparez-les à l'aide d'une virgule (par exemple, `FQXHMEM0214I,FQXHMEM0214I`).
- **Correspondance par code d'événement**. Entrez les ID d'un ou de plusieurs événements à acheminer. Si vous entrez plusieurs ID, séparez-les à l'aide d'une virgule.
- **Exclusion par catégorie d'événement**.
  1. Pour exclure tous les événements d'audit, quel que soit le niveau de l'état, sélectionnez **Exclure tous les événements d'audit**.
  2. Pour exclure tous les événements de garantie, sélectionnez **Exclure les événements de garantie**.
  3. Pour exclure tous les événements de modification de l'état de santé, sélectionnez **Exclure les événements de changement d'état**.
  4. Pour exclure tous les événements de mise à jour de l'état de santé, sélectionnez **Exclure les événements de mise à jour d'état**.
  5. Sélectionnez les classes d'événement et le niveau de facilité de maintenance à exclure.
  6. Entrez les ID d'un ou de plusieurs événements à acheminer. Séparez-les à l'aide d'une virgule.
- **Exclusion par code d'événement**. Entrez les ID d'un ou de plusieurs événements à exclure. Si vous entrez plusieurs ID, séparez-les à l'aide d'une virgule.

Etape 12. Choisissez d'inclure ou non certains types d'événements.

- **Inclure tous les événements d'audit**. Envoie des notifications à propos des événements d'audit, sur la base des catégories et des gravités sélectionnées pour les événements.
- **Inclure les événements de garantie**. Envoie des notifications à propos des garanties.
- **Inclure les événements de modification d'état**. Envoie des notifications à propos des modifications d'état.
- **Inclure les événements de mise à jour d'état**. Notifications envoyées au sujet de nouvelles alertes.
- **Inclure les événements du bulletin**. Envoie des notifications à propos des nouveaux bulletins.

Etape 13. Sélectionnez les types d'événements et les gravités pour lesquels vous souhaitez recevoir une notification.

Etape 14. Sélectionnez si oui ou non vous souhaitez filtrer les événements en fonction de la facilité de maintenance.

Etape 15. Cliquez sur **Suivant** pour afficher la page **Planificateur**.

Etape 16. **Facultatif :** Définissez les heures et les jours auxquels vous souhaitez que les événements spécifiés soient acheminés vers ce système d'acheminement d'événement. Seuls les événements qui se produisent pendant le créneau horaire indiqué sont acheminés.

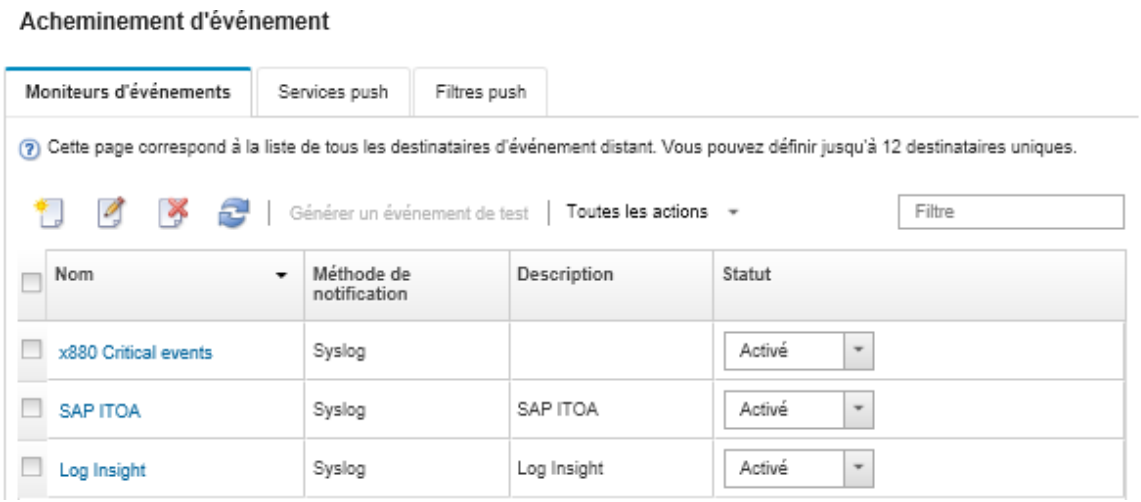
Si vous ne créez pas de planning pour le système d'acheminement d'événement, les événements sont acheminés 24h/24 et 7j/7.

1. Utilisez l'icône **Défiler vers la gauche** (◀) et l'icône **Défiler vers la droite** (▶), ainsi que les boutons **Jour**, **Semaine** et **Mois** pour définir le jour et l'heure de début du planning.
2. Cliquez deux fois sur le créneau horaire pour ouvrir la boîte de dialogue Nouvelle période.
3. Indiquez les informations requises, y compris la date et les heures de début et de fin et précisez si le planning est répétitif.
4. Cliquez sur **Créer** pour enregistrer le planning et fermer la boîte de dialogue. Le nouveau planning est ajouté au calendrier.

Astuce :
- Vous pouvez modifier le créneau horaire en faisant glisser l'entrée du planning vers un autre créneau horaire du calendrier.
- Vous pouvez modifier la durée en sélectionnant le haut ou le bas de l'entrée de planning et en le faisant glisser vers la nouvelle heure dans le calendrier.
- Vous pouvez modifier l'heure de fin en sélectionnant le bas de l'entrée de planning et en le faisant glisser vers la nouvelle heure dans le calendrier.
- Vous pouvez modifier un planning en cliquant deux fois sur l'entrée de planning et en cliquant sur **Éditer l'entrée**.
- Vous pouvez afficher un résumé de toutes les entrées de planning en sélectionnant **Afficher le récapitulatif du planificateur**. Le récapitulatif comprend le créneau horaire pour chaque entrée et indique les entrées qui sont répétables.
- Vous pouvez supprimer une entrée de planning du calendrier ou planifier un récapitulatif en sélectionnant l'entrée, puis en cliquant sur **Supprimer une entrée**.

Etape 17. Cliquez sur **Créer**.

Le système d'acheminement d'événement figure dans le tableau Acheminement d'événement.



Etape 18. Sélectionnez le nouveau système d'acheminement d'événement, cliquez sur **Générer un événement de test**, puis assurez-vous que les événements sont acheminés correctement vers le serveur Analyse de journal Azure approprié.

Après avoir terminé

Sur la page Acheminement d'événement, vous pouvez effectuer les actions suivantes sur un système d'acheminement d'événement sélectionné.

- Actualiser la liste des systèmes d'acheminement d'événement en cliquant sur l'icône **Actualiser** ().
- Afficher les détails relatifs à un système d'acheminement d'événement spécifique en cliquant sur le lien dans la colonne **Nom**.
- Modifier les propriétés et les critères de filtrage d'un système d'acheminement d'événement en cliquant sur le nom de celui-ci dans la colonne **Nom**.
- Supprimer le système d'acheminement d'événement en cliquant sur l'icône **Supprimer** ().
- Suspendre l'acheminement d'événement (voir Interruption de l'acheminement d'événement).

Configuration de l'acheminement d'événement vers un un service de messagerie utilisant SMTP

Vous pouvez configurer Lenovo XClarity Administrator pour acheminer des événements spécifiques vers un service de messagerie utilisant SMTP.

Avant de commencer

Pour permettre l'acheminement d'un e-mail vers un service de messagerie Web (par exemple, Gmail, Hotmail ou Yahoo), votre serveur SMTP doit prendre en charge l'acheminement d'e-mails sur le Web.

Avant de configurer un système d'acheminement d'événement vers un service Web Gmail, passez en revue les informations décrites dans Configuration de l'acheminement d'événement vers un serveur SMTP GmailConfiguration de l'acheminement d'événement vers syslog, un gestionnaire SNMP distant ou un e-mail dans la documentation en ligne de Lenovo XClarity Administrator.

À propos de cette tâche

Vous pouvez créer et activer jusqu'à 20 système d'acheminement d'événement pour l'envoi d'événements à des destinataires spécifiques.

Si XClarity Administrator est réamorcé après la configuration des systèmes d'acheminement d'événement, vous devez attendre que le serveur de gestion regénère des données internes pour que les événements soient correctement acheminés.

Remarque : À compter de XClarity Administrator version 1.2.0, la zone **Commutateurs** est incluse sur l'onglet **Événements** dans les boîtes de dialogue Nouveau système d'acheminement d'événement et Modifier les systèmes d'acheminement d'événement. Si vous avez effectué une mise à niveau vers la version 1.2.0 ou une version ultérieure à partir d'une édition antérieure, pensez à mettre à jour vos systèmes d'acheminement d'événement de manière à inclure ou exclure les événements RackSwitch, le cas échéant. Cette action est nécessaire même si vous avez coché la case **Tous les systèmes** pour sélectionner tous les appareils.

Procédure

Procédez comme suit pour créer un système d'acheminement d'événement pour un service de messagerie utilisant SMTP.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez **Surveillance → Acheminement d'événement**. La page Acheminement d'événement s'affiche.

Etape 2. Cliquez sur l'onglet **Réexpéditeur d'événement**.

Etape 3. Cliquez sur l'icône **Créer** ( ). L'onglet **Général** de la boîte de dialogue Nouveau système d'acheminement d'événement s'affiche.

Etape 4. Sélectionnez **E-mail** comme type de système d'acheminement d'événement, puis indiquez les informations spécifiques au protocole :

- Entrez le nom, l'hôte de destination et la description facultative du système d'acheminement d'événement.
- Entrez le port à utiliser pour l'acheminement des événements. La valeur par défaut est `25`.
- Entrez le délai d'attente (en secondes) pour la demande. La valeur par défaut est 30 secondes.
- Entrez l'adresse e-mail de chaque destinataire. Si vous entrez plusieurs adresses e-mail, séparez-les à l'aide d'une virgule.

  Pour envoyer l'e-mail au contact de support qui est affecté pour l'appareil, sélectionnez **Utiliser le ou les e-mails de contact de support** (voir Définition des contacts de support pour un appareil dans la documentation en ligne de XClarity Administrator).
- **Facultatif :** Entrez l'adresse e-mail de l'expéditeur de l'e-mail (par exemple, `john@company.com`).

  Si vous ne spécifiez pas d'adresse e-mail, l'adresse de l'expéditeur est `LXCA.`<*source_identifier*>`@`<*smtp_host*> par défaut.

  Si vous spécifiez uniquement le domaine de l'expéditeur, le format de l'adresse de l'expéditeur est <*LXCA_host_name*>`@`<*sender_domain*> (par exemple, XClarity1@company.com).

  Remarques :

  – Si vous configurez votre serveur SMTP de telle sorte qu'un nom d'hôte est requis pour l'acheminement des e-mails et que vous ne configurez pas de nom d'hôte pour XClarity Administrator, les événements acheminés seront peut-être rejetés par le serveur SMTP. Si XClarity Administrator ne possède pas de nom d'hôte, l'événement est acheminé à l'aide de l'adresse IP. Si l'adresse IP ne peut pas être obtenue, « localhost » est envoyé à la place, ce qui peut entraîner le rejet de l'événement par le serveur SMTP.

  – Si vous spécifiez le domaine de l'expéditeur, la source n'est pas identifiée dans l'adresse de l'expéditeur. En revanche, des informations sur la source de l'événement sont incluses dans le corps de l'e-mail, y compris le nom de système, l'adresse IP, le type/modèle et le numéro de série.

  – Si le serveur SMTP accepte uniquement les e-mails qui ont été envoyés par un utilisateur enregistré, l'adresse d'expéditeur par défaut (`LXCA.`<*source_identifier*>`@`<*smtp_host*>) est rejetée. Dans ce cas, vous devez indiquer au moins un nom de domaine dans la zone **Depuis l'adresse**.
- **Facultatif :** Pour établir une connexion sécurisée au serveur SMTP, sélectionnez les types de connexion suivants :
  – **SSL**. Utilise le protocole SSL lors de la communication.
  – **STARTTLS**. Utilise TLS pour établir une communication sécurisée via un canal non sécurisé.

  Si l'un de ces types de connexion est sélectionné, LXCA tente de télécharger et d'importer le certificat du serveur SMTP dans son fichier de clés certifiées. Vous êtes invité à accepter l'ajout de ce certificat dans le fichier de clés certifiées.
- **Facultatif :** Si l'authentification est requise, sélectionnez l'un des types d'authentification suivants :
  – **Normal**. Effectue l'authentification auprès du serveur SMTP spécifié à l'aide de l'ID utilisateur et du mot de passe spécifiés.
  – **NTLM**. Utilise le protocole NTLM (NT LAN Manager) pour l'authentification auprès du serveur SMTP spécifié à l'aide de l'ID utilisateur, du mot de passe et du nom de domaine spécifiés.

– **OAUTH2**. Utilise le protocole SASL (Simple Authentication and Security Layer) pour l'authentification auprès du serveur SMTP spécifié à l'aide du nom d'utilisateur et du jeton de sécurité spécifiés. Généralement, le nom d'utilisateur correspond à l'adresse e-mail.

  Attention : Le jeton de sécurité expire au terme d'un courte période. Il est de votre responsabilité d'actualiser le jeton de sécurité.
– **Aucun**. Aucune authentification n'est utilisée.

Etape 5. Cliquez sur **Format de sortie** pour choisir le format de sortie des données d'événement à acheminer dans le corps de l'e-mail et le format de l'objet de l'e-mail. Les informations varient pour chaque type de système d'acheminement d'événement.

L'exemple de format de sortie suivante est le format par défaut pour les destinataires email. Tous les mots entre crochets doubles sont les variables qui sont remplacées par des valeurs réelles lors de l'acheminement d'un événement. Les variables disponibles pour les destinataires email sont répertoriées dans la boîte de dialogue Format de sortie.

Objet de l'e-mail

```
[[DeviceName]]-[[EventMessage]]
```

Corps de l'e-mail

```
Alert: [[EventDate]] [[EventMessage]]\n
\n
Hardware Information:\n
Managed Endpoint    : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
Device name          : [[DeviceName]]\n
Product name         : [[DeviceProductName]]\n
Host name            : [[DeviceHostName]]\n
Machine Type         : [[DeviceMachineType]]\n
Machine Model        : [[DeviceMachineModel]]\n
Serial Number        : [[DeviceSerialNumber]]\n
DeviceHealthStatus   : [[DeviceHealthStatus]]\n
IPv4 addresses       : [[DeviceIPV4Addresses]]\n
IPv6 addresses       : [[DeviceIPV6Addresses]]\n
Chassis              : [[DeviceChassisName]]\n
DeviceBays           : [[DeviceBays]]\n
\n
LXCA is: [[ManagementServerIP]]\n
\n
Event Information:\n
  Event ID         : [[EventID]]\n
  Common Event ID : [[CommonEventID]]\n
  EventSeverity    : [[EventSeverity]]\n
  Event Class      : [[EventClass]]\n
  Sequence ID      : [[EventSequenceID]]\n
  Event Source ID : [[EventSourceUUID]]\n
  Component ID     : [[EventComponentUUID]]\n
  Serial Num       : [[EventSerialNumber]]\n
  MTM              : [[EventMachineTypeModel]]\n
  EventService     : [[EventService]]\n
  Console link     : [[ConsoleLink]]\n
  iOS link         : [[iOSLink]]\n
  Android link     : [[AndroidLink]]\n
  System Name      : [[DeviceFullPathName]]\n
```

Vous pouvez cliquer sur **Réinitialiser aux valeurs par défaut** pour rétablir le format de sortie dans les zones par défaut.

Etape 6. Cliquez sur le bouton **Autoriser les événements exclus** pour autoriser ou empêcher le transfert des événements exclus.

Etape 7. Sélectionnez **Activer ce réexpéditeur** pour activer l'acheminement d'événement pour ce système d'acheminement d'événement.

Etape 8. Cliquez sur **Suivant** pour afficher l'onglet **Appareils**.

Etape 9. Sélectionnez les appareils et les groupes que vous souhaitez surveiller pour ce système d'acheminement d'événement.

Astuce : Pour acheminer des événements pour tous les appareils gérés (actuels et ultérieurs), cochez la case **Faire correspondre tous les systèmes**.Si vous ne cochez pas la case **Faire correspondre tous les systèmes**, assurez-vous que la colonne UUID des appareils sélectionnés ne contient pas d'UUID factice. Un UUID factice est affecté aux appareils qui n'ont pas encore été récupérés après un redémarrage ou qui ne sont pas complètement reconnus par le serveur de gestion. Si vous sélectionnez un appareil doté d'un UUID factice, l'acheminement d'événement fonctionne pour cet appareil jusqu'à ce que celui-ci soit complètement reconnu ou récupéré et que l'UUID factice soit remplacé par un UUID réel.

Etape 10. Cliquez sur **Suivant** pour afficher la page **Evénements**.

Etape 11. Sélectionnez les filtres à utiliser pour ce système d'acheminement d'événement.

- **Correspondance par catégorie d'événement**.
  1. Pour acheminer tous les événements d'audit, quel que soit le niveau de l'état, sélectionnez **Inclure tous les événements d'audit**.
  2. Pour acheminer tous les événements de garantie, sélectionnez **Inclure les événements de garantie**.
  3. Pour acheminer tous les événements de modification de l'état de santé, sélectionnez **Inclure les événements de changement d'état**.
  4. Pour acheminer tous les événements de mise à jour de l'état de santé, sélectionnez **Inclure les événements de mise à jour d'état**.
  5. Sélectionnez les classes d'événement et le niveau de facilité de maintenance à acheminer.
  6. Entrez les ID d'un ou de plusieurs événements à exclure de l'acheminement. Séparez-les à l'aide d'une virgule (par exemple, `FQXHMEM0214I,FQXHMEM0214I`).
- **Correspondance par code d'événement**. Entrez les ID d'un ou de plusieurs événements à acheminer. Si vous entrez plusieurs ID, séparez-les à l'aide d'une virgule.
- **Exclusion par catégorie d'événement**.
  1. Pour exclure tous les événements d'audit, quel que soit le niveau de l'état, sélectionnez **Exclure tous les événements d'audit**.
  2. Pour exclure tous les événements de garantie, sélectionnez **Exclure les événements de garantie**.
  3. Pour exclure tous les événements de modification de l'état de santé, sélectionnez **Exclure les événements de changement d'état**.
  4. Pour exclure tous les événements de mise à jour de l'état de santé, sélectionnez **Exclure les événements de mise à jour d'état**.
  5. Sélectionnez les classes d'événement et le niveau de facilité de maintenance à exclure.
  6. Entrez les ID d'un ou de plusieurs événements à acheminer. Séparez-les à l'aide d'une virgule.
- **Exclusion par code d'événement**. Entrez les ID d'un ou de plusieurs événements à exclure. Si vous entrez plusieurs ID, séparez-les à l'aide d'une virgule.

Etape 12. Choisissez d'inclure ou non certains types d'événements.

- **Inclure tous les événements d'audit**. Envoie des notifications à propos des événements d'audit, sur la base des catégories et des gravités sélectionnées pour les événements.

- **Inclure les événements de garantie**. Envoie des notifications à propos des garanties.
- **Inclure les événements de modification d'état**. Envoie des notifications à propos des modifications d'état.
- **Inclure les événements de mise à jour d'état**. Notifications envoyées au sujet de nouvelles alertes.
- **Inclure les événements du bulletin**. Envoie des notifications à propos des nouveaux bulletins.

Etape 13. Sélectionnez les types d'événements et les gravités pour lesquels vous souhaitez recevoir une notification.

Etape 14. Sélectionnez si oui ou non vous souhaitez filtrer les événements en fonction de la facilité de maintenance.

Etape 15. Cliquez sur **Suivant** pour afficher la page **Planificateur**.

Etape 16. **Facultatif :** Définissez les heures et les jours auxquels vous souhaitez que les événements spécifiés soient acheminés vers ce système d'acheminement d'événement. Seuls les événements qui se produisent pendant le créneau horaire indiqué sont acheminés.

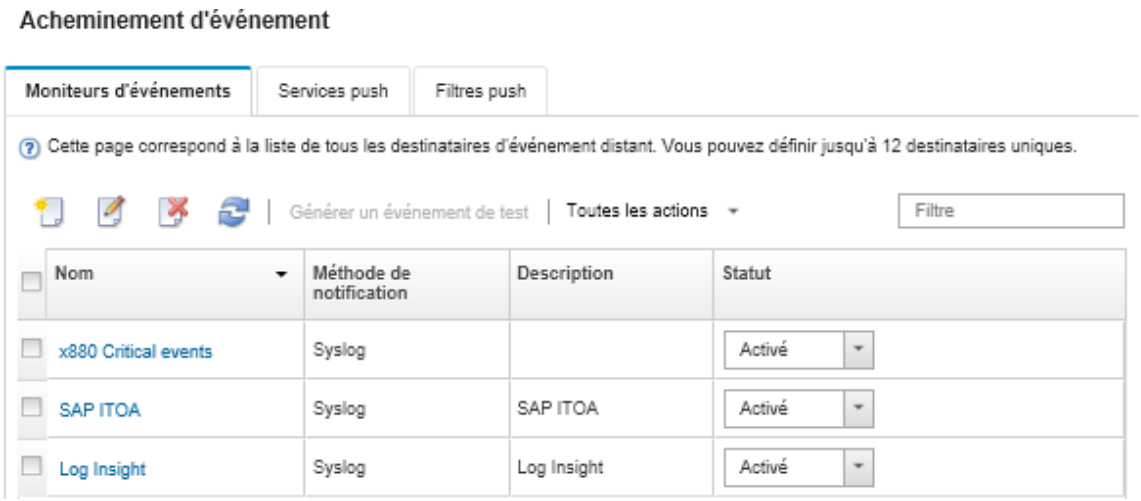
Si vous ne créez pas de planning pour le système d'acheminement d'événement, les événements sont acheminés 24h/24 et 7j/7.

1. Utilisez l'icône **Défiler vers la gauche** (◀) et l'icône **Défiler vers la droite** (▶), ainsi que les boutons **Jour**, **Semaine** et **Mois** pour définir le jour et l'heure de début du planning.
2. Cliquez deux fois sur le créneau horaire pour ouvrir la boîte de dialogue Nouvelle période.
3. Indiquez les informations requises, y compris la date et les heures de début et de fin et précisez si le planning est répétitif.
4. Cliquez sur **Créer** pour enregistrer le planning et fermer la boîte de dialogue. Le nouveau planning est ajouté au calendrier.

Astuce :
- Vous pouvez modifier le créneau horaire en faisant glisser l'entrée du planning vers un autre créneau horaire du calendrier.
- Vous pouvez modifier la durée en sélectionnant le haut ou le bas de l'entrée de planning et en le faisant glisser vers la nouvelle heure dans le calendrier.
- Vous pouvez modifier l'heure de fin en sélectionnant le bas de l'entrée de planning et en le faisant glisser vers la nouvelle heure dans le calendrier.
- Vous pouvez modifier un planning en cliquant deux fois sur l'entrée de planning et en cliquant sur **Éditer l'entrée**.
- Vous pouvez afficher un résumé de toutes les entrées de planning en sélectionnant **Afficher le récapitulatif du planificateur**. Le récapitulatif comprend le créneau horaire pour chaque entrée et indique les entrées qui sont répétables.
- Vous pouvez supprimer une entrée de planning du calendrier ou planifier un récapitulatif en sélectionnant l'entrée, puis en cliquant sur **Supprimer une entrée**.

Etape 17. Cliquez sur **Créer**.

Le système d'acheminement d'événement figure dans le tableau Acheminement d'événement.



Etape 18. Sélectionnez le nouveau système d'acheminement d'événement, cliquez sur **Générer un événement de test**, puis assurez-vous que les événements sont acheminés correctement vers le service de messagerie approprié.

Après avoir terminé

Sur la page Acheminement d'événement, vous pouvez effectuer les actions suivantes sur un système d'acheminement d'événement sélectionné.

- Actualiser la liste des systèmes d'acheminement d'événement en cliquant sur l'icône **Actualiser** ( ).
- Afficher les détails relatifs à un système d'acheminement d'événement spécifique en cliquant sur le lien dans la colonne **Nom**.
- Modifier les propriétés et les critères de filtrage d'un système d'acheminement d'événement en cliquant sur le nom de celui-ci dans la colonne **Nom**.
- Supprimer le système d'acheminement d'événement en cliquant sur l'icône **Supprimer** ( ).
- Suspendre l'acheminement d'événement (voir Interruption de l'acheminement d'événement).

Configuration de l'acheminement d'événement vers un service SMTP Gmail

Vous pouvez configurer Lenovo XClarity Administrator pour acheminer des événements surveillés vers un service de messagerie Web, par exemple, Gmail.

Servez-vous des exemples de configuration suivants pour vous aider à configurer votre système d'acheminement d'événement avec le service SMTP Gmail.

Remarque : Gmail recommande d'utiliser la méthode d'authentification OAUTH2 pour obtenir la communication la plus sécurisée qui soit. Si vous choisissez d'utiliser une authentification normale, vous recevez un e-mail indiquant qu'une application a tenté d'utiliser votre compte sans utiliser les dernières normes de sécurité. Cet e-mail contient des instructions vous permettant de configurer votre compte de messagerie afin d'accepter ces types d'application.

Pour plus d'informations sur la configuration d'un serveur SMTP Gmail, voir https://support.google.com/a/answer/176600?hl=en.

Authentification normale à l'aide de SSL sur le port 465

Cet exemple communique avec le serveur SMTP Gmail à l'aide du protocole SSL sur le port 465 et procède à l'authentification à l'aide d'un compte utilisateur et d'un mot de passe Gmail valides.

Paramètre	Valeur
Hôte	smtp.gmail.com
Port	465
SSL	Sélectionner
STARTTLS	Effacer
Authentification	Normale
Utilisateur	Adresse e-mail Gmail valide
Mot de passe	Mot de passe d'authentification SMTP Gmail
Depuis l'adresse	(facultatif).

Authentification normale à l'aide de TLS sur le port 587

Cet exemple communique avec le serveur SMTP Gmail à l'aide du protocole TLS sur le port 587 et procède à l'authentification à l'aide d'un compte utilisateur et d'un mot de passe Gmail valides.

Paramètre	Valeur
Hôte	smtp.gmail.com
Port	587
SSL	Effacer
STARTTLS	Sélectionner
Authentification	Normale
Utilisateur	Adresse e-mail Gmail valide
Mot de passe	Mot de passe d'authentification SMTP Gmail
Depuis l'adresse	(facultatif).

Authentification OAUTH2 à l'aide de TLS sur le port 587

Cet exemple communique avec le serveur SMTP Gmail à l'aide du protocole TLS sur le port 587 et procède à l'authentification à l'aide d'un compte utilisateur et d'un jeton de sécurité Gmail valides.

Utilisez l'exemple de procédure suivant pour obtenir le jeton de sécurité :

1. Créez un projet dans la console des développeurs Google et récupérez l'ID client et le secret client. Pour plus d'informations, voir le site Web Page Web Connexion Google pour les sites Web.
   a. À partir d'un navigateur Web, ouvrez la Page Web API Google.
   b. Cliquez sur **Select a project → Create a project** dans le menu qui apparaît sur cette page Web. La boîte de dialogue New Project s'affiche.
   c. Tapez un nom, sélectionnez **Yes** pour accepter les dispositions du contrat de licence, puis cliquez sur **Create**.
   d. Sur l'onglet **Overview**, tapez « gmail » dans la zone de recherche.
   e. Cliquez sur **GMAIL API** dans les résultats de la recherche.
   f. Cliquez sur **Enable**.
   g. Cliquez sur l'onglet **Credentials**.
   h. Cliquez sur **Écran d'accord OAuth**.
   i. Tapez un nom dans la zone **Nom de produit affiché pour les utilisateurs**, puis cliquez sur **Save**.

j. Cliquez sur **Create credentials → OAuth client ID**.

k. Sélectionnez **Other** et entrez un nom.

l. Cliquez sur **Créer**. La boîte de dialogue OAuth client s'affiche avec votre ID client et votre secret client.

m. Enregistrez l'ID client et le secret client afin de les utiliser ultérieurement.

n. Cliquez sur **OK** pour fermer la boîte de dialogue.

2. Utilisez le script Python oauth2.py pour générer et autoriser un jeton de sécurité en entrant l'ID client et le secret client générés lors de la création du projet.

   Remarque : Python 2.7 est requis pour exécuter cette étape. Vous pouvez télécharger et installer Python 2.7 à partir du Site Web Python.

   a. À partir d'un navigateur Web, ouvrez la Page Web gmail-oauth2-tools.

   b. Cliquez sur **Raw**, puis enregistrez le contenu sous le nom de fichier `oauth2.py` sur votre système local.

   c. Exécutez la commande suivante dans une fenêtre de terminal (Linux) ou sur une ligne de commande (Windows) :

   ```
   py oauth2.py --user=<your_email> --client_id=<client_id>
      --client_secret=<client_secret> --generate_oauth2_token
   ```

   Par exemple

   ```
   py oauth2.py --user=jon@gmail.com
      --client_id=884243132302-458elfqjiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com
      --client_secret=3tnyXgEiBIbT2m0OzqnlTszk --generate_oauth2_token
   ```

   Cette commande renvoie une URL que vous devez utiliser pour autoriser le jeton et extraire un code de vérification à partir du site Web Google, par exemple :

   ```
   To authorize token, visit this url and follow the directions:

   https://accounts.google.com/o/oauth2/auth?client_id=884243132302
   -458elfqjiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com&amp;redirect_uri=
   urn%3Aietf%3Awg%3Aoauth%3A2.0%3Aoob&amp;response_type=code&amp;scope=https%3A%2F%2Fmail.
   google.com%2F

   Enter verification code:
   ```

   d. À partir d'un navigateur Web, ouvrez l'URL qui a été renvoyée au cours de l'étape précédente.

   e. Cliquez sur **Allow** pour accepter les conditions d'utilisation de ce service. Un code de vérification est renvoyé.

   f. Entrez le code de vérification dans la commande `oauth2.py`.

   La commande renvoie le jeton de sécurité et actualise le jeton, par exemple :

   ```
   Refresh Token: 1/K8lPGx6UQQajj7tQGYKq8mVG8lVvGIVzHqzxFIMeYEQMEudVrK5jSpoR3OzcRFq6
   Access Token: ya29.CjHXAsyoH9GuCZutgIOxm1SGSqKrUkjIoH14SGMnljZ6rwp3gZmK7SrGDPCQx_KN-34f
   Access Token Expiration Seconds: 3600
   ```

   Important : Le jeton de sécurité expire au terme d'une période définie. Vous pouvez utiliser le script Python oauth2.py et le jeton actualisé pour générer un nouveau jeton de sécurité. Il est de votre responsabilité de générer le nouveau jeton de sécurité et de mettre à jour le système d'acheminement d'événement dans Lenovo XClarity Administrator avec le nouveau jeton.

3. Dans l'interface Web Lenovo XClarity Administrator, configurez le système d'acheminement d'événement pour un service de messagerie à l'aide des attributs suivants :

Paramètre	Valeur
Hôte	smtp.gmail.com
Port	587
SSL	Effacer
STARTTLS	Sélectionner
Authentification	OAUTH2
Utilisateur	Adresse e-mail Gmail valide
Jeton	Jeton de sécurité
Depuis l'adresse	(facultatif).

Configuration de l'acheminement d'événement vers un serveur FTP

Vous pouvez configurer Lenovo XClarity Administrator pour l'acheminement d'événements spécifiques vers un serveur FTP.

À propos de cette tâche

Vous pouvez créer et activer jusqu'à 20 système d'acheminement d'événement pour l'envoi d'événements à des destinataires spécifiques.

Si XClarity Administrator est réamorcé après la configuration des systèmes d'acheminement d'événement, vous devez attendre que le serveur de gestion regénère des données internes pour que les événements soient correctement acheminés.

Remarque : À compter de XClarity Administrator version 1.2.0, la zone **Commutateurs** est incluse sur l'onglet **Événements** dans les boîtes de dialogue Nouveau système d'acheminement d'événement et Modifier les systèmes d'acheminement d'événement. Si vous avez effectué une mise à niveau vers la version 1.2.0 ou une version ultérieure à partir d'une édition antérieure, pensez à mettre à jour vos systèmes d'acheminement d'événement de manière à inclure ou exclure les événements RackSwitch, le cas échéant. Cette action est nécessaire même si vous avez coché la case **Tous les systèmes** pour sélectionner tous les appareils.

Procédure

Procédez comme suit pour créer un système d'acheminement d'événement pour un serveur FTP.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez **Surveillance → Acheminement d'événement**. La page Acheminement d'événement s'affiche.

Etape 2. Cliquez sur l'onglet **Réexpéditeur d'événement**.

Etape 3. Cliquez sur l'icône **Créer** ( ). L'onglet **Général** de la boîte de dialogue Nouveau système d'acheminement d'événement s'affiche.

Etape 4. Sélectionnez **FTP** comme type de système d'acheminement d'événement, puis indiquez les informations spécifiques au protocole :

- Entrez le nom, l'hôte de destination et la description facultative des systèmes d'acheminement d'événement.
- Entrez le port à utiliser pour l'acheminement des événements. La valeur par défaut est 21.
- Entrez le délai d'attente (en secondes) pour la demande. La valeur par défaut est 30 secondes.
- **Facultatif :** Spécifiez la séquence de caractères à supprimer du contenu du fichier.

- Entrez le format de nom de fichier à utiliser pour le fichier qui contient l'événement acheminé. Le format par défaut est `event_[[EventSequenceID]].txt`.

  Remarque : Chaque fichier contient des informations sur un seul événement.
- Entrez le chemin d'accès au serveur FTP distant où le fichier doit être chargé.
- Cliquez sur le codage de caractères, **UTF8** ou **Big5**. Il s'agit de UTF-8 par défaut.
- Sélectionnez le type d'authentification. Les valeurs possibles sont les suivantes.
  - **Anonyme**. (par défaut) Aucune authentification n'est utilisée
  - **Base**. Effectue l'authentification auprès du serveur FTP à l'aide de l'ID utilisateur et du mot de passe spécifiés.

Etape 5. Cliquez sur **Format de sortie** pour choisir le format de sortie des données d'événements à acheminer. Les informations varient pour chaque type de système d'acheminement d'événement.

L'exemple de format de sortie suivante est le format par défaut pour les destinataires FTP. Tous les mots entre crochets doubles sont les variables qui sont remplacées par des valeurs réelles lors de l'acheminement d'un événement. Les variables disponibles pour les destinataires FTP sont répertoriées dans la boîte de dialogue Format de sortie.

```
Alert: [[EventDate]] [[EventMessage]]\n
\n
Hardware Information:\n
Managed Endpoint    : [[DeviceHardwareType]] at [[DeviceIPAddress]]\n
Device name          : [[DeviceName]]\n
Product name         : [[DeviceProductName]]\n
Host name            : [[DeviceHostName]]\n
Machine Type         : [[DeviceMachineType]]\n
Machine Model        : [[DeviceMachineModel]]\n
Serial Number        : [[DeviceSerialNumber]]\n
DeviceHealthStatus   : [[DeviceHealthStatus]]\n
IPv4 addresses       : [[DeviceIPV4Addresses]]\n
IPv6 addresses       : [[DeviceIPV6Addresses]]\n
Chassis              : [[DeviceChassisName]]\n
DeviceBays           : [[DeviceBays]]\n
\n
LXCA is: [[ManagementServerIP]]\n
\n
Event Information:\n
  Event ID         : [[EventID]]\n
  Common Event ID : [[CommonEventID]]\n
  EventSeverity    : [[EventSeverity]]\n
  Event Class      : [[EventClass]]\n
  Sequence ID      : [[EventSequenceID]]\n
  Event Source ID : [[EventSourceUUID]]\n
  Component ID     : [[EventComponentUUID]]\n
  Serial Num       : [[EventSerialNumber]]\n
  MTM              : [[EventMachineTypeModel]]\n
  EventService     : [[EventService]]\n
  Console link     : [[ConsoleLink]]\n
  iOS link         : [[iOSLink]]\n
  Android link     : [[AndroidLink]]\n
  System Name      : [[DeviceFullPathName]]\n"
```

Vous pouvez cliquer sur **Réinitialiser aux valeurs par défaut** pour rétablir le format de sortie dans les zones par défaut.

Etape 6. Cliquez sur le bouton **Autoriser les événements exclus** pour autoriser ou empêcher le transfert des événements exclus.

Etape 7. Sélectionnez **Activer ce réexpéditeur** pour activer l'acheminement d'événement pour ce système d'acheminement d'événement.

Etape 8. Cliquez sur **Suivant** pour afficher l'onglet **Appareils**.

Etape 9. Sélectionnez les appareils et les groupes que vous souhaitez surveiller pour ce système d'acheminement d'événement.

Astuce : Pour acheminer des événements pour tous les appareils gérés (actuels et ultérieurs), cochez la case **Faire correspondre tous les systèmes**.Si vous ne cochez pas la case **Faire correspondre tous les systèmes**, assurez-vous que la colonne UUID des appareils sélectionnés ne contient pas d'UUID factice. Un UUID factice est affecté aux appareils qui n'ont pas encore été récupérés après un redémarrage ou qui ne sont pas complètement reconnus par le serveur de gestion. Si vous sélectionnez un appareil doté d'un UUID factice, l'acheminement d'événement fonctionne pour cet appareil jusqu'à ce que celui-ci soit complètement reconnu ou récupéré et que l'UUID factice soit remplacé par un UUID réel.

Etape 10. Cliquez sur **Suivant** pour afficher la page **Evénements**.

Etape 11. Sélectionnez les filtres à utiliser pour ce système d'acheminement d'événement.

- **Correspondance par catégorie d'événement**.
  1. Pour acheminer tous les événements d'audit, quel que soit le niveau de l'état, sélectionnez **Inclure tous les événements d'audit**.
  2. Pour acheminer tous les événements de garantie, sélectionnez **Inclure les événements de garantie**.
  3. Pour acheminer tous les événements de modification de l'état de santé, sélectionnez **Inclure les événements de changement d'état**.
  4. Pour acheminer tous les événements de mise à jour de l'état de santé, sélectionnez **Inclure les événements de mise à jour d'état**.
  5. Sélectionnez les classes d'événement et le niveau de facilité de maintenance à acheminer.
  6. Entrez les ID d'un ou de plusieurs événements à exclure de l'acheminement. Séparez-les à l'aide d'une virgule (par exemple, `FQXHMEM0214I,FQXHMEM0214I`).
- **Correspondance par code d'événement**. Entrez les ID d'un ou de plusieurs événements à acheminer. Si vous entrez plusieurs ID, séparez-les à l'aide d'une virgule.
- **Exclusion par catégorie d'événement**.
  1. Pour exclure tous les événements d'audit, quel que soit le niveau de l'état, sélectionnez **Exclure tous les événements d'audit**.
  2. Pour exclure tous les événements de garantie, sélectionnez **Exclure les événements de garantie**.
  3. Pour exclure tous les événements de modification de l'état de santé, sélectionnez **Exclure les événements de changement d'état**.
  4. Pour exclure tous les événements de mise à jour de l'état de santé, sélectionnez **Exclure les événements de mise à jour d'état**.
  5. Sélectionnez les classes d'événement et le niveau de facilité de maintenance à exclure.
  6. Entrez les ID d'un ou de plusieurs événements à acheminer. Séparez-les à l'aide d'une virgule.
- **Exclusion par code d'événement**. Entrez les ID d'un ou de plusieurs événements à exclure. Si vous entrez plusieurs ID, séparez-les à l'aide d'une virgule.

Etape 12. Choisissez d'inclure ou non certains types d'événements.

- **Inclure tous les événements d'audit**. Envoie des notifications à propos des événements d'audit, sur la base des catégories et des gravités sélectionnées pour les événements.

- **Inclure les événements de garantie**. Envoie des notifications à propos des garanties.
- **Inclure les événements de modification d'état**. Envoie des notifications à propos des modifications d'état.
- **Inclure les événements de mise à jour d'état**. Notifications envoyées au sujet de nouvelles alertes.
- **Inclure les événements du bulletin**. Envoie des notifications à propos des nouveaux bulletins.

Etape 13. Sélectionnez les types d'événements et les gravités pour lesquels vous souhaitez recevoir une notification.

Etape 14. Sélectionnez si oui ou non vous souhaitez filtrer les événements en fonction de la facilité de maintenance.

Etape 15. Cliquez sur **Suivant** pour afficher la page **Planificateur**.

Etape 16. **Facultatif :** Définissez les heures et les jours auxquels vous souhaitez que les événements spécifiés soient acheminés vers ce système d'acheminement d'événement. Seuls les événements qui se produisent pendant le créneau horaire indiqué sont acheminés.

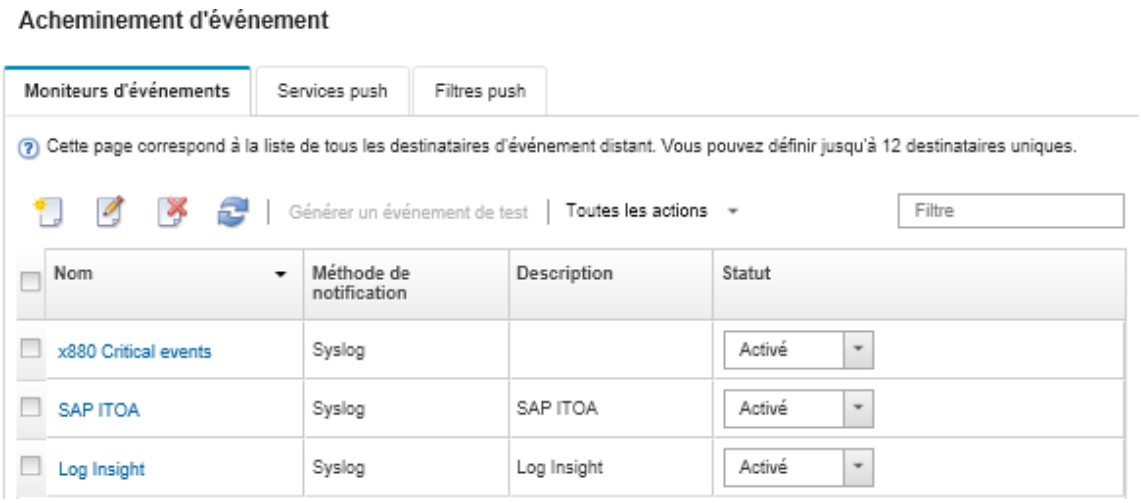
Si vous ne créez pas de planning pour le système d'acheminement d'événement, les événements sont acheminés 24h/24 et 7j/7.

1. Utilisez l'icône **Défiler vers la gauche** (◀) et l'icône **Défiler vers la droite** (▶), ainsi que les boutons **Jour**, **Semaine** et **Mois** pour définir le jour et l'heure de début du planning.
2. Cliquez deux fois sur le créneau horaire pour ouvrir la boîte de dialogue Nouvelle période.
3. Indiquez les informations requises, y compris la date et les heures de début et de fin et précisez si le planning est répétitif.
4. Cliquez sur **Créer** pour enregistrer le planning et fermer la boîte de dialogue. Le nouveau planning est ajouté au calendrier.

Astuce :
- Vous pouvez modifier le créneau horaire en faisant glisser l'entrée du planning vers un autre créneau horaire du calendrier.
- Vous pouvez modifier la durée en sélectionnant le haut ou le bas de l'entrée de planning et en le faisant glisser vers la nouvelle heure dans le calendrier.
- Vous pouvez modifier l'heure de fin en sélectionnant le bas de l'entrée de planning et en le faisant glisser vers la nouvelle heure dans le calendrier.
- Vous pouvez modifier un planning en cliquant deux fois sur l'entrée de planning et en cliquant sur **Éditer l'entrée**.
- Vous pouvez afficher un résumé de toutes les entrées de planning en sélectionnant **Afficher le récapitulatif du planificateur**. Le récapitulatif comprend le créneau horaire pour chaque entrée et indique les entrées qui sont répétables.
- Vous pouvez supprimer une entrée de planning du calendrier ou planifier un récapitulatif en sélectionnant l'entrée, puis en cliquant sur **Supprimer une entrée**.

Etape 17. Cliquez sur **Créer**.

Le système d'acheminement d'événement figure dans le tableau Acheminement d'événement.



Etape 18. Sélectionnez le nouveau système d'acheminement d'événement, cliquez sur **Générer un événement de test**, puis assurez-vous que les événements sont acheminés correctement vers le serveur FTP approprié.

Après avoir terminé

Sur la page Acheminement d'événement, vous pouvez effectuer les actions suivantes sur un système d'acheminement d'événement sélectionné.

- Actualiser la liste des systèmes d'acheminement d'événement en cliquant sur l'icône **Actualiser** ( ).
- Afficher les détails relatifs à un système d'acheminement d'événement spécifique en cliquant sur le lien dans la colonne **Nom**.
- Modifier les propriétés et les critères de filtrage d'un système d'acheminement d'événement en cliquant sur le nom de celui-ci dans la colonne **Nom**.
- Supprimer le système d'acheminement d'événement en cliquant sur l'icône **Supprimer** ( ).
- Suspendre l'acheminement d'événement (voir Interruption de l'acheminement d'événement).

Configuration de l'acheminement d'événement vers un service Web REST

Vous pouvez configurer Lenovo XClarity Administrator pour l'acheminement d'événements spécifiques vers un service Web REST.

À propos de cette tâche

Vous pouvez créer et activer jusqu'à 20 système d'acheminement d'événement pour l'envoi d'événements à des destinataires spécifiques.

Si XClarity Administrator est réamorcé après la configuration des systèmes d'acheminement d'événement, vous devez attendre que le serveur de gestion regénère des données internes pour que les événements soient correctement acheminés.

Remarque : À compter de XClarity Administrator version 1.2.0, la zone **Commutateurs** est incluse sur l'onglet **Événements** dans les boîtes de dialogue Nouveau système d'acheminement d'événement et Modifier les systèmes d'acheminement d'événement. Si vous avez effectué une mise à niveau vers la version 1.2.0 ou une version ultérieure à partir d'une édition antérieure, pensez à mettre à jour vos systèmes d'acheminement d'événement de manière à inclure ou exclure les événements RackSwitch, le cas échéant. Cette action est nécessaire même si vous avez coché la case **Tous les systèmes** pour sélectionner tous les appareils.

Procédure

Procédez comme suit pour créer un système d'acheminement d'événement pour un service Web REST.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez **Surveillance → Acheminement d'événement**. La page Acheminement d'événement s'affiche.

Etape 2. Cliquez sur l'onglet **Réexpéditeur d'événement**.

Etape 3. Cliquez sur l'icône **Créer** ( ). L'onglet **Général** de la boîte de dialogue Nouveau système d'acheminement d'événement s'affiche.

Etape 4. Sélectionnez **REST** comme type de système d'acheminement d'événement, puis indiquez les informations spécifiques au protocole :

- Entrez le chemin d'accès aux ressources sur lequel le réexpéditeur doit publier les événements (par exemple, /rest/test).
- Sélectionnez le protocole à utiliser pour l'acheminement des événements. Les valeurs possibles sont les suivantes.
  - **HTTP**
  - **HTTPS**
- Sélectionnez la méthode REST. Les valeurs possibles sont les suivantes.
  - **PUT**
  - **POST**
- Entrez le délai d'attente (en secondes) pour la demande. La valeur par défaut est 30 secondes.
- **Facultatif :** Si l'authentification est requise, sélectionnez l'un des types d'authentification suivants :
  - **Base**. Effectue l'authentification auprès du serveur spécifié à l'aide de l'ID utilisateur et du mot de passe spécifiés.
  - **Aucun**. Aucune authentification n'est utilisée.

Etape 5. Cliquez sur **Format de sortie** pour choisir le format de sortie des données d'événements à acheminer. Les informations varient pour chaque type de système d'acheminement d'événement.

L'exemple de format de sortie suivante est le format par défaut pour les destinataires du service Web REST. Tous les mots entre crochets doubles sont les variables qui sont remplacées par des valeurs réelles lors de l'acheminement d'un événement. Les variables disponibles pour les destinataires du service Web REST sont répertoriées dans la boîte de dialogue Format de sortie.

```
{\"msg\":\"[[EventMessage]]\",\"eventID\":\"[[EventID]]\",\"serialnum\":
\"[[EventSerialNumber]]\",\"senderUUID\":\"[[EventSenderUUID]]\",\"flags\":
\"[[EventFlags]]\",\"userid\":\"[[EventUserName]]\",\"localLogID\":
\"[[EventLocalLogID]]\",\"systemName\":\"[[DeviceFullPathName]]\",\"action\":
[[EventActionNumber]],\"failFRUNumbers\":\"[[EventFailFRUs]]\",\"severity\":
[[EventSeverityNumber]],\"sourceID\":\"[[EventSourceUUID]]\",
\"sourceLogSequence\":[[EventSourceLogSequenceNumber]],\"failFRUSNs\":
\"[[EventFailSerialNumbers]]\",\"failFRUUUIDs\":\"[[EventFailFRUUUIDs]]\",
\"eventClass\":[[EventClassNumber]],\"componentID\":\"[[EventComponentUUID]]\",
\"mtm\":\"[[EventMachineTypeModel]]\",\"msgID\":\"[[EventMessageID]]\",
"sequenceNumber\":\"[[EventSequenceID]]\",\"timeStamp\":\"[[EventTimeStamp]]\",
\"args\":[[EventMessageArguments]],\"service\":[[EventServiceNumber]],
\"commonEventID\":\"[[CommonEventID]]\",\"eventDate\":\"[[EventDate]]\"}"
```

Vous pouvez cliquer sur **Réinitialiser aux valeurs par défaut** pour rétablir le format de sortie dans les zones par défaut.

Etape 6. Cliquez sur le bouton **Autoriser les événements exclus** pour autoriser ou empêcher le transfert des événements exclus.

Etape 7. Sélectionnez **Activer ce réexpéditeur** pour activer l'acheminement d'événement pour ce système d'acheminement d'événement.

Etape 8. Cliquez sur **Suivant** pour afficher l'onglet **Appareils**.

Etape 9. Sélectionnez les appareils et les groupes que vous souhaitez surveiller pour ce système d'acheminement d'événement.

Astuce : Pour acheminer des événements pour tous les appareils gérés (actuels et ultérieurs), cochez la case **Faire correspondre tous les systèmes**.Si vous ne cochez pas la case **Faire correspondre tous les systèmes**, assurez-vous que la colonne UUID des appareils sélectionnés ne contient pas d'UUID factice. Un UUID factice est affecté aux appareils qui n'ont pas encore été récupérés après un redémarrage ou qui ne sont pas complètement reconnus par le serveur de gestion. Si vous sélectionnez un appareil doté d'un UUID factice, l'acheminement d'événement fonctionne pour cet appareil jusqu'à ce que celui-ci soit complètement reconnu ou récupéré et que l'UUID factice soit remplacé par un UUID réel.

Etape 10. Cliquez sur **Suivant** pour afficher la page **Evénements**.

Etape 11. Sélectionnez les filtres à utiliser pour ce système d'acheminement d'événement.

- **Correspondance par catégorie d'événement**.
  1. Pour acheminer tous les événements d'audit, quel que soit le niveau de l'état, sélectionnez **Inclure tous les événements d'audit**.
  2. Pour acheminer tous les événements de garantie, sélectionnez **Inclure les événements de garantie**.
  3. Pour acheminer tous les événements de modification de l'état de santé, sélectionnez **Inclure les événements de changement d'état**.
  4. Pour acheminer tous les événements de mise à jour de l'état de santé, sélectionnez **Inclure les événements de mise à jour d'état**.
  5. Sélectionnez les classes d'événement et le niveau de facilité de maintenance à acheminer.
  6. Entrez les ID d'un ou de plusieurs événements à exclure de l'acheminement. Séparez-les à l'aide d'une virgule (par exemple, `FQXHMEM0214I`,`FQXHMEM0214I`).
- **Correspondance par code d'événement**. Entrez les ID d'un ou de plusieurs événements à acheminer. Si vous entrez plusieurs ID, séparez-les à l'aide d'une virgule.
- **Exclusion par catégorie d'événement**.
  1. Pour exclure tous les événements d'audit, quel que soit le niveau de l'état, sélectionnez **Exclure tous les événements d'audit**.
  2. Pour exclure tous les événements de garantie, sélectionnez **Exclure les événements de garantie**.
  3. Pour exclure tous les événements de modification de l'état de santé, sélectionnez **Exclure les événements de changement d'état**.
  4. Pour exclure tous les événements de mise à jour de l'état de santé, sélectionnez **Exclure les événements de mise à jour d'état**.
  5. Sélectionnez les classes d'événement et le niveau de facilité de maintenance à exclure.
  6. Entrez les ID d'un ou de plusieurs événements à acheminer. Séparez-les à l'aide d'une virgule.
- **Exclusion par code d'événement**. Entrez les ID d'un ou de plusieurs événements à exclure. Si vous entrez plusieurs ID, séparez-les à l'aide d'une virgule.

Etape 12. Choisissez d'inclure ou non certains types d'événements.

- **Inclure tous les événements d'audit**. Envoie des notifications à propos des événements d'audit, sur la base des catégories et des gravités sélectionnées pour les événements.

- **Inclure les événements de garantie**. Envoie des notifications à propos des garanties.
- **Inclure les événements de modification d'état**. Envoie des notifications à propos des modifications d'état.
- **Inclure les événements de mise à jour d'état**. Notifications envoyées au sujet de nouvelles alertes.
- **Inclure les événements du bulletin**. Envoie des notifications à propos des nouveaux bulletins.

Etape 13. Sélectionnez les types d'événements et les gravités pour lesquels vous souhaitez recevoir une notification.

Etape 14. Sélectionnez si oui ou non vous souhaitez filtrer les événements en fonction de la facilité de maintenance.

Etape 15. Cliquez sur **Suivant** pour afficher la page **Planificateur**.

Etape 16. **Facultatif :** Définissez les heures et les jours auxquels vous souhaitez que les événements spécifiés soient acheminés vers ce système d'acheminement d'événement. Seuls les événements qui se produisent pendant le créneau horaire indiqué sont acheminés.

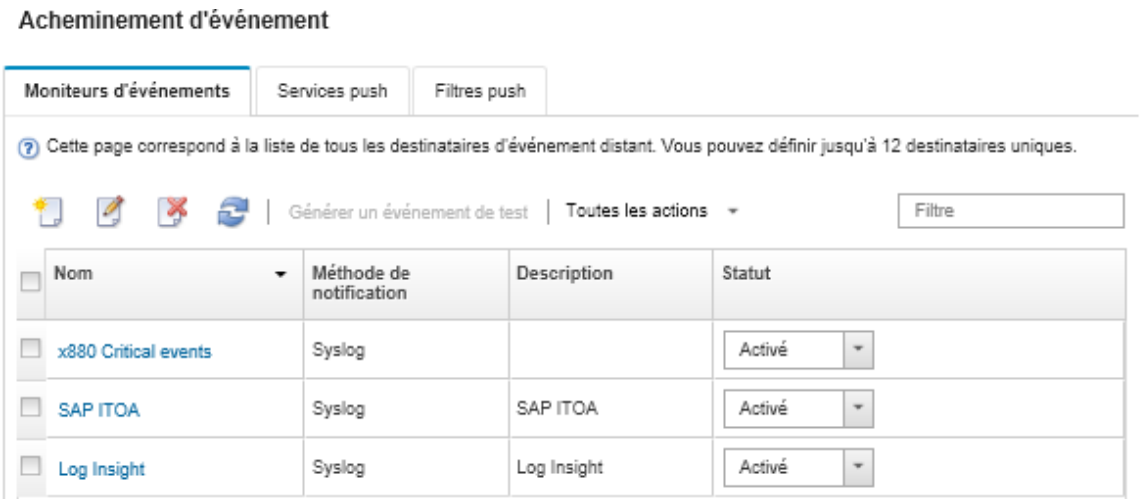
Si vous ne créez pas de planning pour le système d'acheminement d'événement, les événements sont acheminés 24h/24 et 7j/7.

1. Utilisez l'icône **Défiler vers la gauche** (◀) et l'icône **Défiler vers la droite** (▶), ainsi que les boutons **Jour**, **Semaine** et **Mois** pour définir le jour et l'heure de début du planning.
2. Cliquez deux fois sur le créneau horaire pour ouvrir la boîte de dialogue Nouvelle période.
3. Indiquez les informations requises, y compris la date et les heures de début et de fin et précisez si le planning est répétitif.
4. Cliquez sur **Créer** pour enregistrer le planning et fermer la boîte de dialogue. Le nouveau planning est ajouté au calendrier.

Astuce :
- Vous pouvez modifier le créneau horaire en faisant glisser l'entrée du planning vers un autre créneau horaire du calendrier.
- Vous pouvez modifier la durée en sélectionnant le haut ou le bas de l'entrée de planning et en le faisant glisser vers la nouvelle heure dans le calendrier.
- Vous pouvez modifier l'heure de fin en sélectionnant le bas de l'entrée de planning et en le faisant glisser vers la nouvelle heure dans le calendrier.
- Vous pouvez modifier un planning en cliquant deux fois sur l'entrée de planning et en cliquant sur **Éditer l'entrée**.
- Vous pouvez afficher un résumé de toutes les entrées de planning en sélectionnant **Afficher le récapitulatif du planificateur**. Le récapitulatif comprend le créneau horaire pour chaque entrée et indique les entrées qui sont répétables.
- Vous pouvez supprimer une entrée de planning du calendrier ou planifier un récapitulatif en sélectionnant l'entrée, puis en cliquant sur **Supprimer une entrée**.

Etape 17. Cliquez sur **Créer**.

Le système d'acheminement d'événement figure dans le tableau Acheminement d'événement.



Etape 18. Sélectionnez le nouveau système d'acheminement d'événement, cliquez sur **Générer un événement de test**, puis assurez-vous que les événements sont acheminés correctement vers le service Web REST approprié.

Après avoir terminé

Sur la page Acheminement d'événement, vous pouvez effectuer les actions suivantes sur un système d'acheminement d'événement sélectionné.

- Actualiser la liste des systèmes d'acheminement d'événement en cliquant sur l'icône **Actualiser** ( ).
- Afficher les détails relatifs à un système d'acheminement d'événement spécifique en cliquant sur le lien dans la colonne **Nom**.
- Modifier les propriétés et les critères de filtrage d'un système d'acheminement d'événement en cliquant sur le nom de celui-ci dans la colonne **Nom**.
- Supprimer le système d'acheminement d'événement en cliquant sur l'icône **Supprimer** ( ).
- Suspendre l'acheminement d'événement (voir Interruption de l'acheminement d'événement).

Configuration de l'acheminement d'événement vers un gestionnaire SNMPv1 ou SNMPv3 distant

Vous pouvez configurer Lenovo XClarity Administrator pour acheminer des événements spécifiques vers un gestionnaire SNMPv1 ou SNMPv3 distant.

À propos de cette tâche

Vous pouvez créer et activer jusqu'à 20 système d'acheminement d'événement pour l'envoi d'événements à des destinataires spécifiques.

Si XClarity Administrator est réamorcé après la configuration des systèmes d'acheminement d'événement, vous devez attendre que le serveur de gestion regénère des données internes pour que les événements soient correctement acheminés.

Remarque : À compter de XClarity Administrator version 1.2.0, la zone **Commutateurs** est incluse sur l'onglet **Événements** dans les boîtes de dialogue Nouveau système d'acheminement d'événement et Modifier les systèmes d'acheminement d'événement. Si vous avez effectué une mise à niveau vers la version 1.2.0 ou une version ultérieure à partir d'une édition antérieure, pensez à mettre à jour vos systèmes d'acheminement d'événement de manière à inclure ou exclure les événements RackSwitch, le cas échéant. Cette action est nécessaire même si vous avez coché la case **Tous les systèmes** pour sélectionner tous les appareils.

Pour plus d'informations sur le MIB XClarity Administrator, voir Fichier lenovoMgrAlert.mib.

Procédure

Pour créer un réexpéditeur d'événement pour un gestionnaireSNMPv1 ou SNMPv3 distant, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez **Surveillance → Acheminement d'événement**. La page Acheminement d'événement s'affiche.

Etape 2. Cliquez sur l'onglet **Réexpéditeur d'événement**.

Etape 3. Cliquez sur l'icône **Créer** ( ). L'onglet **Général** de la boîte de dialogue Nouveau système d'acheminement d'événement s'affiche.

Etape 4. Sélectionnez **SNMPv1** ou **SNMPv3** comme type de système d'acheminement d'événement, puis indiquez les informations spécifiques au protocole :

- Entrez le nom et l'hôte de destination du système d'acheminement d'événement.
- Entrez le port à utiliser pour l'acheminement des événements. La valeur par défaut est `162`.
- **Facultatif :** Entrez des informations supplémentaires, y compris la description, le nom de contact et l'emplacement.
- Sélectionnez la version SNMP. Les valeurs possibles sont les suivantes.
  - **SNMPv1**. Si cette version est sélectionnée, indiquez le mot de passe de communauté qui est envoyé avec chaque demande SNMP émise vers l'appareil.
  - **SNMPv3**. Il s'agit de la valeur par défaut, recommandée pour une sécurité renforcée. Si la version SNMPv3 est sélectionnée, indiquez éventuellement l'ID utilisateur, le type et le mot de passe d'authentification, ainsi que le type et le mot de passe de confidentialité.

    Si le destinataire de l'alerte SNMPv3 requiert l'ID de moteur pour l'instance XClarity Administrator, vous pouvez rechercher l'ID de moteur de la manière suivante :

    1. Assurez-vous que les paramètres de connexion (username, authProtocol, authPassword, privProtocol, privPassword) correspondent à ceux qui sont définis dans XClarity Administrator.
    2. À l'aide de votre logiciel préféré (par exemple, snmpwalk), exécutez une demande GET SNMP sur le serveur XClarity Administrator en utilisant l'un des ID objet suivants :
       - EngineID : 1.3.6.1.6.3.10.2.1.1.0
       - EngineBoots : 1.3.6.1.6.3.10.2.1.2.0

       Utilisez la syntaxe suivante pour la commande `snmpget`. Veuillez noter que le type d'authentification réexpéditeur -a peut être SHA ou vide (aucune authentification).
       ```
       snmpget -v 3 -u <FORWARDER_USER_ID> -l authPriv -a <FORWARDER_AUTH_TYPE> -A <FORWARDER_A
       ```

       Par exemple, si l'adresse IP de XClarity Administrator est 192.0.1.0, le type d'authentification est SHA et le type de confidentialité est AES, la commande ci-après présente engineID.
       ```
       snmpget -v 3 -u someUserID -l authPriv -a SHA -A someUserIDPassword_1 -x AES -X somePrivacyPassword_1
       ```

       L'exemple de réponse suivant est renvoyé. Dans cet exemple, l'engineID est 0x80001370017F00000134C27E12.
       ```
       iso.3.6.1.6.3.10.2.1.1.0 = Hex-STRING: 80 00 13 70 01 7F 00 00 01 34 C2 7E 12
       ```
- Entrez le délai d'attente (en secondes) pour la demande. La valeur par défaut est 30 secondes.
- **Facultatif** : Si l'authentification d'alerte est nécessaire, entrez l'ID utilisateur et le mot de passe d'authentification. Les mêmes ID utilisateur et mot de passe doivent être saisis dans le gestionnaire SNMP à distance, vers lequel les alertes sont réacheminées.

- Sélectionnez le protocole d'authentification qui est utilisé par le gestionnaire SNMP distant afin de vérifier l'émetteur de l'alerte. Les valeurs possibles sont les suivantes
  - **SHA**. Utilise le protocole SHA pour l'authentification auprès du serveur SNMP spécifié à l'aide de l'ID utilisateur, du mot de passe et du nom de domaine spécifiés.
  - **Aucun**. Aucune authentification n'est utilisée
- Si le chiffrement de l'alerte est nécessaire, entrez le type de confidentialité (protocole de chiffrement) et le mot de passe. Les valeurs possibles sont les suivantes. Les mêmes protocole et mot de passe doivent être saisis dans le gestionnaire SNMP distant, vers lequel les alertes sont réacheminées.
  - **AES**
  - **DES**
  - **Aucun**

Etape 5. Cliquez sur le bouton **Autoriser les événements exclus** pour autoriser ou empêcher le transfert des événements exclus.

Etape 6. Sélectionnez **Activer ce réexpéditeur** pour activer l'acheminement d'événement pour ce système d'acheminement d'événement.

Etape 7. Cliquez sur **Suivant** pour afficher l'onglet **Appareils**.

Etape 8. Sélectionnez les appareils et les groupes que vous souhaitez surveiller pour ce système d'acheminement d'événement.

Astuce : Pour acheminer des événements pour tous les appareils gérés (actuels et ultérieurs), cochez la case **Faire correspondre tous les systèmes**.Si vous ne cochez pas la case **Faire correspondre tous les systèmes**, assurez-vous que la colonne UUID des appareils sélectionnés ne contient pas d'UUID factice. Un UUID factice est affecté aux appareils qui n'ont pas encore été récupérés après un redémarrage ou qui ne sont pas complètement reconnus par le serveur de gestion. Si vous sélectionnez un appareil doté d'un UUID factice, l'acheminement d'événement fonctionne pour cet appareil jusqu'à ce que celui-ci soit complètement reconnu ou récupéré et que l'UUID factice soit remplacé par un UUID réel.

Etape 9. Cliquez sur **Suivant** pour afficher la page **Evénements**.

Etape 10. Sélectionnez les filtres à utiliser pour ce système d'acheminement d'événement.

- **Correspondance par catégorie d'événement**.
  1. Pour acheminer tous les événements d'audit, quel que soit le niveau de l'état, sélectionnez **Inclure tous les événements d'audit**.
  2. Pour acheminer tous les événements de garantie, sélectionnez **Inclure les événements de garantie**.
  3. Pour acheminer tous les événements de modification de l'état de santé, sélectionnez **Inclure les événements de changement d'état**.
  4. Pour acheminer tous les événements de mise à jour de l'état de santé, sélectionnez **Inclure les événements de mise à jour d'état**.
  5. Sélectionnez les classes d'événement et le niveau de facilité de maintenance à acheminer.
  6. Entrez les ID d'un ou de plusieurs événements à exclure de l'acheminement. Séparez-les à l'aide d'une virgule (par exemple, `FQXHMEM0214I`,`FQXHMEM0214I`).
- **Correspondance par code d'événement**. Entrez les ID d'un ou de plusieurs événements à acheminer. Si vous entrez plusieurs ID, séparez-les à l'aide d'une virgule.
- **Exclusion par catégorie d'événement**.
  1. Pour exclure tous les événements d'audit, quel que soit le niveau de l'état, sélectionnez **Exclure tous les événements d'audit**.

2. Pour exclure tous les événements de garantie, sélectionnez **Exclure les événements de garantie**.
3. Pour exclure tous les événements de modification de l'état de santé, sélectionnez **Exclure les événements de changement d'état**.
4. Pour exclure tous les événements de mise à jour de l'état de santé, sélectionnez **Exclure les événements de mise à jour d'état**.
5. Sélectionnez les classes d'événement et le niveau de facilité de maintenance à exclure.
6. Entrez les ID d'un ou de plusieurs événements à acheminer. Séparez-les à l'aide d'une virgule.

- **Exclusion par code d'événement**. Entrez les ID d'un ou de plusieurs événements à exclure. Si vous entrez plusieurs ID, séparez-les à l'aide d'une virgule.

Etape 11. Choisissez d'inclure ou non certains types d'événements.

- **Inclure tous les événements d'audit**. Envoie des notifications à propos des événements d'audit, sur la base des catégories et des gravités sélectionnées pour les événements.
- **Inclure les événements de garantie**. Envoie des notifications à propos des garanties.
- **Inclure les événements de modification d'état**. Envoie des notifications à propos des modifications d'état.
- **Inclure les événements de mise à jour d'état**. Notifications envoyées au sujet de nouvelles alertes.
- **Inclure les événements du bulletin**. Envoie des notifications à propos des nouveaux bulletins.

Etape 12. Sélectionnez les types d'événements et les gravités pour lesquels vous souhaitez recevoir une notification.

Etape 13. Sélectionnez si oui ou non vous souhaitez filtrer les événements en fonction de la facilité de maintenance.

Etape 14. Cliquez sur **Suivant** pour afficher la page **Planificateur**.

Etape 15. **Facultatif :** Définissez les heures et les jours auxquels vous souhaitez que les événements spécifiés soient acheminés vers ce système d'acheminement d'événement. Seuls les événements qui se produisent pendant le créneau horaire indiqué sont acheminés.

Si vous ne créez pas de planning pour le système d'acheminement d'événement, les événements sont acheminés 24h/24 et 7j/7.

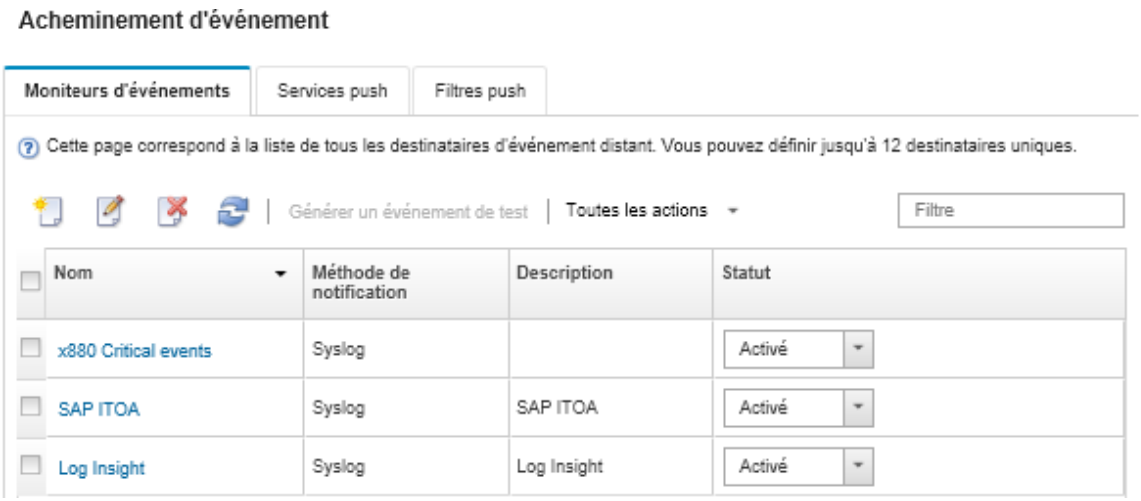
1. Utilisez l'icône **Défiler vers la gauche** (◀) et l'icône **Défiler vers la droite** (▶), ainsi que les boutons **Jour**, **Semaine** et **Mois** pour définir le jour et l'heure de début du planning.
2. Cliquez deux fois sur le créneau horaire pour ouvrir la boîte de dialogue Nouvelle période.
3. Indiquez les informations requises, y compris la date et les heures de début et de fin et précisez si le planning est répétitif.
4. Cliquez sur **Créer** pour enregistrer le planning et fermer la boîte de dialogue. Le nouveau planning est ajouté au calendrier.

Astuce :
- Vous pouvez modifier le créneau horaire en faisant glisser l'entrée du planning vers un autre créneau horaire du calendrier.
- Vous pouvez modifier la durée en sélectionnant le haut ou le bas de l'entrée de planning et en le faisant glisser vers la nouvelle heure dans le calendrier.
- Vous pouvez modifier l'heure de fin en sélectionnant le bas de l'entrée de planning et en le faisant glisser vers la nouvelle heure dans le calendrier.
- Vous pouvez modifier un planning en cliquant deux fois sur l'entrée de planning et en cliquant sur **Éditer l'entrée**.

- Vous pouvez afficher un résumé de toutes les entrées de planning en sélectionnant **Afficher le récapitulatif du planificateur**. Le récapitulatif comprend le créneau horaire pour chaque entrée et indique les entrées qui sont répétables.
- Vous pouvez supprimer une entrée de planning du calendrier ou planifier un récapitulatif en sélectionnant l'entrée, puis en cliquant sur **Supprimer une entrée**.

Etape 16. Cliquez sur **Créer**.

Le système d'acheminement d'événement figure dans le tableau Acheminement d'événement.



Etape 17. Sélectionnez le nouveau système d'acheminement d'événement, cliquez sur **Générer un événement de test**, puis assurez-vous que les événements sont acheminés correctement vers le gestionnaire SNMP distant.

Après avoir terminé

Sur la page Acheminement d'événement, vous pouvez effectuer les actions suivantes sur un système d'acheminement d'événement sélectionné.

- Actualiser la liste des systèmes d'acheminement d'événement en cliquant sur l'icône **Actualiser** ( ).
- Afficher les détails relatifs à un système d'acheminement d'événement spécifique en cliquant sur le lien dans la colonne **Nom**.
- Modifier les propriétés et les critères de filtrage d'un système d'acheminement d'événement en cliquant sur le nom de celui-ci dans la colonne **Nom**.
- Supprimer le système d'acheminement d'événement en cliquant sur l'icône **Supprimer** ( ).
- Suspendre l'acheminement d'événement (voir Interruption de l'acheminement d'événement).
- Téléchargez le fichier MIB qui contient des informations sur les alertes SNMP en cliquant sur l'icône **Créer** ( ), puis sur **Télécharger le fichier MIB** dans l'onglet Général de la boîte de dialogue Nouvel acheminement d'événement.

Fichier lenovoMgrAlert.mib

Ce fichier de base d'informations de gestion (MIB) décrit les interruptions SNMP que Lenovo XClarity Administrator génère, dont les alertes lancées par XClarity Administrator et les appareils gérés. Vous pouvez compiler ce fichier MIB dans n'importe quel gestionnaire d'alerte SNMP afin que les alertes SNMP envoyées par XClarity Administrator puissent être représentées correctement.

Vous pouvez télécharger le fichier MIB depuis l'interface Web en cliquant sur **Surveillance** ➙ **Acheminement d'événement** depuis la barre de menus, en cliquant sur l'icône **Créer** (), en sélectionnant **SNMP** pour le type de réexpéditeur d'événement, puis en cliquant sur **Télécharger le fichier MIB** au bas de la boîte de dialogue.

Les objets ci-après sont inclus dans toutes les alertes SNMP sortantes. Des objets supplémentaires peuvent être inclus dans certaines alertes SNMP. Tous les objets sont décrits dans le fichier MIB. Veuillez notez que les informations de récupération ne sont pas incluses dans l'interruption.

Remarque : Cette liste peut ne pas être identique d'une version à une autre de XClarity Administrator.
- **mgrTrapAppId**. Il s'agit de « Lenovo Event Manager ».
- **mgrTrapCommonEvtID**. ID d'événement commun
- **mgrTrapDateTime**. La date et l'heure locales du moment où l'événement a été généré
- **mgrTrapEventClass**. Source de l'événement. Il peut s'agir de : audit, refroidissement, alimentation, disques, mémoire, processeurs, système, test, adaptateur, extension, module d'E-S ou lame.
- **mgrTrapEvtID**. L'identificateur unique de l'événement
- **mgrTrapFailFRUs**. Une liste des UUID FRU défaillants et séparés par une virgule, le cas échéant
- **mgrTrapFailSNs**. Il s'agit d'une liste des numéros de série des FRU défaillants, séparés par une virgule, le cas échéant.
- **mgrTrapFullyQualifiedDomainName**. Il s'agit du nom de domaine qualifié dans son intégralité : le nom d'hôte et le nom de domaine
- **mgrTrapID**. ID alerte
- **mgrTrapMsgText**. Texte du message (anglais uniquement)
- **mgrTrapMsgID**. Identificateur du message
- **mgrTrapMtm**. Type du modèle de l'appareil ayant généré l'événement
- **mgrTrapService**. Indicateur de la facilité de maintenance. Il peut s'agir de 000 (inconnu), 100 (aucun), 200 (centre de maintenance) ou 300 (client)
- **mgrTrapSeverity**. Indicateur de gravité. Il y a différences possibilités : information, avertissement, mineur, majeur ou critique
- **mgrTrapSN**. Numéro de série de l'appareil ayant généré l'événement.
- **mgrTrapSrcIP**. Adresse IP de l'appareil à partir duquel l'événement généré a été reçu
- **mgrTrapSrcLoc**. Emplacement de l'appareil qui a généré l'événement, en langue anglaise uniquement (par exemple, Slot#xx)
- **mgrTrapSrcName**. Nom d'hôte ou nom d'affichage de l'appareil qui a généré l'événement
- **mgrTrapSysContact**. ID de coordonnées configuré par l'utilisateur
- **mgrTrapSysLocation**. Informations sur l'emplacement de l'appareil configurées par l'utilisateur
- **mgrTrapSystemName**. Nom de l'appareil, nom de composant et emplacement
- **mgrTrapTxtId**. Nom d'hôte ou adresse IP du serveur Lenovo Event Manager ayant généré l'interruption
- **mgrTrapUserid**. ID utilisateur associé à l'événement (si l'événement est interne et que la classe d'événements est Audit)
- **mgrTrapUuid**. UUID de l'appareil qui a généré l'événement

Configuration de l'acheminement d'événement vers un syslog

Vous pouvez configurer Lenovo XClarity Administrator pour l'acheminement d'événements spécifiques vers un syslog.

À propos de cette tâche

Vous pouvez créer et activer jusqu'à 20 système d'acheminement d'événement pour l'envoi d'événements à des destinataires spécifiques.

Si XClarity Administrator est réamorcé après la configuration des systèmes d'acheminement d'événement, vous devez attendre que le serveur de gestion regénère des données internes pour que les événements soient correctement acheminés.

Remarque : À compter de XClarity Administrator version 1.2.0, la zone **Commutateurs** est incluse sur l'onglet **Événements** dans les boîtes de dialogue Nouveau système d'acheminement d'événement et Modifier les systèmes d'acheminement d'événement. Si vous avez effectué une mise à niveau vers la version 1.2.0 ou une version ultérieure à partir d'une édition antérieure, pensez à mettre à jour vos systèmes d'acheminement d'événement de manière à inclure ou exclure les événements RackSwitch, le cas échéant. Cette action est nécessaire même si vous avez coché la case **Tous les systèmes** pour sélectionner tous les appareils.

Procédure

Procédez comme suit pour créer un système d'acheminement d'événement pour un syslog.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez **Surveillance → Acheminement d'événement**. La page Acheminement d'événement s'affiche.

Etape 2. Cliquez sur l'onglet **Réexpéditeur d'événement**.

Etape 3. Cliquez sur l'icône **Créer** ( ). L'onglet **Général** de la boîte de dialogue Nouveau système d'acheminement d'événement s'affiche.

Etape 4. Sélectionnez **Syslog** comme type de système d'acheminement d'événement, puis indiquez les informations spécifiques au protocole :

- Entrez le nom, l'hôte de destination et la description facultative du système d'acheminement d'événement.
- Entrez le port à utiliser pour l'acheminement des événements. La valeur par défaut est `514`.
- Sélectionnez le protocole à utiliser pour l'acheminement des événements. Les valeurs possibles sont les suivantes.
  - **UDP**
  - **TCP**
- Entrez le délai d'attente (en secondes) pour la demande. La valeur par défaut est 30 secondes.
- Vous pouvez aussi sélectionner le format de l'horodatage dans le syslog. Les valeurs possibles sont les suivantes.
  - **Heure locale**. Format par défaut, par exemple `Fri Mar 31 05:57:18 EDT 2017`.
  - **Heure GMT**. Norme internationale (ISO8601) pour les dates et les heures, par exemple `2017-03-31T05:58:20-04:00`.

Etape 5. Cliquez sur **Format de sortie** pour choisir le format de sortie des données d'événements à acheminer. Les informations varient pour chaque type de système d'acheminement d'événement.

L'exemple de format de sortie suivante est le format par défaut pour les destinataires sylog. Tous les mots entre crochets doubles sont les variables qui sont remplacées par des valeurs réelles lors de l'acheminement d'un événement. Les variables disponibles pour les destinataires sylog sont répertoriées dans la boîte de dialogue Format de sortie.

```
<8[[SysLogSeverity]]> [[EventTimeStamp]] [appl=LXCA service=[[EventService]] severity=[[EventSeverity]]
class=[[EventClass]] appladdr=[[LXCA_IP]] user=[[EventUserName]] src=[[SysLogSource]] uuid=[[UUID]]
me=[[DeviceSerialNumber]] resourceIP=[[DeviceIPAddress]] systemName=[[DeviceFullPathName]]
seq=[[EventSequenceID]] EventID=[[EventID]] CommonEventID=[[CommonEventID]]
```

Vous pouvez cliquer sur **Réinitialiser aux valeurs par défaut** pour rétablir le format de sortie dans les zones par défaut.

Etape 6. Cliquez sur le bouton **Autoriser les événements exclus** pour autoriser ou empêcher le transfert des événements exclus.

Etape 7. Sélectionnez **Activer ce réexpéditeur** pour activer l'acheminement d'événement pour ce système d'acheminement d'événement.

Etape 8. Cliquez sur **Suivant** pour afficher l'onglet **Appareils**.

Etape 9. Sélectionnez les appareils et les groupes que vous souhaitez surveiller pour ce système d'acheminement d'événement.

Astuce : Pour acheminer des événements pour tous les appareils gérés (actuels et ultérieurs), cochez la case **Faire correspondre tous les systèmes**.Si vous ne cochez pas la case **Faire correspondre tous les systèmes**, assurez-vous que la colonne UUID des appareils sélectionnés ne contient pas d'UUID factice. Un UUID factice est affecté aux appareils qui n'ont pas encore été récupérés après un redémarrage ou qui ne sont pas complètement reconnus par le serveur de gestion. Si vous sélectionnez un appareil doté d'un UUID factice, l'acheminement d'événement fonctionne pour cet appareil jusqu'à ce que celui-ci soit complètement reconnu ou récupéré et que l'UUID factice soit remplacé par un UUID réel.

Etape 10. Cliquez sur **Suivant** pour afficher la page **Evénements**.

Etape 11. Sélectionnez les filtres à utiliser pour ce système d'acheminement d'événement.

- **Correspondance par catégorie d'événement**.
  1. Pour acheminer tous les événements d'audit, quel que soit le niveau de l'état, sélectionnez **Inclure tous les événements d'audit**.
  2. Pour acheminer tous les événements de garantie, sélectionnez **Inclure les événements de garantie**.
  3. Pour acheminer tous les événements de modification de l'état de santé, sélectionnez **Inclure les événements de changement d'état**.
  4. Pour acheminer tous les événements de mise à jour de l'état de santé, sélectionnez **Inclure les événements de mise à jour d'état**.
  5. Sélectionnez les classes d'événement et le niveau de facilité de maintenance à acheminer.
  6. Entrez les ID d'un ou de plusieurs événements à exclure de l'acheminement. Séparez-les à l'aide d'une virgule (par exemple, `FQXHMEM0214I,FQXHMEM0214I`).
- **Correspondance par code d'événement**. Entrez les ID d'un ou de plusieurs événements à acheminer. Si vous entrez plusieurs ID, séparez-les à l'aide d'une virgule.
- **Exclusion par catégorie d'événement**.
  1. Pour exclure tous les événements d'audit, quel que soit le niveau de l'état, sélectionnez **Exclure tous les événements d'audit**.
  2. Pour exclure tous les événements de garantie, sélectionnez **Exclure les événements de garantie**.
  3. Pour exclure tous les événements de modification de l'état de santé, sélectionnez **Exclure les événements de changement d'état**.
  4. Pour exclure tous les événements de mise à jour de l'état de santé, sélectionnez **Exclure les événements de mise à jour d'état**.
  5. Sélectionnez les classes d'événement et le niveau de facilité de maintenance à exclure.
  6. Entrez les ID d'un ou de plusieurs événements à acheminer. Séparez-les à l'aide d'une virgule.
- **Exclusion par code d'événement**. Entrez les ID d'un ou de plusieurs événements à exclure. Si vous entrez plusieurs ID, séparez-les à l'aide d'une virgule.

Etape 12. Choisissez d'inclure ou non certains types d'événements.

- **Inclure tous les événements d'audit**. Envoie des notifications à propos des événements d'audit, sur la base des catégories et des gravités sélectionnées pour les événements.
- **Inclure les événements de garantie**. Envoie des notifications à propos des garanties.

- **Inclure les événements de modification d'état**. Envoie des notifications à propos des modifications d'état.
- **Inclure les événements de mise à jour d'état**. Notifications envoyées au sujet de nouvelles alertes.
- **Inclure les événements du bulletin**. Envoie des notifications à propos des nouveaux bulletins.

Etape 13. Sélectionnez les types d'événements et les gravités pour lesquels vous souhaitez recevoir une notification.

Etape 14. Sélectionnez si oui ou non vous souhaitez filtrer les événements en fonction de la facilité de maintenance.

Etape 15. Cliquez sur **Suivant** pour afficher la page **Planificateur**.

Etape 16. **Facultatif :** Définissez les heures et les jours auxquels vous souhaitez que les événements spécifiés soient acheminés vers ce système d'acheminement d'événement. Seuls les événements qui se produisent pendant le créneau horaire indiqué sont acheminés.

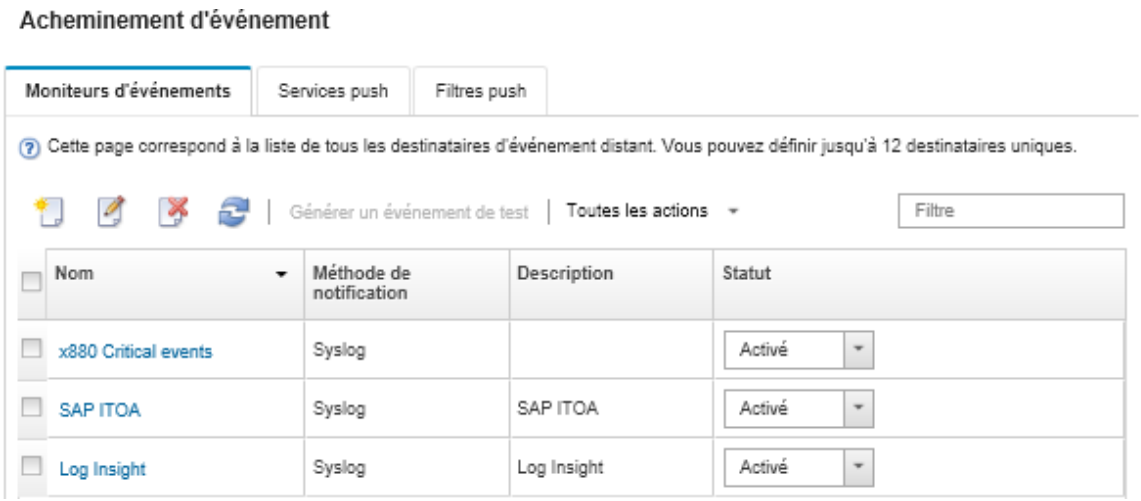
Si vous ne créez pas de planning pour le système d'acheminement d'événement, les événements sont acheminés 24h/24 et 7j/7.

1. Utilisez l'icône **Défiler vers la gauche** (◄) et l'icône **Défiler vers la droite** (►), ainsi que les boutons **Jour**, **Semaine** et **Mois** pour définir le jour et l'heure de début du planning.
2. Cliquez deux fois sur le créneau horaire pour ouvrir la boîte de dialogue Nouvelle période.
3. Indiquez les informations requises, y compris la date et les heures de début et de fin et précisez si le planning est répétitif.
4. Cliquez sur **Créer** pour enregistrer le planning et fermer la boîte de dialogue. Le nouveau planning est ajouté au calendrier.

Astuce :
- Vous pouvez modifier le créneau horaire en faisant glisser l'entrée du planning vers un autre créneau horaire du calendrier.
- Vous pouvez modifier la durée en sélectionnant le haut ou le bas de l'entrée de planning et en le faisant glisser vers la nouvelle heure dans le calendrier.
- Vous pouvez modifier l'heure de fin en sélectionnant le bas de l'entrée de planning et en le faisant glisser vers la nouvelle heure dans le calendrier.
- Vous pouvez modifier un planning en cliquant deux fois sur l'entrée de planning et en cliquant sur **Éditer l'entrée**.
- Vous pouvez afficher un résumé de toutes les entrées de planning en sélectionnant **Afficher le récapitulatif du planificateur**. Le récapitulatif comprend le créneau horaire pour chaque entrée et indique les entrées qui sont répétables.
- Vous pouvez supprimer une entrée de planning du calendrier ou planifier un récapitulatif en sélectionnant l'entrée, puis en cliquant sur **Supprimer une entrée**.

Etape 17. Cliquez sur **Créer**.

Le système d'acheminement d'événement figure dans le tableau Acheminement d'événement.



Etape 18. Sélectionnez le nouveau système d'acheminement d'événement, cliquez sur **Générer un événement de test**, puis assurez-vous que les événements sont acheminés correctement vers le syslog approprié.

Après avoir terminé

Sur la page Acheminement d'événement, vous pouvez effectuer les actions suivantes sur un système d'acheminement d'événement sélectionné.

- Actualiser la liste des systèmes d'acheminement d'événement en cliquant sur l'icône **Actualiser** ( ).
- Afficher les détails relatifs à un système d'acheminement d'événement spécifique en cliquant sur le lien dans la colonne **Nom**.
- Modifier les propriétés et les critères de filtrage d'un système d'acheminement d'événement en cliquant sur le nom de celui-ci dans la colonne **Nom**.
- Supprimer le système d'acheminement d'événement en cliquant sur l'icône **Supprimer** ( ).
- Suspendre l'acheminement d'événement (voir Interruption de l'acheminement d'événement).

Interruption de l'acheminement d'événement

Vous pouvez suspendre l'acheminement d'événement en désactivant le système d'acheminement d'événement. La suspension de l'acheminement d'événement arrête la surveillance des événements entrants. Les événements qui sont reçus alors que la surveillance est suspendue ne sont pas acheminés.

À propos de cette tâche

L'état Désactivé n'est pas persistant. Si le nœud de gestion est redémarré, tous les réexpéditeurs d'événement sont activés.

Procédure

Procédez comme suit pour désactiver l'acheminement des événements.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez **Surveillance → Acheminement des événements**. La page Acheminement d'événement s'affiche.

Etape 2. Sélectionnez **Désactiver** dans la colonne **État** pour chaque système d'acheminement d'événement que vous souhaitez suspendre.

Acheminement des événements vers des appareils mobiles

Vous pouvez configurer Lenovo XClarity Administrator pour envoyer des notifications d'événement à des appareils mobiles.

Avant de commencer

Les conditions suivantes doivent être réunies pour permettre l'acheminement des événements vers des appareils mobiles :

- Vérifiez qu'un serveur DNS valide est configuré pour autoriser Lenovo XClarity Administrator à se connecter aux serveurs push Apple ou Google. Cette configuration peut être effectuée en cliquant sur **Administration → Accès réseau → Éditer l'accès réseau**, puis en cliquant sur l'onglet **Paramètres Internet** (voir Configuration de l'accès réseau).
- Vérifiez que tous les ports requis pour la gestion des événements sont ouverts sur le réseau et les pare-feu. Pour plus d'informations sur les exigences liées aux ports, voir Disponibilité de port dans la documentation en ligne de Lenovo XClarity Administrator.

À propos de cette tâche

Lorsque l'application Lenovo XClarity Mobile est installée sur un appareil mobile, vous pouvez activer chaque instance Lenovo XClarity Administrator connectée pour envoyer des notifications d'événement à cet appareil mobile. Lorsque les notifications push sont activées pour une instance spécifique, une souscription est créée dans Lenovo XClarity Administrator pour cet appareil mobile.

Vous pouvez définir les événements qui sont envoyés à l'appareil mobile en affectant des filtres d'événements globaux prédéfinis ou personnalisés à chaque instance Lenovo XClarity Administrator. Les filtres d'événements globaux prédéfinis sont activés par défaut. Lenovo XClarity Administrator démarre la surveillance d'événements entrants selon des critères de filtrage. Lorsqu'une concordance est trouvée, l'événement est acheminé vers l'appareil mobile.

Pour plus d'informations sur Lenovo XClarity Mobile et les appareils mobiles pris en charge, voir Utilisation de l'application Lenovo XClarity Mobile.

Procédure

Pour configurer l'envoi de notifications push à cet appareil mobile, procédez comme suit à partir de l'application Lenovo XClarity Mobile sur votre appareil mobile.

Etape 1. Activer les notifications push :

- Vous pouvez activer les notifications push lorsque vous créez une connexion à une instance Lenovo XClarity Administrator. Les notifications push sont activées par défaut.
- Vous pouvez activer les notifications push sur des connexions existantes en activant un ou plusieurs filtres d'événements.

Etape 2. Affecter des filtres d'événements globaux pour définir les événements qui doivent être acheminés vers l'appareil mobile :

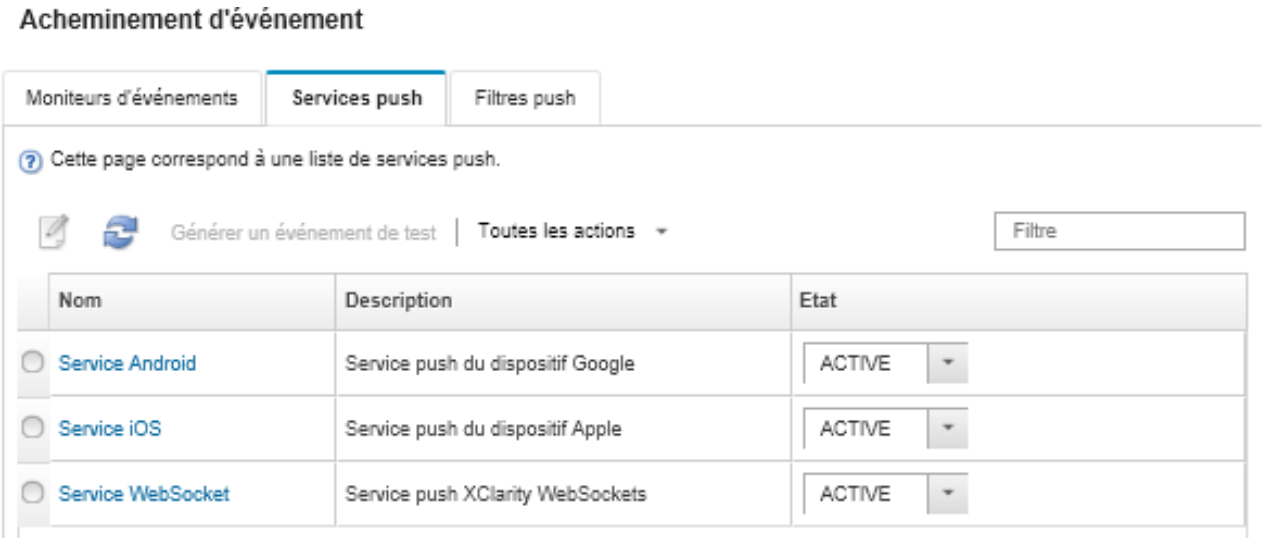
Remarque : Vous pouvez ajouter ou retirer des filtres globaux dans la souscription uniquement à partir de l'application Lenovo XClarity Mobile. Vous pouvez créer des filtres globaux uniquement à partir de l'interface Web Lenovo XClarity Administrator. Pour plus d'informations sur la création de filtres d'événements globaux personnalisés, voir Création de filtres d'événements pour des appareils mobiles et des applications WebSocket.

1. Appuyez sur **Paramètres → Notifications push**. Une liste de connexions Lenovo XClarity Administrator s'affiche.
2. Appuyez sur l'instance Lenovo XClarity Administrator pour afficher une liste de filtres push.

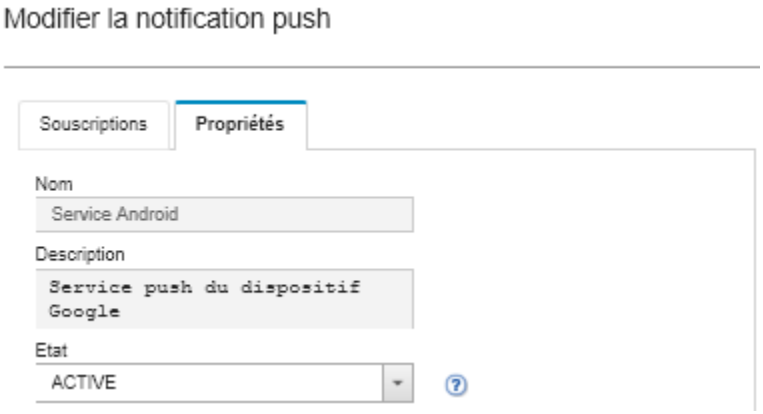
3. Activez les filtres d'événements pour les événements qui doivent être acheminés vers l'appareil mobile pour l'instance Lenovo XClarity Administrator.
4. Appuyez sur **Toucher pour générer une notification push test** afin de vérifier que les notifications d'événement sont correctement envoyées.

Résultats

Vous pouvez gérer des souscriptions sur la page Acheminement d'événement dans l'interface Web Lenovo XClarity Administrator. Cliquez sur **Surveillance → Acheminement d'événement** pour afficher la page Acheminement d'événement.



- Vous pouvez modifier les propriétés du service de notification d'appareil à partir de l'onglet **Services push** de la page Acheminement d'événement en cliquant sur le lien vers le service de notification push (Google ou Apple) dans la colonne **Nom** afin d'afficher la boîte de dialogue Modifier la notification push, puis en cliquant sur l'onglet **Propriétés**.



- Vous pouvez activer et désactiver des souscriptions :
  - Activez ou désactivez toutes les souscriptions relatives à un service de notification d'appareil donné à partir de l'onglet **Services push** de la page Acheminement d'événement en sélectionnant l'état **Activé** ou **Désactivé** dans le tableau du service de notification d'appareil concerné.
  - Activez ou désactivez toutes les souscriptions relatives à un appareil donné à partir de l'application Lenovo XClarity Mobile en appuyant sur **Paramètres → Notification push**, puis en activant ou en désactivant la notification push activée.

  - Activez ou désactivez une souscription donnée à partir de l'application Lenovo XClarity Mobile en appuyant sur **Paramètres → Notification push**, en appuyant sur une connexion Lenovo XClarity Administrator et en activant au moins un filtre d'événements ou en désactivant tous les filtres d'événements.
- Vous pouvez générer un événement de test pour toutes les souscriptions relatives à un service mobile donné à partir de l'onglet **Services push** de la page Acheminement d'événement en sélectionnant le service mobile et en cliquant sur **Générer un événement de test**.
- Vous pouvez afficher la liste des souscriptions actuelles. Sur l'onglet **Services push** de la page Acheminement d'événement, cliquez sur le lien vers le service de notification d'appareil applicable (Android ou iOS) dans la colonne **Nom** afin d'afficher la boîte de dialogue Modifier la notification push, puis cliquez sur l'onglet **Souscriptions**. L'ID d'appareil identifie chaque souscription.

  Astuces :

  - L'ID d'appareil correspond au premier et aux six derniers chiffres de l'ID d'inscription push. Vous pouvez rechercher l'ID d'inscription push à partir de l'application Lenovo XClarity Mobile en appuyant sur **Paramètres → À propos de → ID d'inscription push**.
  - Si vous êtes connecté en tant qu'utilisateur disposant de l'un des rôles énumérés ci-après, toutes les souscriptions sont affichées ; sinon, seules les souscriptions pour l'utilisateur connecté sont affichées.
    - **lxc-admin**
    - **lxc-supervisor**
    - **lxc-security-admin**
    - **lxc-sysmgr**
- Vous pouvez afficher la liste des filtres d'événements affectés à la souscription à partir de l'onglet **Souscriptions** de la boîte de dialogue Modifier la notification push en développant **Liste de filtres** dans la colonne **Filtres d'événements** pour la souscription.

- Vous pouvez créer des filtres d'événements pour une souscription donnée à partir de l'onglet **Souscriptions** de la boîte de dialogue Modifier la notification push en sélectionnant la souscription, puis en cliquant sur l'icône **Créer** ( ).

  Remarque : Ces filtres d'événements s'appliquent uniquement à une souscription donnée et ne peuvent pas être utilisés par d'autres souscriptions.

  Vous pouvez également éditer ou retirer un filtre d'événements en sélectionnant celui-ci, puis en cliquant sur l'icône **Éditer** ( ) ou **Retirer** ( ), respectivement.

- Vous pouvez déterminer l'état de la dernière tentative d'envoi de type push pour une souscription donnée à partir de l'onglet **Souscriptions** de la boîte de dialogue Modifier la notification push. La colonne **Horodatage** indique la date et l'heure de la dernière tentative d'envoi de type push. La colonne **État** Indique si la notification push a été correctement distribuée au service push. Aucun état indiquant si la notification push a été distribuée ou non sur l'appareil par le service n'est disponible. Si la distribution du service push a échoué, la colonne État fournit des informations supplémentaires sur cet échec.
- Vous pouvez générer un événement de test pour une souscription donnée à partir de l'onglet **Souscriptions** de la boîte de dialogue Modifier la notification push en sélectionnant la souscription et en cliquant sur **Générer un événement de test**.
- Vous pouvez retirer une souscription à partir de l'onglet **Souscriptions** de la boîte de dialogue Modifier la notification push en sélectionnant la souscription, puis en cliquant sur l'icône **Retirer** ().

Acheminement des événements vers des services WebSocket

Vous pouvez configurer Lenovo XClarity Administrator pour envoyer des notifications d'événement à des services WebSocket.

À propos de cette tâche

Les souscriptions WebSocket ne sont pas stockées de manière persistante dans Lenovo XClarity Administrator. Lorsque Lenovo XClarity Administrator est réamorcé, les souscripteurs WebSocket doivent souscrire à nouveau.

Procédure

Pour envoyer une notification d'événement à un service WebSocket, procédez comme suit.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez **Surveillance → Acheminement d'événement**. La page Acheminement d'événement s'affiche.

Etape 2. Cliquez sur l'onglet **Services push**.

Etape 3. Cliquez sur le lien **Service WebSocket** dans la colonne **Nom**. La boîte de dialogue Modifier la notification push s'affiche.

Etape 4. Cliquez sur l'onglet **Souscriptions**.

Etape 5. Cliquez sur l'icône **Créer** ().

Etape 6. Saisissez l'adresse IP de l'hôte de destination.

Etape 7. Cliquez sur **Créer**.

Etape 8. Sélectionnez la nouvelle souscription, cliquez sur **Générer un événement de test**, puis assurez-vous que les événements sont acheminés correctement vers le service WebSocket.

Résultats

Sur l'onglet **Souscriptions** de la boîte de dialogue Modifier la notification push, vous pouvez effectuer les actions suivantes sur une souscription WebSocket sélectionnée :

- Actualiser la liste des services WebSocket en cliquant sur l'icône **Actualiser** ().
- Supprimer des souscriptions en sélectionnant les souscriptions concernées et en cliquant sur l'icône **Supprimer** ().
- Déterminer l'état de la dernière tentative d'envoi de type push pour une souscription donnée en affichant le contenu de la colonne **État**. Si la tentative échoue, cette colonne contient un message qui décrit l'erreur.

Sur l'onglet **Propriétés** de la boîte de dialogue Modifier la notification push, vous pouvez effectuer les actions suivantes :

- Modifier les propriétés de service WebSocket, y compris le délai d'inactivité de connexion, la taille maximale de mémoire tampon, le nombre maximal de souscripteurs et le délai d'attente d'inscription.
- Vous pouvez réinitialiser le service WebSocket avec les paramètres par défaut en cliquant sur **Restaurer les valeurs par défaut**.
- Suspendre l'envoi des notifications d'événement à toutes les souscriptions du service WebSocket en sélectionnant la valeur Désactivé pour **État**.

Sur l'onglet **Services push** de la page Acheminement d'événement, vous pouvez générer un événement de test pour toutes les souscriptions WebSocket en sélectionnant le service WebSocket et en cliquant sur **Générer un événement de test**.

Création de filtres d'événements pour des appareils mobiles et des applications WebSocket

Vous pouvez créer des filtres d'événements globaux utilisables dans une ou plusieurs souscriptions pour des appareils mobiles et des applications WebSocket. Vous pouvez également créer des filtres d'événements qui sont spécifiques à une souscription.

Avant de commencer

Vous devez posséder des droits de superviseur pour créer des filtres d'événements.

Vous pouvez créer jusqu'à 20 filtres d'événements globaux.

À propos de cette tâche

Les filtres d'événements globaux suivants sont prédéfinis :

- **Faire correspondre tous les événements critiques**. Ce filtre fait correspondre tous les événements critiques qui sont générés par un appareil géré ou par XClarity Administrator.
- **Faire correspondre tous les événements d'avertissement**. Ce filtre fait correspondre tous les événements d'avertissement qui sont générés par un appareil géré ou par XClarity Administrator.

Procédure

Pour créer un filtre d'événements global, procédez comme suit.

- Créez un filtre d'événements global utilisable par n'importe quelle souscription.
  1. Dans la barre de menus de XClarity Administrator, cliquez **Surveillance → Acheminement d'événement**. La page Acheminement d'événement s'affiche.
  2. Cliquez sur l'onglet **Filtres push**.
  3. Cliquez sur l'icône **Créer** ( ). L'onglet **Général** de la boîte de dialogue Nouveau filtre push s'affiche.
  4. Spécifiez un nom et une description d'option pour ce filtre d'événements.
  5. Cliquez sur **Suivant** pour afficher la page **Systèmes**.
  6. Sélectionnez les dispositifs à surveiller.

     Astuce : Pour acheminer des événements pour tous les appareils gérés (actuels et ultérieurs), cochez la case **Faire correspondre tous les systèmes**.Si vous ne cochez pas la case **Faire correspondre tous les systèmes**, assurez-vous que la colonne UUID des appareils sélectionnés ne contient pas d'UUID factice. Un UUID factice est affecté aux appareils qui n'ont pas encore été récupérés après

un redémarrage ou qui ne sont pas complètement reconnus par le serveur de gestion. Si vous sélectionnez un appareil doté d'un UUID factice, l'acheminement d'événement fonctionne pour cet appareil jusqu'à ce que celui-ci soit complètement reconnu ou récupéré et que l'UUID factice soit remplacé par un UUID réel.

7. Cliquez sur **Suivant** pour afficher la page **Evénements**.
8. Sélectionnez les composants et les niveaux de gravité pour lesquels vous souhaitez que des événements soient acheminés.

   Astuce :
   - Pour acheminer tous les événements matériel, sélectionnez **Faire correspondre tous les événements**.
   - Pour acheminer des événements d'audit, sélectionnez **Inclure tous les événements d'audit**.
   - Pour acheminer des événements de garantie, sélectionnez **Inclure les événements de garantie**.
9. Cliquez sur **Créer**.

- Créez un filtre d'événements pour une souscription spécifique :
  1. Dans la barre de menus de XClarity Administrator, cliquez **Surveillance → Acheminement d'événement**. La page Nouvel acheminement d'événement s'affiche.
  2. Cliquez sur l'onglet **Filtres push**.
  3. Sélectionnez le lien du type d'appareil mobile (Android ou iOS) dans la colonne Nom de la table. La boîte de dialogue Modifier la notification push s'affiche.
  4. Cliquez sur l'onglet **Souscriptions** pour afficher une liste de souscriptions actives.
  5. Sélectionnez la souscription, puis cliquez sur l'icône **Créer** ( ). L'onglet **Général** de la boîte de dialogue Nouveau filtre d'événements s'affiche.
  6. Spécifiez un nom et une description d'option pour ce filtre d'événements.
  7. Cliquez sur **Suivant** pour afficher la page **Systèmes**.
  8. Sélectionnez les dispositifs à surveiller.

     Astuce : Pour acheminer des événements pour tous les appareils gérés (actuels et ultérieurs), cochez la case **Faire correspondre tous les systèmes**.Si vous ne cochez pas la case **Faire correspondre tous les systèmes**, assurez-vous que la colonne UUID des appareils sélectionnés ne contient pas d'UUID factice. Un UUID factice est affecté aux appareils qui n'ont pas encore été récupérés après un redémarrage ou qui ne sont pas complètement reconnus par le serveur de gestion. Si vous sélectionnez un appareil doté d'un UUID factice, l'acheminement d'événement fonctionne pour cet appareil jusqu'à ce que celui-ci soit complètement reconnu ou récupéré et que l'UUID factice soit remplacé par un UUID réel.
  9. Cliquez sur **Suivant** pour afficher la page **Evénements**.
  10. Sélectionnez les composants et les niveaux de gravité pour lesquels vous souhaitez que des événements soient acheminés.

      Astuce :
      - Pour acheminer tous les événements matériel, sélectionnez **Faire correspondre tous les événements**.
      - Pour acheminer des événements d'audit, sélectionnez **Inclure tous les événements d'audit**.
      - Pour acheminer des événements de garantie, sélectionnez **Inclure les événements de garantie**.
  11. Cliquez sur **Créer**.

Après avoir terminé

Sur l'onglet Filtres push de la page Acheminement d'événement, vous pouvez effectuer les actions suivantes sur un filtre d'événements sélectionné :

- Actualiser la liste de filtre d'événements en cliquant sur l'icône **Actualiser** ().
- Afficher les détails relatifs à un filtre d'événements spécifique en cliquant sur le lien dans la colonne **Nom**.
- Modifier les propriétés de filtre d'événements et les critères de filtre en cliquant sur l'icône **Éditer** ().

Supprimer le filtre d'événements en cliquant sur l'icône **Supprimer** ().

Gestion des travaux

Les *Travaux* sont des tâches plus longues qui sont effectuées sur un ou plusieurs appareils. Vous pouvez planifier certains travaux pour qu'ils s'exécutent une seule fois (immédiatement ou ultérieurement), de manière récurrente ou en cas d'événement spécifique.

Les travaux s'exécutent en arrière-plan. Vous pouvez voir l'état de chaque tâche en consultant le journal des travaux.

Surveillance des travaux

Vous pouvez afficher un journal de tous les travaux qui sont démarrés par Lenovo XClarity Administrator. Le journal des travaux inclut des travaux qui sont en cours d'exécution, terminés ou présentent des erreurs.

À propos de cette tâche

Les *Travaux* sont des tâches plus longues qui sont effectuées sur un ou plusieurs dispositifs. Par exemple, si vous déployez un système d'exploitation sur plusieurs serveurs, chaque déploiement de serveur est répertorié sous la forme d'un travail distinct.

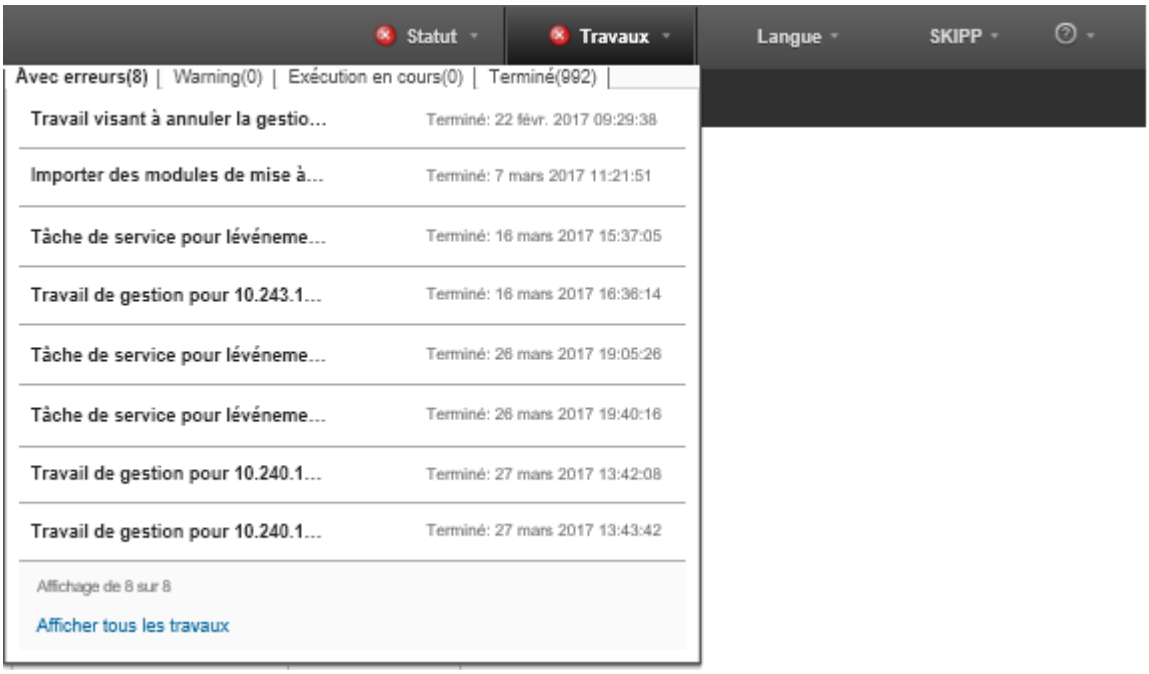
Les travaux s'exécutent en arrière-plan. Vous pouvez voir l'état de chaque tâche en consultant le journal des travaux.

Le journal des travaux contient des informations sur chaque travail. Le journal contient un maximum de 1 000 travaux ou 1 Go. Lorsque la taille maximale est atteinte, les travaux terminés les plus anciens sont supprimés. En l'absence de travaux terminés avec succès dans le journal, les travaux terminés avec avertissements les plus anciens sont supprimés. En l'absence de travaux terminés avec succès ou avec avertissements dans le journal, les travaux terminés avec erreurs les plus anciens sont supprimés.

Procédure

Procédez selon l'une des étapes suivantes pour afficher le journal des travaux.

- Dans la barre de titre de XClarity Administrator, cliquez sur **Travaux** pour afficher un récapitulatif des travaux qui s'exécutent, sont terminés et contiennent des erreurs.



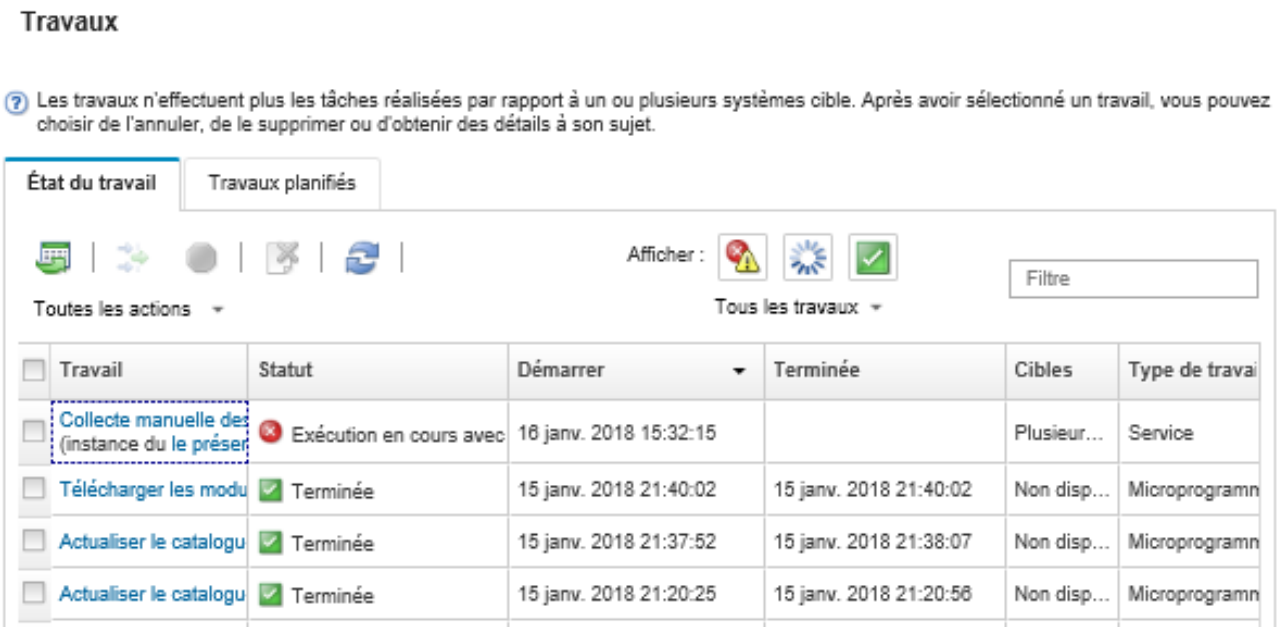
Dans cette liste déroulante, vous pouvez cliquer sur les onglets suivants :
- **Erreurs**. Affiche une liste de tous les travaux auxquels des erreurs sont associés.
- **Avertissements**. Affiche une liste de tous les travaux auxquels des avertissements sont associés.
- **Exécution en cours**. Affiche la liste de tous les travaux actuellement en cours.
- **Terminé**. Affiche la liste de tous les travaux terminés.

Survolez une entrée de travail dans la liste déroulante pour obtenir plus d'informations sur le travail, y compris l'état, la progression et l'utilisateur qui a créé le travail.

- Dans la barre de titre de XClarity Administrator, cliquez sur **Travaux**, puis cliquez sur le lien **Afficher tous les travaux** pour afficher la page État des travaux.
- Dans la barre de menu de XClarity Administrator, cliquez sur **Surveiller → Travaux**, puis cliquez sur l'onglet **État des travaux** pour afficher la page État des travaux.

Après avoir terminé

La page Travaux s'affiche avec une liste de tous les travaux pour XClarity Administrator.



Depuis cette page, vous pouvez effectuer les actions suivantes :

- Créer des planifications de travail en cliquant sur l'onglet **Travaux planifiés** (voir Planification des travaux).
- Pour afficher des informations supplémentaires sur un travail spécifique, cliquez sur la description du travail dans la colonne **Travaux**. Un dialogue s'affiche avec une liste de sous-tâches (sous-travaux) et leurs cibles, un résumé des sous-tâches avec toutes les actions nécessaires, et les détails du journal tels que la gravité et l'horodatage de chaque message. Vous pouvez choisir de masquer ou d'afficher les journaux des tâches enfants.
- Pour les travaux planifiés, vous pouvez afficher des informations sur la planification de travail en cliquant sur « ce » lien sous la description du travail dans la colonne **Travaux**.
- Modifiez le nombre de travaux qui sont affichés par page. La valeur par défaut est de 10 travaux. Vous pouvez afficher 25, 50 ou tous les travaux.
- Limitez la liste des travaux qui sont affichés :
  - Pour afficher uniquement les travaux d'une source spécifique, cliquez sur **Types de travail** et choisissez les options suivantes.
    - **Tous les types de travail**
    - **Service**
    - **Management**
    - **Configuration**
    - **Firmware**
    - **Health**
    - **Power**
    - **accès à distance**
    - **ID du système**
    - **Images SE**
    - **Déploiement SE**
    - **Exportation du profil de SE**
    - **Custom**
    - **Inventory**
    - **Inconnu**
  - Pour afficher uniquement les travaux associés à un type spécifique de planning, cliquez sur **Types de planning** et choisissez les options suivantes.

  - **Tous les types de planning**
  - **Unique**
  - **Récurrent**
  - **Déclenché**
- Masquez ou affichez des travaux qui contiennent des erreurs ou avertissements en cliquant sur l'icône **Masquer les travaux avec erreur/avertissement** ().
- Affichez ou masquez des travaux actuellement en cours d'exécution en cliquant sur l'icône **Masquer les travaux en cours d'exécution** ().
- Affichez ou masquez des travaux terminés en cliquant sur l'icône **Masquer les travaux terminés** ().
- Répertoriez uniquement les travaux qui contiennent un texte spécifique en indiquant le texte dans la zone **Filtre**.
- Si le filtrage est appliqué à la page, retirez le filtre en cliquant sur l'icône **Afficher tous les travaux** ().
- Triez les travaux par colonne en cliquant sur un en-tête de colonne.

- Exportez la liste des travaux au format CSV en cliquant sur l'icône **Exporter au format CSV** ().

  Remarque : Les horodatages dans le journal exporté utilisent l'heure locale spécifiée par le navigateur Web.
- Annulez les travaux ou sous-tâches en cours d'exécution en sélectionnant un ou plusieurs travaux ou sous-tâches et en cliquant sur l'icône **Arrêter** ().

  Remarque : L'annulation du travail peut prendre plusieurs minutes.
- Supprimez les travaux ou sous-tâches terminés du journal des travaux en sélectionnant un ou plusieurs travaux ou sous-tâches terminés et en cliquant sur l'icône **Supprimer** ().
- Exportez des informations sur des travaux spécifiques en sélectionnant les travaux et en cliquant sur l'icône **Exporter au format CSV** ().
- Actualisez le journal des travaux en cliquant sur l'icône **Actualiser** ().

Planification des travaux

Vous pouvez créer des planifications dans Lenovo XClarity Administrator pour exécuter certaines tâches à des moments spécifiques.

À propos de cette tâche

Vous pouvez planifier les types de travail suivants :
- Tâches simples, par exemple, la mise hors tension et le réamorçage
- La collecte de données de maintenance pour des appareils spécifiques
- Actualisation des catalogues de mise à jour du microprogramme et du pilote de périphérique SE à partir du site Web de Lenovo
- L'actualisation du catalogue de mises à jour XClarity Administrator à partir du site Web de Lenovo
- Le téléchargement de microprogrammes à partir du site Web de Lenovo
- Mise à jour de microprogramme et des pilotes de périphérique du système d'exploitation sur les appareils gérés
- Sauvegarde des données et des paramètres XClarity Administrator
- Sauvegarde et restauration des données de configuration de commutateur

Vous pouvez planifier l'exécution des travaux :

- Une seule fois (immédiatement ou ultérieurement)
- De manière récurrente
- Lorsqu'un événement spécifique se produit

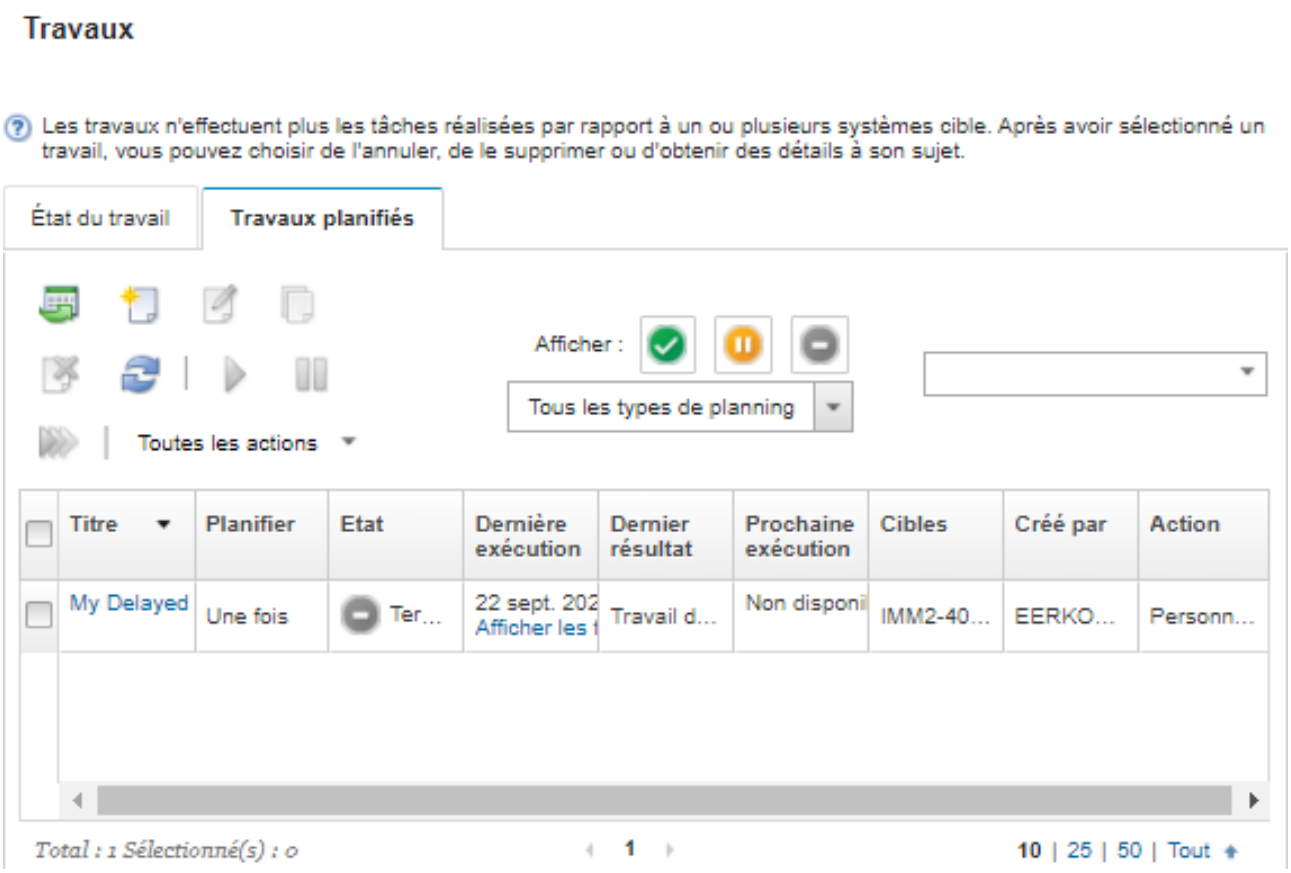
Procédure

Pour créer et planifier un travail, procédez comme suit.

- Pour les tâches complexes, telles que la mise à jour de microprogramme et la collecte de données de maintenance, créez le travail à partir de la page ou de la boîte de dialogue de la tâche en cours.
  1. Cliquez sur **Planning** pour créer une planification pour l'exécution de cette tâche. La boîte de dialogue Planifier un nouveau travail s'affiche.
  2. Entrez un nom pour le travail.
  3. Indiquez la fréquence d'exécution du travail. Les options disponibles dépendent du type de travail. Certains travaux ne peuvent pas être récurrents ou déclenchés par un événement.
     - **Unique**. Ces travaux s'exécutent une seule fois. Indiquez la date et l'heure auxquels vous souhaitez que ce travail s'exécute.
     - **Récurrent** Ces travaux s'exécutent plusieurs fois. Indiquez la fréquence à laquelle vous souhaitez que ce travail s'exécute.
     - **Déclenché par un événement**. Ces tâches s'exécutent lorsqu'un événement spécifique se produit.
       a. Indiquez la date et l'heure auxquels vous souhaitez que ce travail s'exécute, puis cliquez sur **Suivant**.
       b. Sélectionnez l'événement qui doit déclencher le travail.
  4. Cliquez sur **Créer le travail**.
- Pour des tâches simples, telles que la mise sous tension et le réamorçage, créez la planification de travail depuis la page Travaux.
  1. Dans la barre de titre de XClarity Administrator, cliquez sur **Surveiller → Travaux**, puis cliquez sur le lien **Travail planifié** pour afficher la page Travaux planifiés.
  2. Cliquez sur l'icône **Créer** ( ) pour afficher la boîte de dialogue Planifier de nouveaux travaux.
  3. Entrez un nom pour le travail.
  4. Indiquez la fréquence d'exécution du travail.
     - **Unique**. Ces travaux s'exécutent une seule fois.
       a. Indiquez la date et l'heure auxquels vous souhaitez que ce travail s'exécute, puis cliquez sur **Suivant**.
       b. Sélectionnez les appareils gérés sur lequel le travail doit s'exécuter.
     - **Récurrent** Ces travaux s'exécutent plusieurs fois.
       a. Indiquez la fréquence à laquelle vous souhaitez que ce travail s'exécute.
       b. Sélectionnez les appareils gérés sur lequel le travail doit s'exécuter**.**
     - **Déclenché par un événement**. Ces tâches s'exécutent lorsqu'un événement spécifique se produit.
       a. Indiquez la date et l'heure auxquels vous souhaitez que ce travail s'exécute, puis cliquez sur **Suivant**.
       b. Sélectionnez les appareils gérés sur lesquels le travail doit s'exécuter, puis cliquez sur **Suivant**.
       c. Sélectionnez l'événement qui doit déclencher le travail.
  5. Cliquez sur **Créer**.

Après avoir terminé

L'onglet Travaux planifiés s'affiche avec une liste de toutes les planifications de travail dans XClarity Administrator.



Depuis cette page, vous pouvez effectuer les actions suivantes :

- Pour afficher des informations sur tous les travaux actifs et terminés pour une planification de travail spécifique, cliquez sur le lien dans la colonne **Travail**.
  - Pour affiner la liste des planifications de travail affichées par une type de planification spécifique, cliquez sur **Types de planning** et choisissez l'une des options suivantes :
    - **Tous les types de planning**
    - **Unique**
    - **Récurrent**
    - **Déclenché**
  - Pour masquer ou afficher uniquement les planifications de travail qui sont dans un état spécifique, cliquez sur les icônes suivantes :
    - Toutes les travaux planifiés qui sont actifs en cliquant sur l'icône **Actif** ( ).
    - Toutes les travaux planifiés qui ne sont pas actifs en cliquant sur l'icône **Suspendu** ( ).
    - Toutes les travaux planifiés déjà exécutés et qui ne sont pas planifiés pour une autre exécution en cliquant sur l'icône **Arrêté** ( ).
  - Pour afficher uniquement la liste des travaux qui contiennent un texte spécifique, entrez ce texte dans la zone **Filtre**.
  - Pour triez les travaux planifiés par colonne, cliquez sur un en-tête de colonne.

- Pour savoir quand le travail a été exécuté pour la dernière fois, consultez la colonne **Dernière exécution**. Pour afficher l'état de la dernière exécution du travail, cliquez sur le lien « État des travaux » dans cette colonne.
- Pour afficher la prochaine planification d'exécution du travail, consultez la colonne **Prochaine exécution**. Pour afficher une liste de toutes les dates et heures futures, cliquez sur le lien « Plus » dans la colonne.
- Pour exécuter immédiatement le travail qui est associé à la planification, cliquez sur l'icône **Exécuter** ().
- Pour activer ou désactiver une planification, cliquez sur l'icône **Suspendre** () ou **Activer** () respectivement.
- Pour copier et modifier une planification, cliquez sur l'icône **Copier** ().
- Pour éditer une planification, cliquez sur l'icône **Éditer** ().
- Pour supprimez une ou plusieurs planifications de travail, cliquez sur l'icône **Supprimer** ().
- Exportez des informations sur des planifications de travail spécifiques en sélectionnant les planifications et en cliquant sur l'icône **Exporter au format CSV** ().
- Pour actualiser la liste des planifications de travail, cliquez sur l'icône **Toutes les actions → Actualiser**.

Ajouter une résolution et des commentaires à un travail

Vous pouvez ajouter une résolution et des commentaires à un travail finalisé, quel que soit l'état de réussite ou d'erreur. Vous pouvez effectuer cela pour un travail parent et pour les sous-tâches du travail.

Procédure

Effectuez l'une des étapes suivantes pour ajouter une résolution et des commentaires à un travail.

Etape 1. Dans la barre de titre de Lenovo XClarity Administrator, cliquez sur **Surveiller → Travaux**, puis cliquez sur l'onglet **État des travaux** pour afficher la page État des travaux.

Etape 2. Cliquez sur le lien correspondant au travail dans la colonne **Travail** pour afficher les détails du travail.

Etape 3. Cliquez sur l'icône **Notes** () pour afficher la boîte de dialogue Notes.

Depuis cette boîte de dialogue, vous pouvez voir un historique de toutes les notes et résolutions qui ont été ajoutées au travail. Vous pouvez effacer cet historique en cliquant sur **Effacer tous les dossiers**.

Etape 4. Choisissez l'une des résolutions suivantes.
- **Aucune modification**
- **Analyse en cours**
- **Résolu**
- **Annulé**

Etape 5. Ajoutez une remarque dans la zone **Note**.

Etape 6. Cliquez sur **Appliquer**.

Sur la page État des travaux, la résolution s'affiche dans la colonne **État** de ce travail.

Affichage des relations entre les travaux et les événements

Un *organigramme* est une vue graphique qui présente les relations entre les activités (y compris les travaux et les événements) qui sont lancées manuellement par un utilisateur ou lancées automatiquement par Lenovo XClarity Administrator. L'organigramme permet d'identifier les problèmes en illustrant la séquence des actions qui ont été lancées et des événements qui ont été générés, et ce qui les a générés.

Avant de commencer

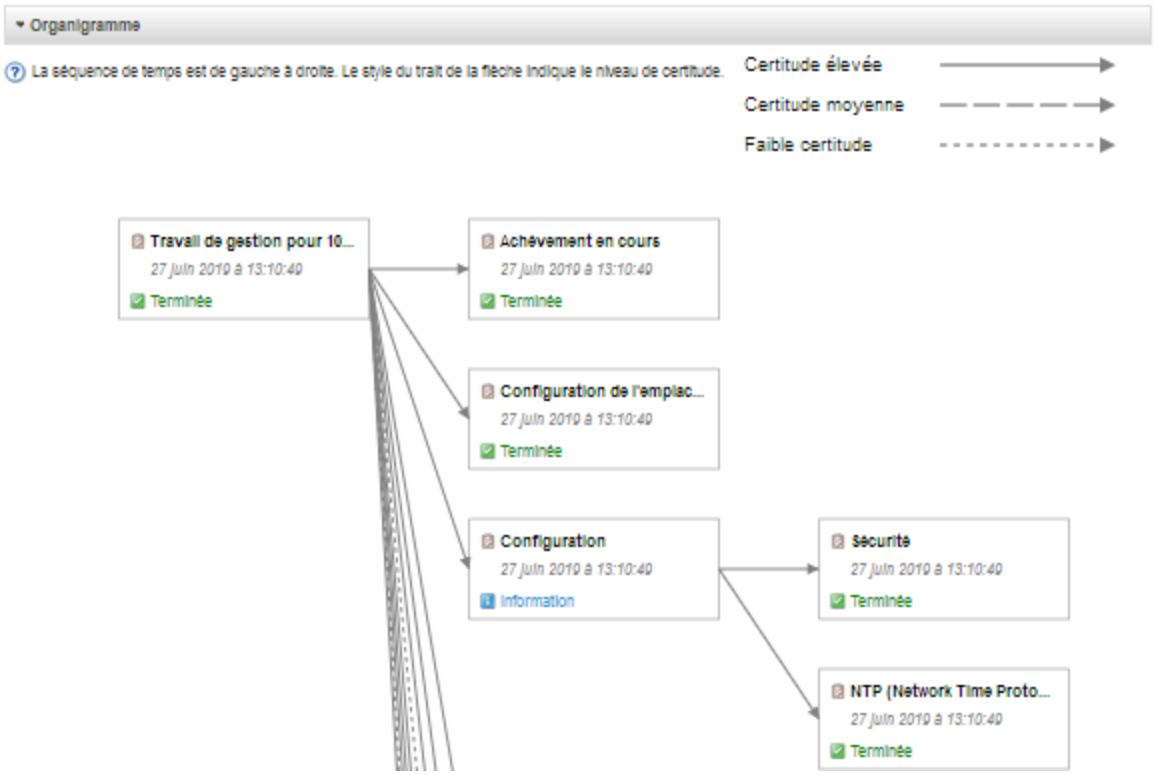
Les flux d'activités sont désactivés par défaut. Vous devez activer les flux d'activités avant que des flux ne puissent être générés pour une activité. Vous ne pouvez afficher les flux que pour les activités qui se produisent lorsque le flux d'activités est activé.

Attention : Les flux d'activités augmentent l'utilisation de la mémoire par XClarity Administrator. Il est recommandé de ne pas activer les flux d'activités si l'utilisation de la mémoire par XClarity Administrator est déjà élevée.

À propos de cette tâche

L'exemple suivant illustre un organigramme. La séquence d'événements va de gauche à droite. Chaque nœud du flux représente une activité unique et inclut la description de l'activité, la date et l'état. Vous pouvez passer le curseur sur le titre du nœud pour afficher des informations supplémentaires sur l'activité.

Le style des lignes entre les nœuds indique la certitude de relation entre les nœuds.
- Les lignes pleines représentent une certitude élevée.
- Les lignes en pointillés longs représentent une certitude moyenne.
- Les lignes en pointillés courts représentent une certitude faible.



Procédure

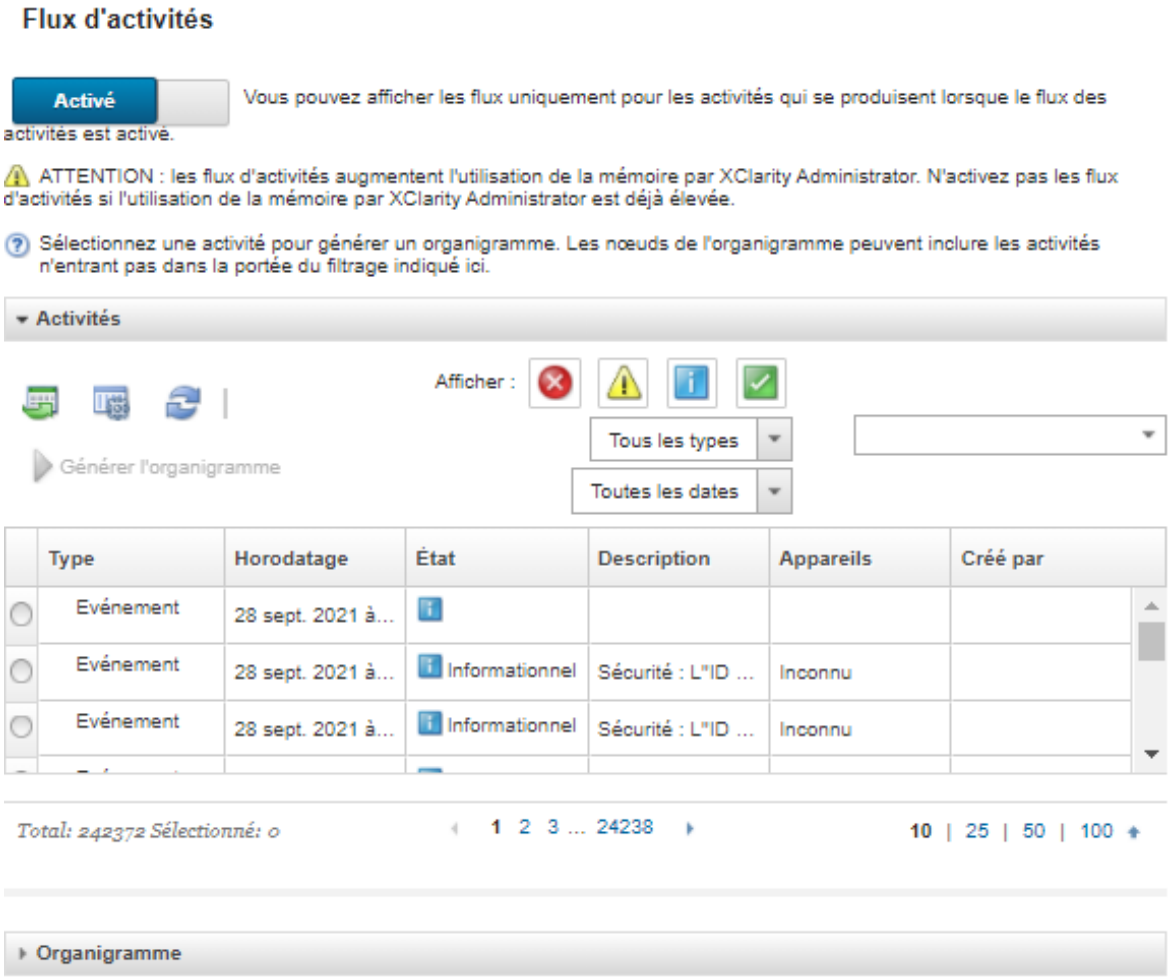
Procédez comme suit pour afficher l'organigramme d'une activité spécifique.

Etape 1. Dans la barre de menus XClarity Administrator, cliquez sur **Surveillance → Flux d'activités** pour afficher la page Flux d'activités

Etape 2. Activez les flux d'activités en sélectionnant **Activer le flux des activités**.

Etape 3. Dans la section **Activités**, sélectionnez le travail ou l'événement.

Vous pouvez trier les colonnes du tableau afin de faciliter la recherche d'activités spécifiques. En outre, vous pouvez sélectionner un type d'état, un type d'activités, entrer un filtre personnalisé ou entrer du texte (par exemple, un nom ou une adresse IP) dans la zone **Filtre**, puis afficher uniquement la liste des activités qui répondent aux critères sélectionnés.



Etape 4. Cliquez sur **Générer un organigramme** pour afficher l'organigramme dans la section **Organigramme**

Après avoir terminé

Depuis cette page, vous pouvez effectuer les actions suivantes :

- Afficher des informations supplémentaires sur chaque activité dans l'organigramme en plaçant le curseur sur l'activité.
- Exporter le flux associé pour les activités sélectionnées dans un fichier CSV en cliquant sur **Actions → Exporter au format CSV**.

Chapitre 4. Considérations relatives à la gestion

Plusieurs solutions sont proposées en matière de gestion d'appareils. Selon les appareils gérés, il se peut que plusieurs solutions de gestion doivent s'exécuter en même temps.

Un appareil ne peut être géré que par une seule instance de Lenovo XClarity Administrator. Toutefois, vous pouvez utiliser d'autres logiciels de gestion (par exemple, VMware vRealize Operations Manager) parallèlement à Lenovo XClarity Administrator pour *surveiller* les appareils gérés par XClarity Administrator.

Attention : Des mesures additionnelles doivent être prises si vous utilisez plusieurs outils de gestion pour gérer vos appareils afin d'éviter des conflits inattendus. Par exemple, la soumissions de modifications d'état d'alimentation à l'aide d'un autre outil peut être en conflit avec des travaux de configuration ou de mise à jour en cours d'exécution dans XClarity Administrator.

Appareils ThinkSystem, ThinkServer et System x

Si vous prévoyez d'utiliser un autre logiciel de gestion pour surveiller vos appareils gérés, créez un nouvel utilisateur local à l'aide des paramètres SNMP ou IPMI corrects de l'interface IMM. Assurez-vous d'accorder des privilèges SNMP ou IPMI, selon vos besoins.

Appareils Flex System

Si vous prévoyez d'utiliser un autre logiciel de gestion pour surveiller vos appareils gérés et si ce logiciel de gestion utilise une communication SNMPv3 ou IPMI, vous devez préparer votre environnement en effectuant les étapes suivantes pour chaque module CMM géré :

1. Connectez-vous à l'interface Web du contrôleur de gestion pour le châssis en utilisant le nom d'utilisateur et le mot de passe `RECOVERY_ID`.
2. Si la valeur **Sécurisé** est affectée à la stratégie de sécurité, modifiez la méthode d'authentification utilisateur.
   a. Cliquez sur **Gestion du module de gestion → Comptes utilisateur**.
   b. Cliquez sur l'onglet **Comptes**.
   c. Cliquez sur **Paramètres de connexion globaux**.
   d. Cliquez sur l'onglet **General**.
   e. Sélectionnez **Authentification externe, puis locale** pour la méthode d'authentification utilisateur.
   f. Cliquez sur **OK**.
3. Créez un utilisateur local avec les paramètres SNMP ou IPMI appropriés à partir de l'interface Web du contrôleur de gestion.
4. Si la valeur **Sécurisé** est affectée à la stratégie de sécurité, déconnectez-vous, puis connectez-vous à l'interface Web du contrôleur de gestion à l'aide du nouveau nom d'utilisateur et du nouveau mot de passe. Lorsque vous y êtes invité, modifiez le mot de passe pour le nouvel utilisateur.

Vous pouvez à présent utiliser le nouvel utilisateur comme utilisateur SNMP ou IPMI actif.

Remarque : Si vous annulez, puis reprenez la gestion du châssis, ce nouveau compte utilisateur est verrouillé et désactivé. Dans ce cas, répétez ces étapes pour créer un nouveau compte utilisateur.

Chapitre 5. Gestion des groupes de ressources

Vous pouvez utiliser un groupe de ressources dans Lenovo XClarity Administrator pour créer un ensemble logique d'appareils gérés que vous pouvez ensuite afficher et manipuler de manière collective.

En savoir plus : XClarity Administrator : Groupes de ressources

À propos de cette tâche

Il existe trois types de groupes de ressources.

- **Static**. Groupe personnalisé d'appareils spécifiques.
- **Dynamique**. Groupe d'appareils basé sur des règles (par exemple, tous les serveurs d'un type spécifique). Ce groupe contient une liste dynamique d'appareils basée sur un ensemble de propriétés d'inventaire.

Il n'est pas possible d'effectuer des actions sur un groupe de ressources. Toutefois, vous pouvez sélectionner tous les appareils du groupe et exécuter des actions de manière collective sur tous les appareils sélectionnés.

Affichage de l'état des appareils présents dans un groupe de ressources

Vous pouvez afficher l'état de tous les appareils gérés présents dans un groupe de ressources.

À propos de cette tâche

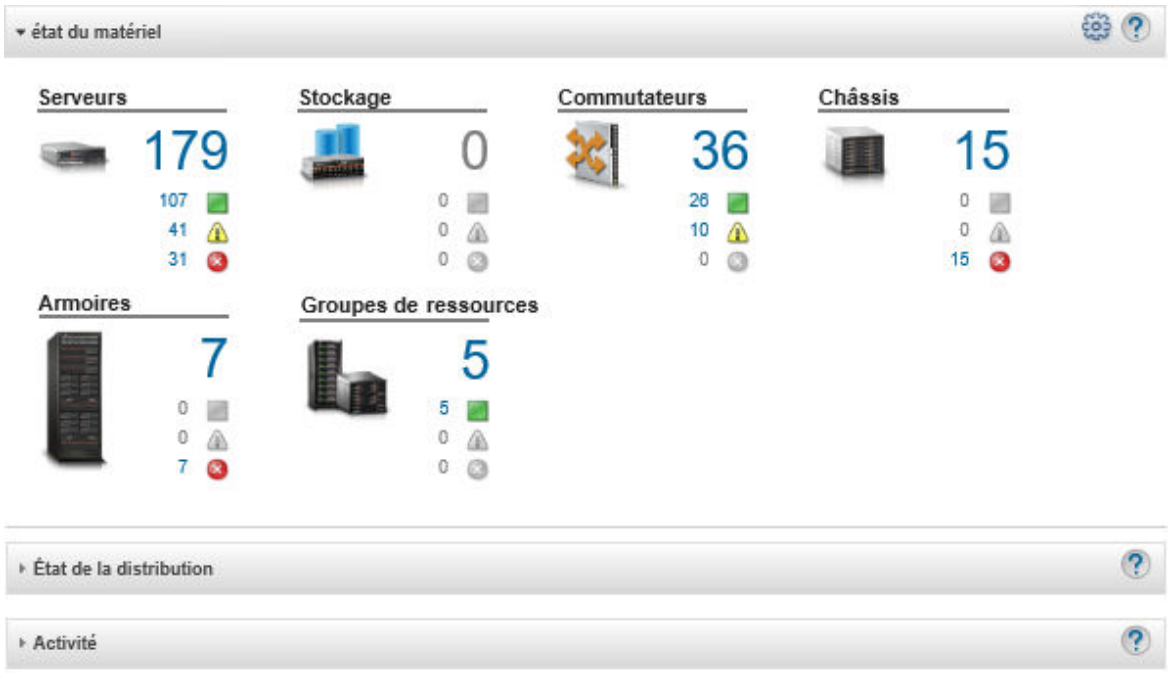
Les icônes d'état suivantes sont utilisées pour indiquer l'intégrité générale de tous les appareils figurant dans un groupe de ressources. L'intégrité générale du groupe indique l'appareil présentant le niveau de gravité le plus élevé dans le groupe.

- Icône **Critique** ( )
- Icône **Avertissement** ( )
- Icône **Normal** ( )

Procédure

Pour afficher l'état des appareils présents dans un groupe de ressources, procédez comme suit.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Tableau de bord**. La page Tableau de bord s'affiche, avec une présentation et l'état de tous les appareils gérés et des autres ressources, notamment des groupes de ressources.



Etape 2. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Groupes de ressources**. La page Tous les groupes de ressources s'affiche.

La page Tous les groupes de ressources affiche chaque groupe de ressources, y compris le nom du groupe, le nombre d'appareils gérés présents dans celui-ci et l'état de l'appareil présentant le niveau de gravité le plus élevé dans le groupe.

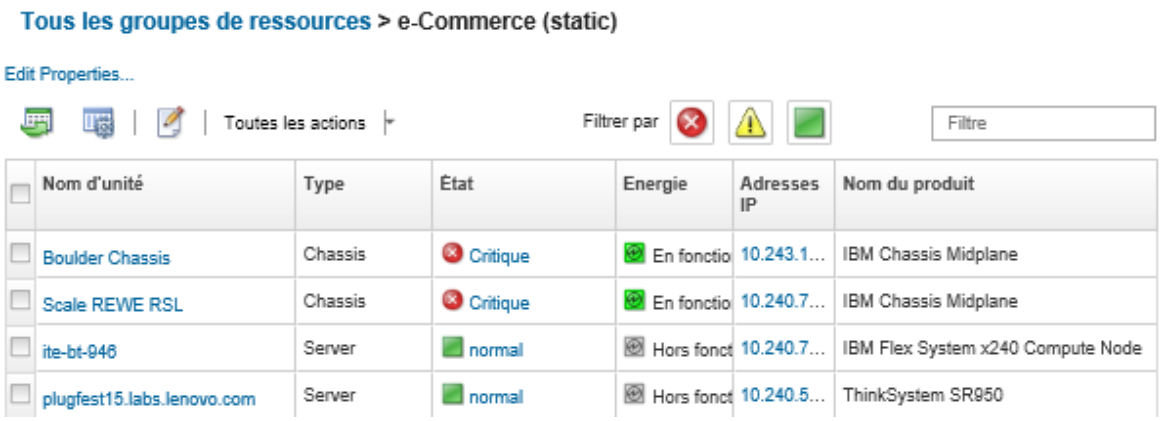
Depuis cette page, vous pouvez effectuer les actions suivantes :

- Créez un groupe de ressources (voir Création d'un groupe de ressources dynamique et Création d'un groupe de ressources statique)
- Modifier l'appartenance à un groupe en sélectionnant un groupe, puis en cliquant sur l'icône **Éditer** ( ).
- Modifier les propriétés du groupe en sélectionnant le groupe, puis en cliquant sur **Toutes les actions → Éditer les propriétés**.
- Retirez un groupe de ressources en sélectionnant un groupe et en cliquant sur l'icône **Supprimer** ( ).

Remarque : Le retrait d'un groupe retire uniquement la définition de groupe. Il n'a pas d'incidence sur les appareils du groupe.

- Exporter des informations détaillées sur tous les appareils figurant dans un ou plusieurs groupes de ressources vers un fichier CSV en cliquant sur l'icône **Exporter** ( ).

Etape 3. Depuis la page Tous les groupes de ressources, cliquez sur le nom dans la colonne **Groupes** pour afficher la liste des appareils de ce groupe.



Depuis cette page, vous pouvez effectuer les actions suivantes :

- Ajouter ou retirer des appareils dans un groupe de ressources statique en cliquant sur l'icône **Éditer** ( ).
- Afficher des informations détaillées sur un appareil spécifique figurant dans le groupe de ressources en cliquant sur son nom dans la colonne **Nom de l'appareil**.
- Exporter des informations détaillées sur tous les appareils figurant dans un ou plusieurs groupes de ressources vers un fichier CSV en cliquant sur l'icône **Exporter** ( ).

Affichage des membres d'un groupe de ressources

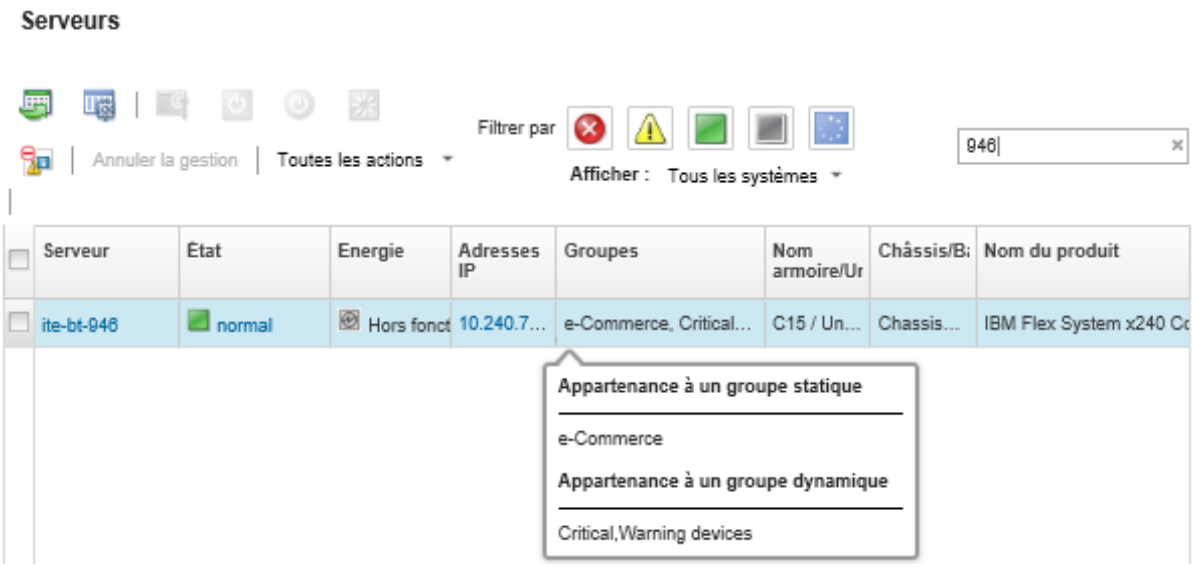
Vous pouvez afficher des informations détaillées sur les groupes de ressources y compris les membres du groupe.

Procédure

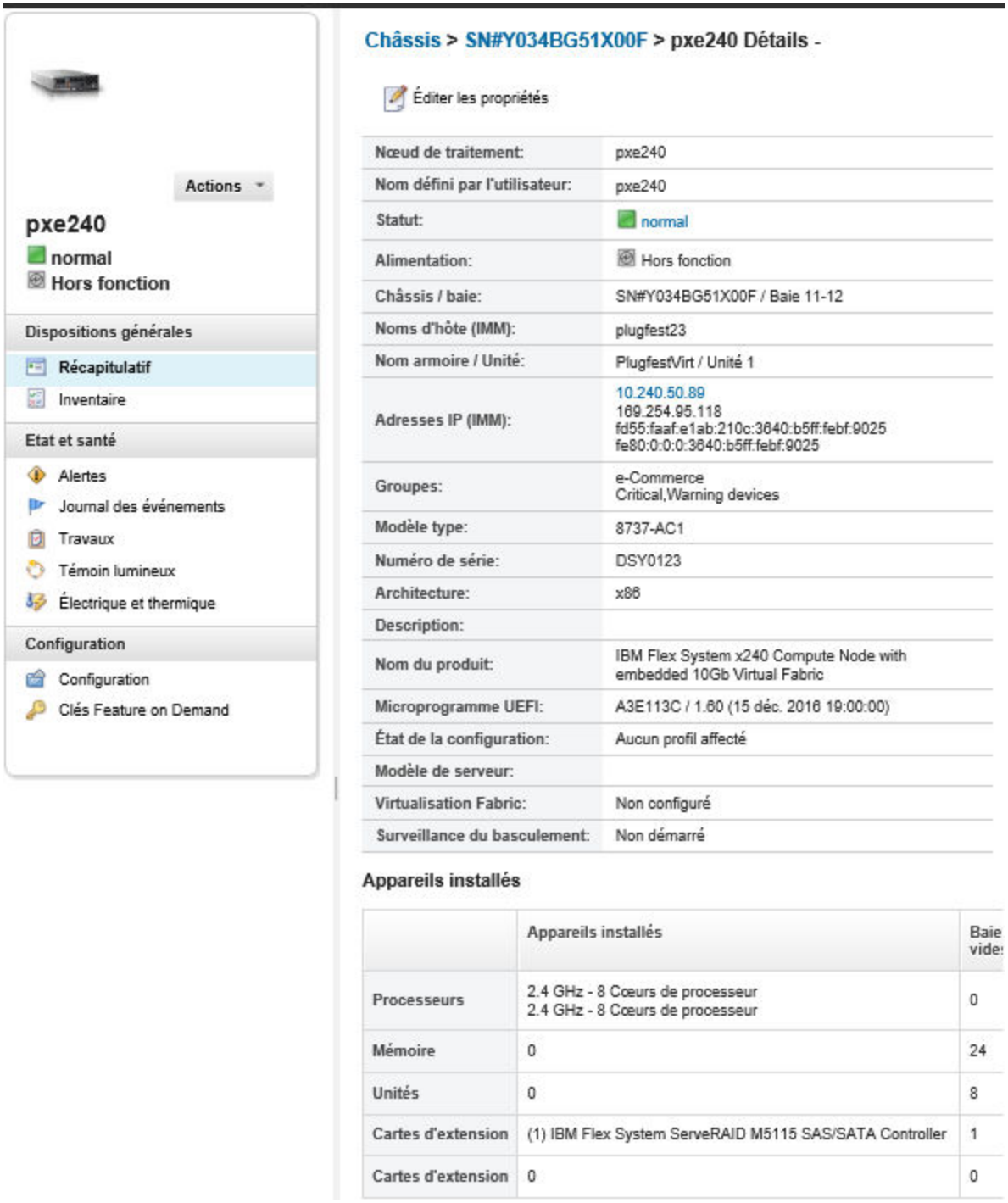
Pour afficher l'appartenance à un groupe, procédez comme suit.

- Pour afficher tous les groupes dont un appareil est membre.
  1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Matériel**, puis cliquez sur le type de dispositif pour afficher la page de tous les dispositifs.

     Survolez les listes de groupes dans la colonne **Groupes** pour afficher la liste des groupes dont l'appareil est membre.



2. Cliquez sur le lien du nom d'appareil dans la première colonne. La page de récapitulatif de cet appareil s'affiche, avec notamment la liste des groupes de ressources dont est membre l'appareil.

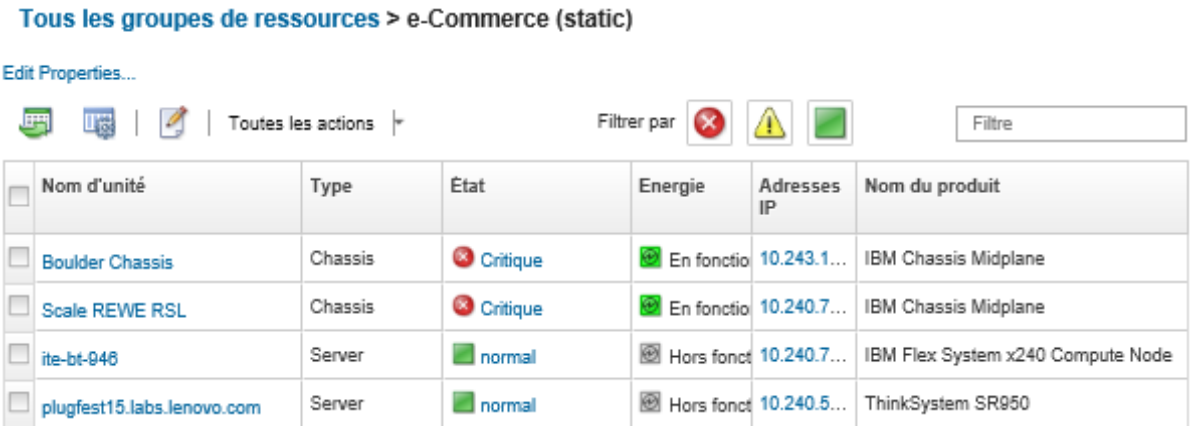


- Pour afficher les membres d'un groupe.
  1. Dans la barre de menus de XClarity Administrator, cliquez sur **Tableau de bord**. La page Tableau de bord affiche la présentation et l'état de tous les appareils gérés et d'autres ressources, compris les armoires.
  2. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Groupes**. La page Groupes de ressources s'affiche.

     Cette page affiche le nombre total de membres et le nombre de membres de chaque type de dispositif dans le groupe.

3. Depuis la page Tous les groupes de ressources, cliquez sur le nom dans la colonne **Groupes** pour afficher les détails du groupe de ressources.

   Cette page affiche chaque appareil qui est membre du groupe de ressources.



Création d'un groupe de ressources dynamique

Vous pouvez créer un groupe de ressources pour un ensemble dynamique d'appareils gérés à partir d'un ensemble de critères.

À propos de cette tâche

Vous pouvez créer un groupe de ressources dynamique à l'aide d'un ou de plusieurs des critères de chaque type de dispositif.

Critères	Châssis	Châssis dense	Serveurs	Commu-tateur Flex System	commu-tateur RackS-witch	Dispositif de stockage
Nom de carte d'extension			✓ (sauf ThinkSer-ver)			
Contactez	✓		✓		✓	✓
Description	✓	✓	✓		✓	✓

Critères	Châssis	Châssis dense	Serveurs	Commu-tateur Flex System	commu-tateur RackS-witch	Dispositif de stockage
Nom de domaine complet	✓		✓			
Nom d'hôte	✓		✓	✓	✓	
Adresse IPv4*	✓		✓	✓	✓	✓
Adresse IPv6	✓		✓	✓	✓	
Emplacement	✓	✓	✓		✓	✓
Type de machine	✓		✓	✓	✓	✓
Modèle	✓		✓	✓	✓	✓
État d'intégrité général	✓		✓	✓	✓	✓
Cœurs de processeur			✓			
Nom du produit	✓		✓	✓	✓	✓
Armoire	✓	✓	✓		✓	✓
Pièce	✓	✓	✓		✓	✓
Nom défini par l'utilisateur	✓	✓	✓	✓	✓	✓

Remarque : Pour les adresses IPv4, vous pouvez spécifier une seule adresse ou une plage d'adresses, séparées par un tiret ou en utilisant un astérisque comme caractère générique (par exemple, `1.1.1.*` ou `1.1.1.1-1.1.1.255` sans espace).

Procédure

Pour créer et remplir un groupe de ressources dynamique, procédez comme suit.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Matériel → Groupes de ressources**. La page Tous les groupes de ressources s'affiche.

Etape 2. Cliquez sur l'icône **Créer** ( ) pour créer un groupe vide. La boîte de dialogue Créer un groupe vide s'affiche.

Etape 3. Sélectionnez **Groupe dynamique** pour regrouper les appareils sur la base d'un jeu de critères.

Etape 4. Cliquez sur **Créer**. La boîte de dialogue Modification du groupe dynamique s'affiche.

Etape 5. Ajoutez les critères de ce groupe dynamique.

- Sélectionnez l'opérateur à utiliser pour le groupe défini. Les valeurs possibles sont les suivantes :
  - **AND**. Les membres doivent satisfaire toutes les valeurs spécifiés.
  - **OR**. Les membres doivent satisfaire une ou plusieurs des valeurs spécifiées.
- Cliquez sur **Créer un critère** pour ajouter un nouveau critère à l'ensemble.
- Cliquez sur **Créer un ensemble de critères** pour ajouter un sous-ensemble de critères.

Remarque : Les nouveaux critères et ensembles de critères sont toujours ajoutés en fin de liste.

Etape 6. Cliquez sur **Appliquer** pour enregistrer les critères de groupe et créer le groupe, ou cliquez sur **Aperçu** pour afficher les appareils inclus dans le groupe en utilisant les critères actuels sans créer le groupe.

Après avoir terminé

- Vous pouvez voir les groupes de ressources auxquels appartient un appareil dans la colonne **Groupes** des pages de tous les appareils et des pages de récapitulatif des appareils.
- Vous pouvez modifier les critères du groupe dynamique en sélectionnant le groupe de ressources et en cliquant sur l'icône **Éditer** ( ).
- Vous pouvez modifier les propriétés du groupe de ressources en cliquant sur **Toutes les actions → Éditer les propriétés**.

Création d'un groupe de ressources statique

Vous pouvez créer un groupe de ressources contenant un ensemble personnalisé d'appareils gérés.

Procédure

Pour créer et remplir un groupe de ressources statique, procédez comme suit.

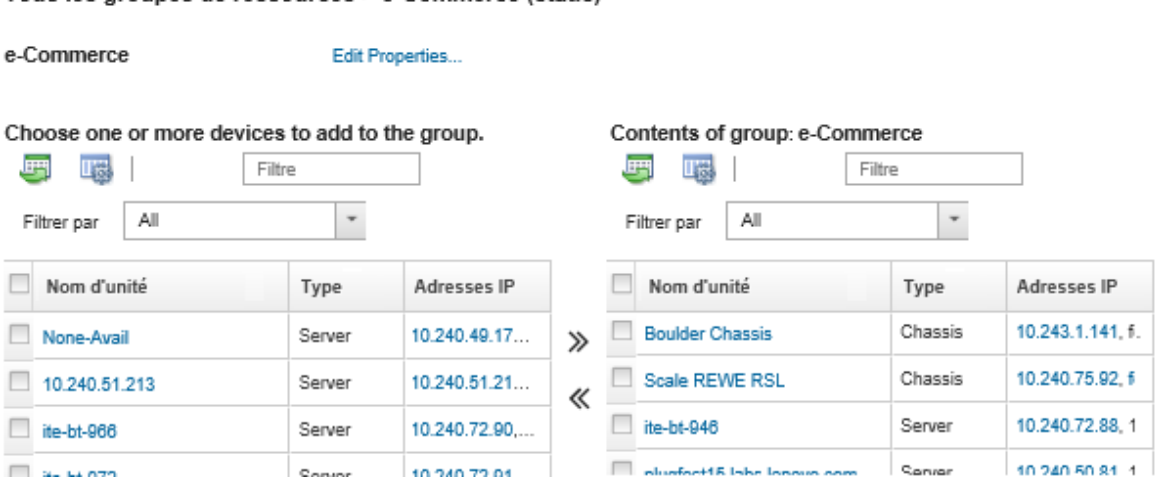
Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Matériel → Groupes de ressources**. La page Groupes de ressources s'affiche.

Etape 2. Cliquez sur l'icône **Créer** ( ) pour créer un groupe vide. La boîte de dialogue Créer un groupe vide s'affiche.

Etape 3. Indiquez le nom de groupe et une description facultative.

Etape 4. Sélectionnez **Groupe statique** pour créer un groupe d'appareils définis de manière explicite.

Etape 5. Cliquez sur **Créer**. La page Modification du groupe statique s'affiche.



Etape 6. Sélectionnez les appareils que vous souhaitez ajouter au groupe dans la liste **Tous les appareils disponibles absents du groupe**, puis cliquez sur l'icône **Ajouter** (≫) pour déplacer les appareils sélectionnés vers la liste **Contenu du groupe**.

Remarques :

- Vous pouvez trier les listes afin de faciliter la recherche d'appareils spécifiques en cliquant sur les en-têtes de colonne. En outre, vous pouvez sélectionner un type d'appareil dans la liste déroulante **Filtrer par**, sélectionner un châssis ou saisir un texte (par exemple, un nom ou une adresse IP) dans la zone **Filtre**, pour afficher uniquement les appareils qui répondent aux critères sélectionnés
- Si vous choisissez de déplacer un châssis dans le groupe, les appareils dans le châssis ne sont pas automatiquement ajoutés au groupe. Pour ajouter tous les composants du châssis au groupe, sélectionnez **Châssis → <*nom_châssis*>** dans le menu déroulant **Afficher** pour afficher tous les composants du châssis spécifié, sélectionnez la case en regard de la colonne Nom de l'appareil pour sélectionner tous les appareils, puis cliquez sur l'icône **ajouter** (≫) afin de déplacer les appareils sélectionnés vers la liste **Contenu du groupe**.

Après avoir terminé

- Vous pouvez voir les groupes de ressources auxquels appartient un appareil dans la colonne **Groupes** des pages de tous les appareils et des pages de récapitulatif des appareils.
- Vous pouvez ajouter ou retirer un appareil d'un groupe de ressources statique dans les pages de tous les dispositifs et les pages de détails des appareils en cliquant sur **Toutes les actions → Groupes → Ajouter au groupe** ou **Toutes les actions → Groupes → Retirer du groupe**.

  Remarque : Vous pouvez ajouter et retirer des appareils uniquement des groupes de ressources statiques. Vous ne pouvez pas les retirer des groupes dynamiques.
- Vous pouvez modifier les propriétés du groupe de ressources en cliquant sur **Toutes les actions → Éditer les propriétés**.

Retrait d'un groupe de ressources

Vous pouvez retirer un groupe de ressources de Lenovo XClarity Administrator.

À propos de cette tâche

La suppression d'un groupe supprime uniquement la définition de groupe. Elle n'a pas d'incidence sur les appareils de ce groupe.

Procédure

Pour retirer un groupe de ressources, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Groupes de ressources**. La page Tous les groupes de ressources s'affiche.

La page Tous les groupes de ressources affiche chaque groupe de ressources, y compris le nom du groupe, le nombre d'appareils gérés présents dans celui-ci et l'état de l'appareil présentant le niveau de gravité le plus élevé dans le groupe.

Etape 2. Sélectionnez le groupe de ressources à retirer.

Etape 3. Cliquez sur l'icône **Supprimer** ( ).

Etape 4. Cliquez sur **Supprimer**.

Modification des propriétés d'un groupe de ressources

Vous pouvez modifier les propriétés d'un groupe de ressources spécifique.

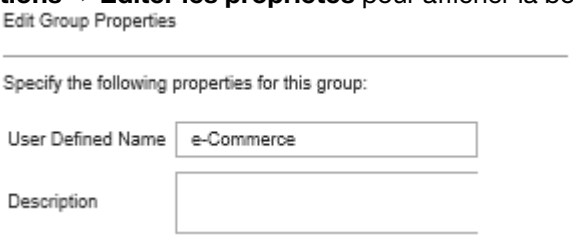
Procédure

Pour modifier les propriétés du groupe de ressources, procédez comme suit

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Groupes de ressources** pour afficher la page Tous les groupes de ressources.

Etape 2. Sélectionnez le groupe de ressources à mettre à jour.

Etape 3. Cliquez sur **Toutes les actions → Éditer les propriétés** pour afficher la boîte de dialogue Édition



des propriétés du groupe.

Etape 4. Modifiez les informations suivantes, si nécessaire.
- Nom de groupe
- Description

Etape 5. Cliquez sur **Enregistrer**.

Remarque : Si vous modifiez ces propriétés, vous devrez peut-être attendre quelques instants avant que les modifications n'apparaissent dans l'interface Web XClarity Administrator

Chapitre 6. Gestion des armoires

Vous pouvez utiliser des armoires dans Lenovo XClarity Administrator pour regrouper vos appareils gérés dans le but de refléter la configuration de l'armoire physique dans votre centre de données.

Avant de commencer

Après avoir déplacé un nœud d'un châssis vers un autre, attendez 5 à 10 minutes avant d'essayer de modifier les armoires dans XClarity Administrator qui contient le châssis.

Lorsque vous déplacez un appareil en dehors d'une armoire, le nom de l'armoire et les valeurs d'unité d'armoire les plus faibles sont désactivées dans l'inventaire. Les valeurs de pièce et d'emplacement ne sont pas désactivées.

À propos de cette tâche

Cette procédure explique comment créer et remplir une armoire avec des appareils gérés et des obturateurs en mode interactif.

Si vous devez ajouter un grand nombre d'appareils dans des armoires ou éditer un grand nombre d'armoires, envisagez d'utiliser un tableau pour effectuer une importation en masse ou d'implémenter un script PowerShell pour automatiser la tâche. Pour plus d'informations sur l'utilisation de l'importation en masse, voir Gestion des châssis et Gestion des serveurs. Pour plus d'informations sur les scripts PowerShell, voir Kit d'outils PowerShell (LXCAPSTool) dans la documentation en ligne de XClarity Administrator.

XClarity Administrator reconnaît les propriétés d'armoire qui sont définies dans un appareil gérable. Lorsque vous gérez cet appareil, XClarity Administrator définit les propriétés système correspondant à cet appareil et met à jour la vue Armoire. Si l'armoire n'existe pas dans XClarity Administrator, une nouvelle armoire est créée et l'appareil est ajouté à la nouvelle armoire.

Remarques :

- Les serveurs System x3500 M5, NeXtScale nx360 M5 et ThinkServer SD350, ainsi que les serveurs au format tour ne sont pas pris en charge dans la vue Armoire.
- Pour les systèmes évolutifs complexes System x3850 X5, vous devez ajouter chaque nœud (serveur) individuellement à l'armoire.
- Le matériel de démonstration n'est pas persistant dans les vues Armoire lorsque XClarity Administrator est redémarré.

Procédure

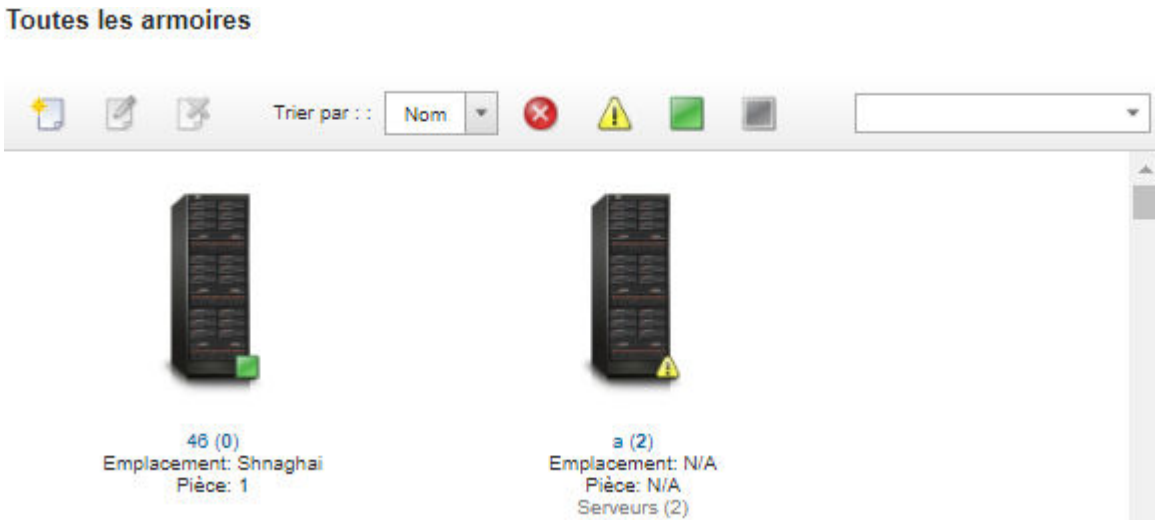
Pour créer et remplir des armoires, procédez comme suit.

- Créer et remplissez une armoire unique avec des appareils gérés.
  1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Armoires**. La page Toutes les armoires s'affiche.

     La page Toutes les armoires affiche chaque armoire sous la forme d'une image miniature avec le nom de l'armoire, le nombre d'appareils gérés présents dans celle-ci et l'état de l'appareil présentant le niveau de gravité le plus élevé.

Remarques : Vous pouvez filtrer les armoires par niveau de gravité en cliquant sur les icônes suivantes dans la barre d'outils. Vous pouvez également entrer un nom d'armoire dans la zone **Filtre** pour filtrer davantage l'affichage des armoires.

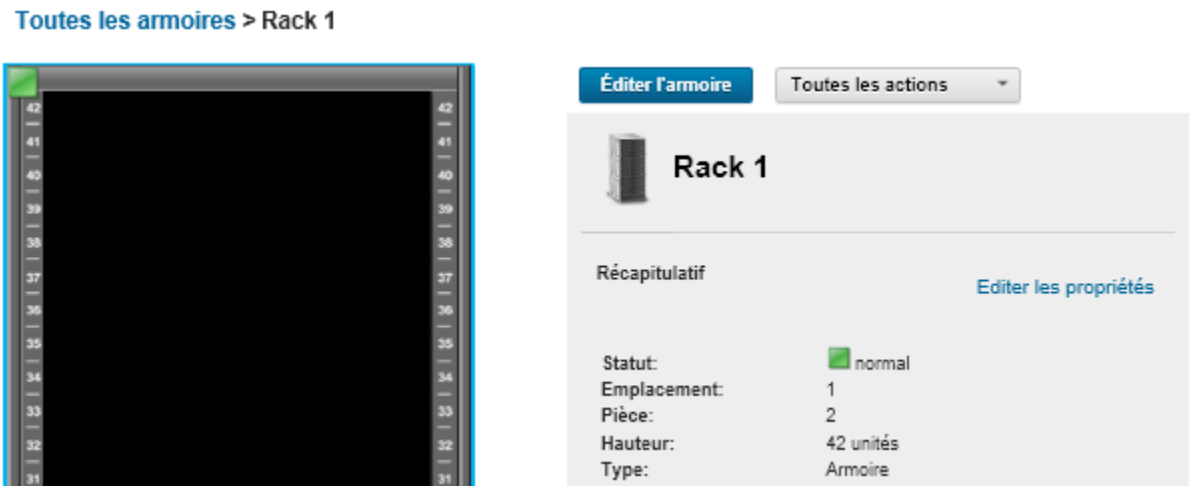
- L'icône **Alertes critiques** ( )
- L'icône **Alertes d'avertissements** ( )
- Icône **Alertes normales** ( )



2. Cliquez sur l'icône **Créer** ( ) pour créer une armoire vide. La boîte de dialogue Créer une armoire vide s'affiche.
3. Indiquez dans la boîte de dialogue le nom, la hauteur et l'emplacement de l'armoire, ainsi que la pièce dans laquelle elle se trouve.

   Remarques :

   - Les noms des armoires n'ont pas besoin d'être uniques. Tant que l'emplacement, la pièce ou les deux sont différents, vous pouvez créer des armoires dotées du même nom.
   - Le nom de l'armoire peut contenir uniquement des lettres majuscules et minuscules, des chiffres et les caractères spéciaux suivants : point (.), tiret (-) et trait de soulignement (_).
   - L'emplacement peut comporter 23 caractères au maximum.
4. Cliquez sur **Créer**. Une image miniature représentant la nouvelle armoire est ajoutée à la page Toutes les armoires.
5. Cliquez deux fois sur l'image miniature représentant l'armoire. La page de la vue Armoire s'affiche avec une image d'armoire vide et les propriétés relatives à cette armoire.



6. Cliquez sur **Éditer l'armoire** pour afficher la page Éditer l'armoire.

7. Ajoutez tous les appareils gérés et obturateurs appropriés à la vue graphique :

   Remarque : Seuls les appareils gérés à l'état En ligne peuvent être ajoutés à l'armoire.

   - Cliquez sur l'onglet **Châssis** pour afficher une liste de châssis gérés qui n'ont pas été ajoutés à une armoire. Faites glisser et déposez un châssis géré à l'emplacement souhaité dans l'armoire pour ajouter ce châssis à l'armoire.
   - Cliquez sur l'onglet **Boîtiers de serveur** pour afficher une liste de serveurs rack et de boîtiers de serveur multinœud gérés qui n'ont pas été ajoutés à une armoire. Faites glisser et déposez un serveur rack ou des boîtiers de serveur dans l'armoire à l'emplacement souhaité pour ajouter le serveur rack à l'armoire.
   - Cliquez sur l'onglet **RackSwitch** pour afficher une liste de commutateurs RackSwitch gérés qui n'ont pas été ajoutés à une armoire. Faites glisser et déposez un commutateur RackSwitch dans l'armoire à l'emplacement souhaité pour ajouter le commutateur à l'armoire.

- Cliquez sur l'onglet **Stockage** pour afficher une liste de différents dispositifs de stockage. Faites glisser et déposez le dispositif de stockage approprié dans l'armoire à l'emplacement souhaité pour ajouter le dispositif de stockage à l'armoire.
- Cliquez sur l'onglet **Obturateurs** pour afficher une liste de différents obturateurs. Faites glisser et déposez l'obturateur approprié dans l'armoire à l'emplacement souhaité pour ajouter l'obturateur à l'armoire.

  Un *obturateur* est n'importe quel appareil présent dans l'armoire qui n'est pas géré par XClarity Administrator. Les obturateurs suivants sont disponibles :
  - Obturateurs génériques
  - Commutateurs d'armoire génériques
  - Contrôleurs de stockage et boîtiers
  - Contrôleurs et boîtiers de stockage partenaires (par exemple, IBM, NetApp et EMC)

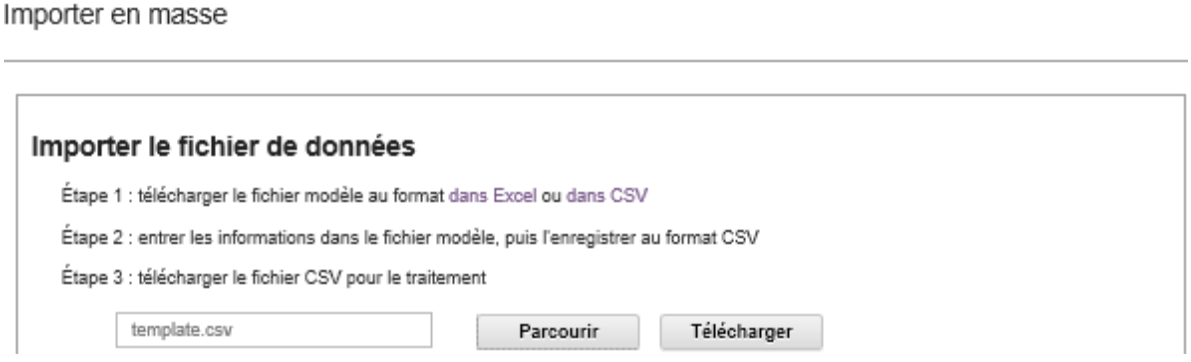
- L'emplacement, la pièce, l'armoire et les propriétés de l'unité d'armoire la plus basse sont mis à jour pour l'appareil lorsque vous ajoutez ou retirez des appareils dans une armoire.
- Vous pouvez trier la liste des appareils sur chaque onglet à l'aide de la liste déroulante **Afficher par**. En outre, vous pouvez saisir un texte (par exemple, un nom ou une adresse IP) dans la zone **Filtre** pour filtrer davantage l'affichage des appareils.
- Vous pouvez retirer des appareils gérés et des obturateurs de l'armoire en faisant glisser et en déposant les objets en dehors de l'armoire.

8. Cliquez sur **Enregistrer** pour enregistrer la configuration de l'armoire.

   La procédure de configuration peut durer quelques minutes. Lors de la configuration, les informations sur l'armoire et l'emplacement sont envoyées au module CMM ou au contrôleur de gestion de la carte mère pour les appareils gérés.
9. Personnalisez les obturateurs que vous avez ajoutés à l'armoire en cliquant sur ces obturateurs, puis en cliquant sur **Éditer les propriétés**. Dans la boîte de dialogue Éditer les propriétés, vous pouvez spécifier un nom, une unité d'armoire la plus basse et une URL permettant de lancer l'interface utilisateur de gestion pour cet appareil.

   Astuce : Une fois la configuration de l'armoire enregistrée, vous pouvez lancer l'interface utilisateur de gestion pour un obturateur de l'armoire en cliquant sur celui-ci, puis en cliquant sur le lien **URL de lancement**.

- Créez et remplissez les armoires à l'aide d'un fichier d'importation en masse.
  1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Reconnaître et gérer de nouveaux appareils**. La page Reconnaître et gérer s'affiche.
  2. Cliquez sur **Importer en masse**. L'assistant Importer en masse s'affiche.

  3. Cliquez sur le lien **dans Excel** ou **dans CSV** sur la page Importer le fichier de données pour télécharger le fichier d'importation en masse modèle au format Excel ou CSV.

Important : Le modèle de fichier peut varier d'une version à une autre. Assurez-vous de toujours utiliser le dernier modèle.

4. Remplissez la feuille de travail de données dans le modèle de fichier et enregistrez celui-ci au format CSV.

   Conseil : Le modèle de fichier Excel inclut une feuille de travail **Données** et une feuille de travail **Readme** . Utilisez la feuille de travail **Données** pour remplir les données de l'appareil. La feuille de travail **Readme** fournit des informations sur la manière de remplir chaque zone sur la feuille de travail **Données** (avec les zones obligatoires) et plusieurs exemples de données.

   Important :

   – Les appareils sont gérés dans l'ordre indiqué dans le fichier d'importation en masse.
   – XClarity Administrator utilise les informations affectation d'armoire qui sont définies dans la configuration de l'appareil lorsque celui-ci est géré. Si vous modifiez l'affectation d'armoire dans XClarity Administrator, XClarity Administrator met à jour la configuration de l'appareil. Si vous mettez à jour la configuration de l'appareil une fois l'appareil géré, les modifications sont répercutées dans XClarity Administrator.
   – Il est recommandé, mais non requis, de créer explicitement une armoire dans le tableur avant d'affecter l'armoire à un appareil. Si une armoire n'est pas explicitement définie et qu'elle n'existe pas dans XClarity Administrator, les informations d'affectation d'armoire spécifiées pour un appareil sont utilisées pour créer l'armoire avec la hauteur par défaut de de 52U.

     Si vous souhaitez utiliser un autre hauteur d'armoire, vous devez définir explicitement l'armoire dans le tableur avant de l'affecter à un appareil.

   Pour définir vos armoires dans le fichier d'importation en masse, complétez les colonnes requises suivantes.
   – (Colonnes A) Indiquez « armoire » comme type d'appareil.
   – (Colonnes V) Indiquez le nom de l'armoire.
   – (Colonne X) Indiquez la hauteur de l'armoire. Les hauteurs d'armoire suivantes sont prises en charge : 6U, 12U, 18U, 25U, 37U, 42U, 45U, 46U, 48U, 50U et 52U.

   La figure suivante illustre un exemple de fichier d'importation en masse avec des armoires définies.

A	V	W	X
Type	Rack name	Lowest rack unit	Height
rack	Rack_01		37
rack	Rack_02		52

   Remarque : Vous pouvez utiliser le même fichier d'importation en masse pour gérer des appareils et ajouter ces appareils à une armoire (voir Gestion des systèmes dans la documentation en ligne Lenovo XClarity Administrator).

5. Dans l'assistant Importer en masse, entrez le nom du fichier CSV pour télécharger le fichier à traiter. Vous pouvez cliquer sur **Parcourir** pour rechercher le fichier.
6. Cliquez sur **Télécharger** pour téléchargement et valider le fichier.
7. Cliquez sur **Suivant** pour afficher la page Récapitulatif des entrées avec une liste d'armoires et d'autres appareils à gérer, puis passez en revue le récapitulatif des armoires et des autres appareils que vous souhaitez gérer.

8. Cliquez sur **Suivant** pour afficher la page des données d'identification de l'appareil. Cliquez sur chaque onglet, et indiquez éventuellement des paramètres globaux et des données d'identification à utiliser pour tous les appareils d'un type spécifique. Les appareils qui utiliseront les paramètres globaux et les données d'identification sont répertoriés sur la partie droite de chaque onglet.
9. Cliquez sur **Gérer**. La page des résultats de surveillance s'affiche avec des informations sur l'état de gestion de chaque appareil dans le fichier d'importation en masse.

   Un travail est créé pour le processus de gestion. Si vous fermez l'assistant d'importation en masse, le processus de gestion continue de s'exécuter en arrière-plan. Vous pouvez surveiller l'état du processus de gestion en consultant le journal des travaux. Pour plus d'informations sur le journal des travaux, voir « Surveillance des travaux » à la page 181.

Après avoir terminé

Vous pouvez modifier la préférence d'ordre de numérotation des armoires (voir Définition des préférences d'inventaire).

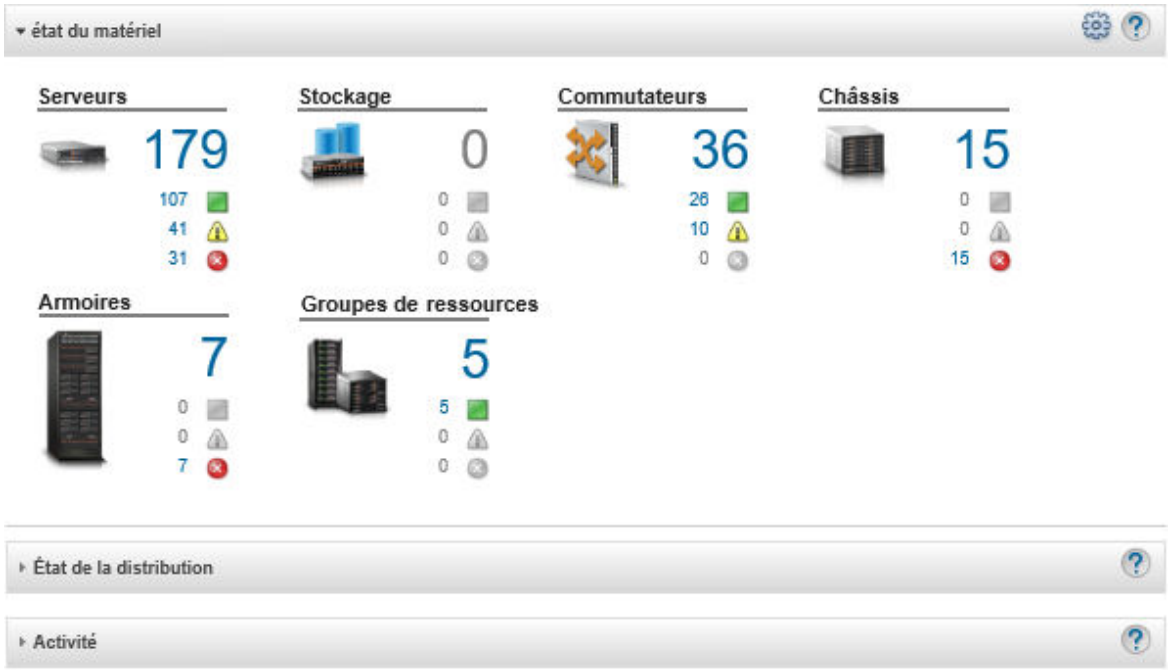
Affichage de l'état des appareils présents dans une armoire

Vous pouvez afficher l'état de tous les appareils gérés présents dans chaque armoire.

Procédure

Exécutez l'une ou plusieurs des actions suivantes pour afficher l'état de tous les appareils présents dans une armoire.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Tableau de bord**. La page Tableau de bord affiche la présentation et l'état de tous les appareils gérés et d'autres ressources, compris les armoires.

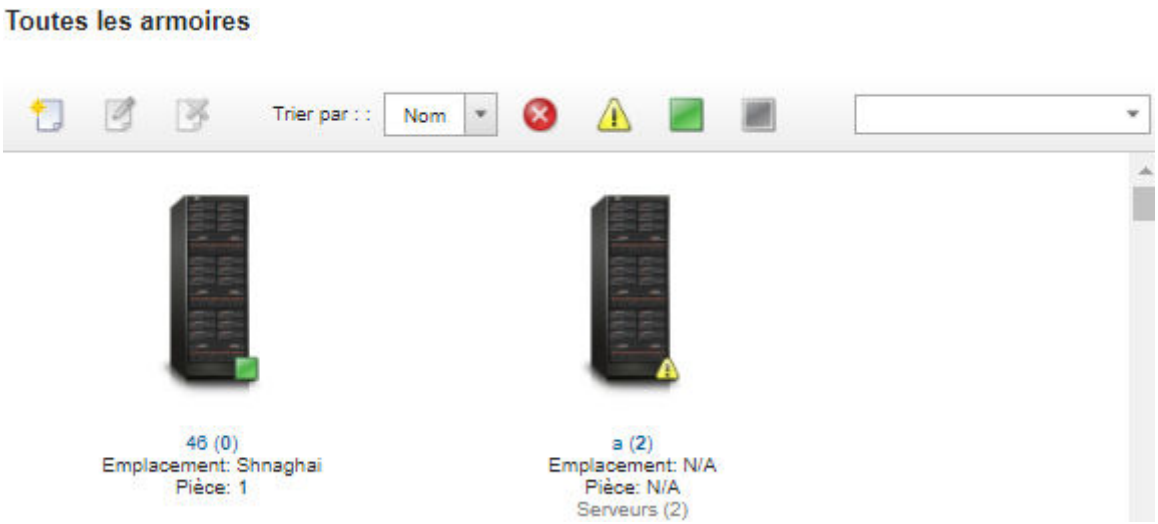


Etape 2. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Armoires**. La page Armoires s'affiche.

La page Armoires affiche chaque armoire sous la forme d'une image miniature avec le nom de l'armoire, le nombre d'appareils gérés présents dans celle-ci et l'état de l'appareil présentant le niveau de gravité le plus élevé.

Remarques : Vous pouvez trier la liste des armoires par nom d'armoire, nombre d'appareils dans l'armoire, ou par niveau de gravité pour simplifier la recherche d'armoires spécifiques. Le tri est effectué de la gauche vers la droite, du haut vers le bas. En outre, vous pouvez filtrer les armoires par niveau de gravité en cliquant sur les icônes suivantes dans la barre d'outils ou en entrant un nom d'armoire dans la zone **Filtre** pour filtrer davantage les armoires qui s'affichent.

- L'icône **Alertes critiques** ( )
- L'icône **Alertes d'avertissements** ( )
- Icône **Alertes normales** ( )



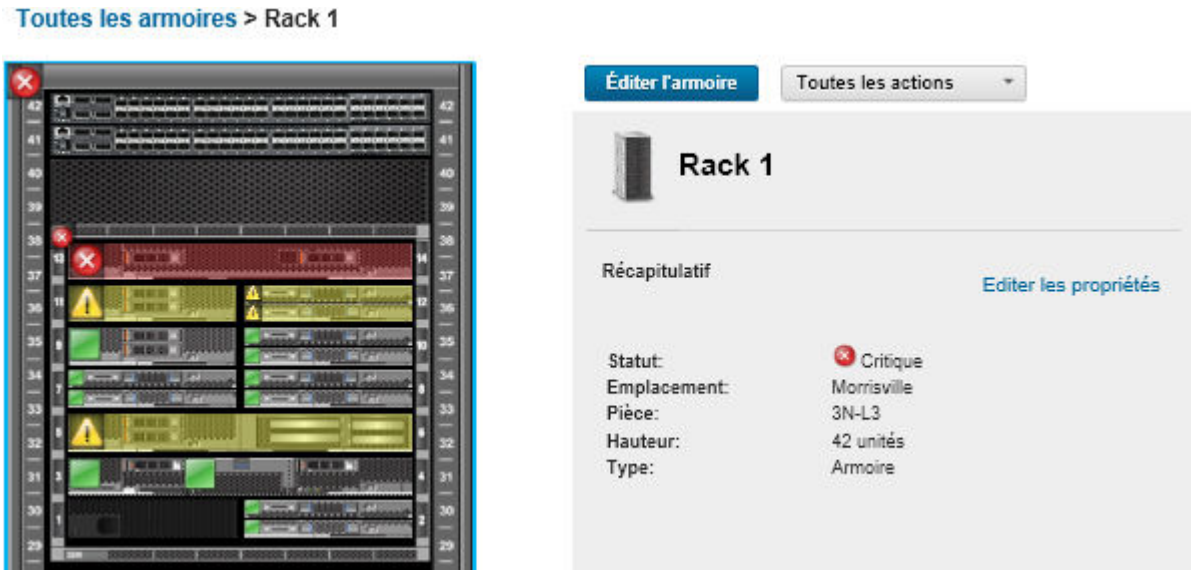
Etape 3. Sur la page Toutes les armoires, cliquez sur le nom de l'armoire ou cliquez deux fois sur une miniature d'armoire pour afficher la vue graphique et les propriétés de cette armoire.

La *vue Armoire* est une vue graphique de l'armoire avant qui affiche chaque appareil présent dans l'armoire, y compris le châssis, les serveurs rack, les commutateurs situés dans la partie supérieure de l'armoire et les obturateurs. Une icône d'état sur chaque appareil indique l'état en cours de cet appareil.

Depuis cette page, vous pouvez effectuer les actions suivantes :

- Ajouter ou retirer des appareils dans l'armoire en cliquant sur **Éditer l'armoire**.

  Remarque : Lorsque vous changez les composants installés dans l'armoire, il se peut que vous deviez attendre quelques instants avant que les informations s'affichent dans l'interface XClarity Administrator.
- Modifiez les propriétés d'appareil et d'obturateur (y compris le nom, l'emplacement et l'URL pour lancer l'interface web de gestion) en cliquant sur l'appareil ou l'obturateur, puis sur **Éditer les propriétés** dans le volet de récapitulatif de l'appareil.
- Consultez l'interface web du contrôleur de gestion d'un appareil ou d'un obturateur en cliquant sur celui-ci, puis en cliquant sur le lien **URL de lancement** dans le volet de récapitulatif de l'appareil.



Etape 4. Affichez l'état récapitulatif ou détaillé d'un appareil ou d'un composant :

a. Cliquez sur un appareil ou un composant présent dans l'armoire pour afficher le récapitulatif de l'état et les propriétés et l'état de cet appareil ou de ce composant.

b. Cliquez deux fois sur un appareil pour afficher la page de détails correspondante.

Procédure

Vous pouvez modifier la préférence d'ordre de numérotation des armoires (voir Définition des préférences d'inventaire).

Retrait d'une armoire

Vous pouvez retirer une armoire de Lenovo XClarity Administrator.

Procédure

Procédez comme suit pour retirer une armoire.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Armoires**. La page Toutes les armoires s'affiche.

La page Toutes les armoires affiche chaque armoire sous la forme d'une image miniature avec le nom de l'armoire, le nombre d'appareils gérés présents dans celle-ci et l'état de l'appareil présentant le niveau de gravité le plus élevé.

Remarques : Vous pouvez trier la liste des armoires par nom d'armoire, nombre d'appareils dans l'armoire, ou par niveau de gravité pour simplifier la recherche d'armoires spécifiques. Le tri est effectué de la gauche vers la droite, du haut vers le bas. En outre, vous pouvez filtrer les armoires par niveau de gravité en cliquant sur les icônes suivantes dans la barre d'outils ou en entrant un nom d'armoire dans la zone **Filtre** pour filtrer davantage les armoires qui s'affichent.

- L'icône **Alertes critiques** ( )
- L'icône **Alertes d'avertissements** ( )
- Icône **Alertes normales** ( )

Etape 2. Sélectionnez la miniature correspondant à l'armoire à retirer.

Etape 3. Cliquez sur l'icône **Retirer** ( ).

Etape 4. Cliquez sur **Retirer**.

Résultats

La miniature correspondant à l'armoire est retirée de la page Toutes les armoires et tous les appareils qui étaient présents dans cette armoire sont désormais disponibles sur la page Éditer les armoires pour être ajoutés à d'autres armoires.

Chapitre 7. Gestion des châssis

Lenovo XClarity Administrator peut gérer plusieurs types de systèmes, notamment le châssis Flex System.

En savoir plus : XClarity Administrator : Reconnaissance

Avant de commencer

Remarque : Les composants de châssis (tels que les modules CMM, les nœuds de traitement Flex et les commutateurs Flex) sont reconnus et gérés automatiquement lorsque vous gérez le châssis qui les contient. Vous ne pouvez pas reconnaître et gérer les composants de châssis distincts de ce dernier.

Avant de gérer des châssis, vérifiez que les conditions suivantes sont remplies :

- Consultez les instructions de gestion avant de gérer un dispositif. Pour plus d'informations, voir Considérations relatives à la gestion dans la documentation en ligne XClarity Administrator.
- Certains ports doivent être disponibles pour communiquer avec le module CMM pour le châssis géré. Vérifiez que ces ports sont disponibles avant de tenter de gérer un châssis. Pour plus d'informations sur les ports, voir Disponibilité de port dans la documentation en ligne de XClarity Administrator.
- Vérifiez que le microprogramme minimal requis est installé sur chaque châssis à gérer avec XClarity Administrator. Vous pouvez rechercher les niveaux de microprogramme minimum requis par la Support de XClarity Administrator – Page Web de compatibilité en cliquant sur l'onglet **Compatibilité**, puis en cliquant sur le lien des types d'appareil appropriés.
- Vérifiez que le paramètre **Nombre de sessions actives simultanées pour les utilisateurs LDAP** du module CMM est défini sur 0 (zéro) pour le châssis. Vous pouvez vérifier ce paramètre à partir de l'interface Web CMM en cliquant sur **Gestion du module de gestion → Comptes utilisateur**, sur **Paramètres de connexion globaux**, puis sur l'onglet **Général**.
- Assurez-vous qu'il existe au moins trois sessions en mode commande TCP définies pour la communication externe avec le module CMM. Pour savoir comment définir le nombre de sessions, voir Commande tcpcmdmode dans la documentation en ligne du module CMM.
- Pour identifier un châssis qui se trouve sur un sous-réseau *différent* de XClarity Administrator, veillez à ce que l'une des conditions suivantes soit remplie :
  - Veillez à activer la transmission SLP multidiffusion sur les commutateurs de la partie supérieure de l'armoire, ainsi que les routeurs de votre environnement. Consultez la documentation fournie avec votre routeur ou commutateur spécifique afin de déterminer si la transmission SLP multidiffusion est activée et de prendre connaissance des procédures permettant de l'activer si elle est désactivée.
  - Si le protocole SLP est désactivé sur le point de terminaison ou sur le réseau, vous pouvez utiliser à la place la méthode de détection DNS en ajoutant manuellement un enregistrement de service (enregistrement SRV) à votre serveur de noms de domaine (DNS), pour XClarity Administrator par exemple.

    ```
    _lxca._tcp.labs.lenovo.com      service = 0 0 443 fvt-xhmc3.labs.lenovo.com.
    ```

    Activez ensuite la reconnaissance DNS sur le module CMM à partir de l'interface Web de gestion en cliquant sur **Gestion du module de gestion → Protocole réseau**, sur l'onglet **DNS**, puis en sélectionnant **Utiliser DNS pour reconnaître Lenovo XClarity Administrator**.

    Remarques :

    - Le module CMM doit exécuter un niveau de microprogramme datant de mai 2017 pour prendre en charge la reconnaissance automatique via DNS.

- S'il existe plusieurs instances XClarity Administrator dans votre environnement, le châssis est uniquement reconnu par la première instance à répondre à la demande de reconnaissance. Le châssis n'est pas reconnu par toutes les instances.

Envisagez d'implémenter des adresses IPv4 *ou* IPv6 pour tous les modules CMM et les commutateurs Flex gérés par XClarity Administrator. Si vous implémentez une adresse IPv4 pour certains modules CMM et des commutateurs Flex et IPv6 pour d'autres, certains événements peuvent ne pas être reçus dans le journal d'audit (ou en tant qu'alertes d'audit).

Attention : Si vous prévoyez de gérer des modules CMM qui exécutent la pile Flex version 1.3.2.1 2PET12K à 2PET12Q comme niveau de microprogramme, qui sont en cours d'exécution depuis plus de trois semaines et qui figurent dans une configuration à deux modules CMM, vous devez réinstaller virtuellement les modules CMM avant de mettre à jour le microprogramme à l'aide de XClarity Administrator.

Important : Si vous prévoyez d'utiliser d'autres logiciels de gestion en plus de Lenovo XClarity Administrator pour surveiller votre châssis, et si ce logiciel de gestion utilise la communication SNMPv3, vous devez d'abord créer un ID utilisateur CMM local configuré avec les informations SNMPv3 appropriées, puis vous connecter au module CMM à l'aide de cet ID utilisateur et modifier le mot de passe. Pour plus d'informations, voir Considérations relatives à la gestion dans la documentation en ligne de XClarity Administrator.

À propos de cette tâche

XClarity Administrator peut détecter automatiquement le châssis dans votre environnement en sondant les systèmes gérables présents dans le même sous-réseau IP que XClarity Administrator. Pour reconnaître les châssis qui se trouvent dans d'autres sous-réseaux, définissez une adresse IP ou une plage d'adresses IP, ou importez les informations à partir d'un tableur.

Une fois que les châssis sont gérés par XClarity Administrator, XClarity Administrator interroge chaque châssis géré de manière périodique afin de collecter des informations, telles que l'inventaire, les données techniques essentielles et l'état. Vous pouvez afficher et contrôler chaque châssis géré et exécuter l'action de gestion (telle que configurer les informations système, le paramètre réseau et le basculement). Pour les châssis qui sont en mode protégé, les actions de gestion sont désactivées.

Les châssis sont gérés par *XClarity Administratorauthentification gérée*.

Par défaut, les appareils sont gérés par XClarity Administrator authentification gérée pour la connexion aux appareils. Lors de la gestion de serveurs rack et de châssis Lenovo, vous pouvez choisir d'utiliser l'authentification locale ou l'authentification gérée pour vous connecter aux appareils.

- Lorsque l'*authentification locale* est utilisée pour les serveurs rack, les châssis Lenovo et les commutateurs d'armoire, XClarity Administrator utilise des données d'identification stockées pour l'authentification sur l'appareil. Les *données d'identification stockées* peuvent être un compte utilisateur actif sur l'appareil ou un compte utilisateur dans un serveur Active Directory.

  Vous devez créer des données d’identification stockées dans XClarity Administrator qui correspondent à un compte utilisateur active sur l’appareil ou un compte utilisateur dans un serveur Active Directory avant de gérer l’appareil à l’aide de l’authentification locale (voir Gestion de données d'identification stockées dans la documentation en ligne XClarity Administrator).

  Remarques :

  - Les appareils RackSwitch prennent en charge uniquement les données d'identification stockées pour l'authentification. Les données d'identification utilisateur XClarity Administrator stockées ne sont pas prises en charge.

- L'*authentification gérée* vous permet de gérer et de surveiller plusieurs appareils à l'aide des données d'identification dans le serveur d'authentification XClarity Administrator au lieu des données d'identification locales. Lorsqu'un appareil (autre que des serveurs ThinkServer, System x M4 et des commutateurs) est géré par authentification gérée, XClarity Administrator configure l'appareil géré et ses composants installés afin d'utiliser le serveur d'authentification XClarity Administrator pour la gestion centralisée.
  - Lorsque l'authentification gérée est activée, vous pouvez gérer des appareils à l'aide de saisies manuelles ou de données d'identification stockées (voir Gestion des comptes utilisateur et dans la documentation en ligne de XClarity Administrator).

    Les données d'identification stockées sont utilisées uniquement jusqu'à ce que XClarity Administrator configure les paramètres LDAP sur l'appareil. Ensuite, toute modification apportée aux données d'identification stockées n'a aucun impact sur la gestion ou la surveillance de cet appareil.

    Remarque : Lorsque l'authentification gérée est activée pour un appareil, vous ne pouvez pas modifier les données d'identification stockées pour cet appareil à l'aide de XClarity Administrator.
  - Si un serveur LDAP local ou externe est utilisé comme serveur d'authentification XClarity Administrator, les comptes utilisateur définis dans le serveur d'authentification sont utilisés pour se connecter à XClarity Administrator, aux modules CMM et aux contrôleurs de gestion de la carte mère dans le domaine XClarity Administrator. Les CMM locaux et les comptes utilisateur du contrôleur de gestion sont désactivés.
  - Si un fournisseur d'identité SAML 2.0 est utilisé comme serveur d'authentification XClarity Administrator, les comptes SAML ne sont pas accessibles pour les appareils gérés. Cependant, lorsque vous utilisez un fournisseur d'identité SAML et un serveur LDAP ensemble et que le fournisseur d'identité utilise des comptes qui existent dans le serveur LDAP, les comptes utilisateur LDAP peuvent être utilisés pour se connecter à des appareils gérés, tandis que des méthodes d'authentification plus avancées qui sont fournies par SAML 2.0 (comme l'authentification à plusieurs facteurs et la connexion unique) peuvent être utilisées pour la connexion à XClarity Administrator.
  - L'authentification unique permet à un utilisateur qui est déjà connecté à XClarity Administrator de se connecter automatiquement au contrôle de gestion de la carte mère. La connexion unique est activée par défaut lorsqu'un serveur ThinkSystem ou ThinkAgile est amené dans la gestion par XClarity Administrator (sauf si le serveur est géré avec des mots de passe CyberArk). Vous pouvez configurer le paramètre global pour activer ou désactiver la connexion unique pour tous les serveurs ThinkSystem et ThinkAgile gérés. L'activation de la connexion unique pour un serveur ThinkSystem et ThinkAgile remplace le paramétrage global pour tous les serveurs ThinkSystem et ThinkAgile (voir).

    Remarque : La connexion unique est automatiquement désactivée lorsque vous faites appel au système de gestion d'identité CyberArk pour vous connecter.
  - Lorsque l'authentification gérée est activée pour les serveurs ThinkSystem SR635 et SR655 :
    - Le microprogramme du contrôleur de gestion de la carte mère prend en charge jusqu'à cinq rôles utilisateur LDAP. XClarity Administrator ajoute ces rôles utilisateur LDAP aux serveurs lors de la gestion : **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin** et **lxc-os-admin**.

      Les utilisateurs doivent être affectés à au moins l'un des rôles utilisateur LDAP spécifiés pour pouvoir communiquer avec les serveurs ThinkSystem SR635 et SR655.
    - Le microprogramme du contrôleur de gestion ne prend pas en charge les utilisateurs LDAP dont le nom d'utilisateur est identique à celui de l'utilisateur local du serveur.
  - Pour les serveurs ThinkServer et System x M4, le serveur d'authentification XClarity Administrator n'est pas utilisé. À la place, un compte IPMI est créé sur l'appareil avec le préfixe « LXCA_ » suivi d'une chaîne aléatoire. (Les comptes utilisateur IPMI locaux ne sont pas désactivés.) Lorsque vous annulez la gestion d'un serveur ThinkServer, le compte utilisateur « LXCA_ » est désactivé, et le préfixe « LXCA_ » est remplacé par le préfixe « DISABLED_ ». Pour déterminer si un serveur ThinkServer est géré par une autre instance, XClarity Administrator recherche les comptes IPMI ayant le préfixe

« LXCA_ ». Si vous choisissez de forcer la gestion d'un serveur ThinkServer géré, tous les comptes IPMI sur l'appareil avec le préfixe « LXCA_ » sont désactivés et renommés. Pensez à supprimer manuellement les comptes IPMI qui ne sont plus utilisés.

Si vous utilisez des données d'identification saisies manuellement, XClarity Administrator crée automatiquement des données d'identification stockées et utilise ces dernières pour gérer l'appareil.

Remarques : Lorsque l'authentification gérée est activée pour un appareil, vous ne pouvez pas modifier les données d'identification stockées pour cet appareil à l'aide de XClarity Administrator.

- Chaque fois que vous gérez un appareil en utilisant des données d'identification saisies manuellement, de nouvelles données d'identification stockées sont créées pour cet appareil, même si d'autres données d'identification stockées ont été créées pour cet appareil lors d'un processus de gestion précédent.
- Lorsque vous annulez la gestion d'un appareil, XClarity Administrator ne supprime pas les données d'identification stockées qui ont été créées automatiquement pour cet appareil lors du processus de gestion.

Un dispositif peut être géré par une seule instance XClarity Administrator à la fois. La gestion par plusieurs instances de XClarity Administrator n'est pas prise en charge. Si un dispositif est géré par une instance de XClarity Administrator, et que vous souhaitez le gérer avec une autre instance de XClarity Administrator, vous devez d'abord annuler la gestion du dispositif dans l'instance de XClarity Administrator en cours, puis la gérer avec la nouvelle instance de XClarity Administrator. Si une erreur se produit lors du processus d'annulation de gestion, vous pouvez sélectionner l'option **Forcer la gestion** lors de la gestion sur la nouvelle instance de XClarity Administrator.

Remarque : En analysant le réseau pour rechercher des dispositifs gérables, XClarity Administrator ne sait pas si un dispositif est déjà géré par un autre gestionnaire avant d'avoir tenté de gérer le dispositif.

Au cours du processus de gestion, XClarity Administrator exécute les actions suivantes :

- Se connecte au châssis à l'aide des données d'identification fournies.
- Collecte l'inventaire pour tous les composants de chaque châssis, tels que le module CMM, les nœuds de traitement, les dispositifs de stockage et Commutateurs Flex.

  Remarque : Certaines données d'inventaire sont collectées une fois le processus de gestion terminé. Le châssis possède l'état En attente jusqu'à ce que toutes les données d'inventaire soient collectées. Vous ne pouvez pas exécuter certaines tâches sur un dispositif géré (comme le déploiement d'un modèle de serveur) jusqu'à ce que toutes les données d'inventaire soient collectées pour ce dispositif et que le châssis ne possède plus l'état En attente.
- Configure les paramètres du serveur NTP de sorte que tous les appareils gérés utilisent le serveur NTP depuis XClarity Administrator.
- Affecte la dernière stratégie de conformité du microprogramme modifiée au châssis.
- Pour les dispositifs Lenovo Flex, configure éventuellement les règles de pare-feu des dispositifs afin que les demandes entrantes soient acceptées uniquement à partir de XClarity Administrator.
- Échange les certificats de sécurité avec le module CMM, en copiant le certificat de sécurité CMM dans le fichier de clés certifiées XClarity Administrator et en envoyant le certificat de sécurité CA XClarity Administrator au module CMM. Le module CMM charge le certificat dans le fichier de clés certifiées CMM et le distribue aux processeurs de service de nœud de traitement pour qu'il soit inclus dans leur fichier de clés certifiées.
- Configure l'authentification gérée. Les paramètres pour le client LDAP CMM sont modifiés de façon à utiliser XClarity Administrator en tant que serveur d'authentification, et les paramètres de connexion globaux dans le module CMM sont modifiés sur le **serveur d'authentification externe uniquement**. Pour plus d'informations sur l'authentification gérée, voir Gestion du serveur d'authentification.

- Crée le compte utilisateur de récupération (`RECOVERY_ID`). Pour plus d'informations sur le compte `RECOVERY_ID`, voir Gestion du serveur d'authentification.

Attention : Lors de la gestion d'un châssis, XClarity Administrator définit sur 15 le nombre maximal de connexions Mode de commande TCP sécurisé simultanées et définit sur 0 le nombre maximal de connexions Mode de commande TCP existant simultanées. Cela remplace les paramètres que vous pouvez avoir déjà définis sur le module CMM.

Remarque : XClarity Administrator ne modifie pas les paramètres de sécurité ni les paramètres cryptographiques (mode cryptographique et mode utilisé pour les communications sécurisées) lors du processus de gestion. Vous pouvez modifier les paramètres cryptographiques une fois le châssis géré (voir Configuration des paramètres cryptographiques sur le serveur de gestion).

Procédure

Suivez l'une des procédures suivantes pour reconnaître et gérer votre châssis avec XClarity Administrator.

- Détectez et gérez un grand nombre de châssis et d'autres appareils à l'aide d'un fichier d'importation en masse (voir Gestion des systèmes dans la documentation en ligne Lenovo XClarity Administrator).
- Reconnaissez et gérez les châssis présents sur le même sous-réseau IP que XClarity Administrator.
  1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Reconnaître et gérer de nouveaux appareils**. La page Reconnaître et gérer de nouveaux appareils s'affiche.

Vous pouvez trier les colonnes du tableau pour trouver plus facilement le châssis que vous souhaitez gérer. En outre, vous pouvez entrer du texte (comme un nom de système ou l'adresse IP) dans le champ **Filtre** pour filtrer davantage les châssis affichés. Vous pouvez modifier les colonnes qui s'affichent et l'ordre de tri par défaut en cliquant sur l'icône **Personnaliser les colonnes** ().

2. Cliquez sur l'icône **Actualiser** () pour reconnaître tous les périphériques gérables dans le domaine XClarity Administrator. La reconnaissance peut prendre plusieurs minutes.
3. Cliquez sur la case à cocher **Activer l'encapsulage de tous les appareils gérés ultérieurs** afin de modifier les règles de pare-feu sur tous les dispositifs lors du processus de gestion, de sorte que les demandes entrantes sont acceptées uniquement à partir de XClarity Administrator.

   L'encapsulage peut être activé ou désactivé sur des dispositifs spécifiques après leur gestion.

   Attention : Si l'encapsulage est activé et que XClarity Administrator n'est plus disponible avant l'annulation de la gestion d'un dispositif, des mesures doivent être prises pour désactiver l'encapsulage afin d'établir la communication avec le dispositif. Pour les procédures de récupération, voir le fichier lenovoMgrAlert.mib et Reprise de la gestion avec un module CMM après une défaillance du serveur de gestion.
4. Sélectionnez un ou plusieurs châssis à gérer.
5. Cliquez sur **Gérer la sélection**.
6. Choisissez d'utiliser XClarity Administrator l'authentification gérée ou l'authentification locale pour cet appareil. L'authentification gérée est sélectionnée par défaut. Pour utiliser l'authentification locale, désactivez l'option **Authentification gérée**.

   Remarque : L'authentification gérée et l'authentification locale ne sont pas prises en charge pour les serveurs ThinkServer et System x M4.
7. Choisissez le type de données d'identification à utiliser pour l'appareil et spécifiez les données d'identification appropriées :
   - **Utiliser des données d'identification saisies manuellement**
     - Spécifiez l'ID utilisateur local et le mot de passe avec des droits **lxc-supervisor** pour l'authentification auprès de CMM.
     - (Facultatif) Spécifiez un nouveau mot de passe pour le compte utilisateur CMM si le mot de passe a expiré sur l'appareil.
   - **Utiliser des données d'identification stockées**

     Sélectionnez les données d'identification stockées dotées de droits **lxc-supervisor** à utiliser pour cet appareil géré. Vous pouvez ajouter des données d'identification stockées en cliquant sur **Gérer les données d'identification stockées**.

     Remarque : Si vous choisissez d'utiliser l'authentification locale, vous devez sélectionner des données d'identification stockées pour gérer l'appareil.

   Astuce : Il est recommandé d'utiliser un compte administrateur ou superviseur pour gérer l'appareil. Si un compte avec un niveau de droits plus bas est utilisé, la gestion peut échouer, ou la gestion peut aboutir, mais d'autres opérations futures XClarity Administrator sur l'appareil peuvent échouer (notamment si l'appareil est géré sans authentification gérée).

   Pour plus d'informations sur les données d'identification normales et stockées, voir Gestion des comptes utilisateur, Gestion de données d'identification stockées.
8. Spécifiez le mot de passe de récupération si l'authentification gérée est sélectionnée.

   Un compte de récupération (`RECOVERY_ID`) est créé sur le module CMM, et tous les comptes utilisateur locaux sont désactivés. En cas de problème avec XClarity Administrator, et s'il cesse de fonctionner

pour une raison quelconque, vous *ne pouvez pas* vous connecter au module CMM en utilisant des comptes utilisateur normaux. Cependant, vous pouvez vous connecter avec le compte `RECOVERY_ID`.

Remarque :

- Le mot de passe de récupération est obligatoire si vous choisissez d'utiliser l'authentification locale mais n'est pas autorisé si vous choisissez l'authentification locale.
- Vous pouvez choisir d'utiliser un compte de récupération local ou des données d'identification de récupération stockées. Dans les deux cas, le nom d'utilisateur est toujours `RECOVERY_ID`.
- Veillez à ce que le mot de passe respecte les règles de sécurité et définies pour les mots de passe sur l'appareil. Les règles de sécurité et de mot de passe peuvent varier.
- Veillez à noter le mot de passe de récupération pour un usage ultérieur.

Pour plus d'informations sur l'ID de récupération, voir Gestion du serveur d'authentification.

9. Cliquez sur **Modifier** pour modifier les groupes de rôles qui doivent être affectés aux appareils.

   Remarques :

   - Vous pouvez effectuer votre sélection dans une liste de groupes de rôles affectée à l'utilisateur en cours.
   - Si vous ne modifiez pas les groupes de rôles, les groupes de rôles par défaut sont utilisés. Pour plus d'informations sur les groupes de rôles par défaut, voir Modification des droits par défaut.

10. Cliquez sur **Gérer**.

    Une boîte de dialogue s'affiche et présente la progression de ce processus de gestion. Pour vérifier si le processus aboutit, surveillez la progression.

    Une fois le processus terminé, la boîte de dialogue affiche le nombre de dispositifs dans le châssis et l'état du châssis.

    Remarque : Certaines données d'inventaire sont collectées une fois le processus de gestion terminé. Le châssis possède l'état En attente jusqu'à ce que toutes les données d'inventaire soient collectées. Vous ne pouvez pas exécuter certaines tâches sur un dispositif géré (comme le déploiement d'un modèle de serveur) jusqu'à ce que toutes les données d'inventaire soient collectées pour ce dispositif et que le châssis ne possède plus l'état En attente.

11. Une fois le processus terminé, cliquez sur **OK**.

    Le dispositif est désormais géré par XClarity Administrator, qui interroge automatiquement et régulièrement le dispositif géré afin de collecter des informations à jour, telles que l'inventaire.

    Si la gestion n'a pas abouti en raison d'une des conditions d'erreur suivantes, répétez cette procédure en utilisant l'option **Forcer la gestion**.

    - Si l'instance de XClarity Administrator a échoué et ne peut pas être récupérée.

      Remarque : Si l'instance de remplacement de XClarity Administrator utilise la même adresse IP que l'instance de XClarity Administrator ayant rencontré une défaillance, vous pouvez gérer à nouveau le dispositif à l'aide du compte et du mot de passe RECOVERY_ID (le cas échéant) et de l'option **Forcer la gestion**.
    - Si l'instance XClarity Administrator de gestion a été mise hors tension avant que la gestion des appareils n'ait été annulée.
    - Si l'annulation de la gestion des appareils n'a pas été correctement effectuée.

    Attention : Les appareils peuvent être géré par une seule instance XClarity Administrator à la fois. La gestion par plusieurs instances de XClarity Administrator n'est pas prise en charge. Si un appareil est géré par une instance de XClarity Administrator, et que vous souhaitez le gérer avec une autre

instance de XClarity Administrator, vous devez d'abord annuler la gestion de l'appareil dans l'instance de XClarity Administrator d'origine, puis la gérer avec la nouvelle instance de XClarity Administrator.

12. S'il s'agit d'un nouveau châssis, cliquez sur **Poursuivre avec la configuration de châssis** pour valider et modifier les paramètres du réseau de gestion pour l'ensemble du châssis (comprenant les nœuds de traitement et les commutateurs Flex) et pour configurer les informations du nœud de traitement, le stockage local, les cartes d'E-S, les cibles d'amorçage et les paramètres de microprogramme lors de la création et du déploiement des modèles de serveur. Pour plus d'informations, voir Modification des paramètres IP de gestion pour un châssis et Configuration des serveurs à l'aide de modèles de configuration.

- Reconnaissez et gérez les châssis qui ne sont pas sur le même sous-réseau IP que XClarity Administrator en spécifiant manuellement des adresses IP.
  1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Reconnaître et gérer de nouveaux appareils**. La page Reconnaître et gérer s'affiche.
  2. Cliquez sur la case à cocher **Activer l'encapsulage de tous les appareils gérés ultérieurs** afin de modifier les règles de pare-feu sur tous les dispositifs lors du processus de gestion, de sorte que les demandes entrantes sont acceptées uniquement à partir de XClarity Administrator.

     L'encapsulage peut être activé ou désactivé sur des dispositifs spécifiques après leur gestion.

     Attention : Si l'encapsulage est activé et que XClarity Administrator n'est plus disponible avant l'annulation de la gestion d'un dispositif, des mesures doivent être prises pour désactiver l'encapsulage afin d'établir la communication avec le dispositif. Pour les procédures de récupération, voir le fichier lenovoMgrAlert.mib et Reprise de la gestion avec un module CMM après une défaillance du serveur de gestion.
  3. Sélectionnez **Saisie manuelle**.
  4. Indiquez les adresses réseau du châssis à gérer :
     - Cliquez sur **Système unique**, puis entrez un nom de domaine d'adresse IP unique, ou un nom de domaine complet (FQDN).

       Remarque : Pour indiquer un nom FQDN, vérifiez qu'un nom de domaine valide est spécifié sur la page Accès réseau (voir Configuration de l'accès réseau).
     - Cliquez sur **Plusieurs systèmes** et entrez une plage d'adresses IP. Pour ajouter une autre plage, cliquez sur l'icône **Ajouter** (). Pour supprimer une plage, cliquez sur l'icône **Supprimer** ().
  5. Cliquez sur **OK**.
  6. Choisissez d'utiliser XClarity Administrator l'authentification gérée ou l'authentification locale pour cet appareil. L'authentification gérée est sélectionnée par défaut. Pour utiliser l'authentification locale, désactivez l'option **Authentification gérée**.

     Remarque : L'authentification gérée et l'authentification locale ne sont pas prises en charge pour les serveurs ThinkServer et System x M4.
  7. Choisissez le type de données d'identification à utiliser pour l'appareil et spécifiez les données d'identification appropriées :
     - **Utiliser des données d'identification saisies manuellement**
       - Spécifiez l'ID utilisateur local et le mot de passe avec des droits **lxc-supervisor** pour l'authentification auprès de CMM.
       - (Facultatif) Spécifiez un nouveau mot de passe pour le compte utilisateur CMM si le mot de passe a expiré sur l'appareil.
     - **Utiliser des données d'identification stockées**

Sélectionnez les données d'identification stockées dotées de droits **lxc-supervisor** à utiliser pour cet appareil géré. Vous pouvez ajouter des données d'identification stockées en cliquant sur **Gérer les données d'identification stockées**.

Remarque : Si vous choisissez d'utiliser l'authentification locale, vous devez sélectionner des données d'identification stockées pour gérer l'appareil.

Astuce : Il est recommandé d'utiliser un compte administrateur ou superviseur pour gérer l'appareil. Si un compte avec un niveau de droits plus bas est utilisé, la gestion peut échouer, ou la gestion peut aboutir, mais d'autres opérations futures XClarity Administrator sur l'appareil peuvent échouer (notamment si l'appareil est géré sans authentification gérée).

Pour plus d'informations sur les données d'identification normales et stockées, voir Gestion des comptes utilisateur, Gestion de données d'identification stockées.

8. Spécifiez le mot de passe de récupération si l'authentification gérée est sélectionnée.

   Un compte de récupération (`RECOVERY_ID`) est créé sur le module CMM, et tous les comptes utilisateur locaux sont désactivés. En cas de problème avec XClarity Administrator, et s'il cesse de fonctionner pour une raison quelconque, vous *ne pouvez pas* vous connecter au module CMM en utilisant des comptes utilisateur normaux. Cependant, vous pouvez vous connecter avec le compte `RECOVERY_ID`.

   Remarque :

   - Le mot de passe de récupération est obligatoire si vous choisissez d'utiliser l'authentification locale mais n'est pas autorisé si vous choisissez l'authentification locale.
   - Vous pouvez choisir d'utiliser un compte de récupération local ou des données d'identification de récupération stockées. Dans les deux cas, le nom d'utilisateur est toujours `RECOVERY_ID`.
   - Veillez à ce que le mot de passe respecte les règles de sécurité et définies pour les mots de passe sur l'appareil. Les règles de sécurité et de mot de passe peuvent varier.
   - Veillez à noter le mot de passe de récupération pour un usage ultérieur.

   Pour plus d'informations sur l'ID de récupération, voir Gestion du serveur d'authentification.

9. Cliquez sur **Modifier** pour modifier les groupes de rôles qui doivent être affectés aux appareils.

   Remarques :

   - Vous pouvez effectuer votre sélection dans une liste de groupes de rôles affectée à l'utilisateur en cours.
   - Si vous ne modifiez pas les groupes de rôles, les groupes de rôles par défaut sont utilisés. Pour plus d'informations sur les groupes de rôles par défaut, voir Modification des droits par défaut.

10. Cliquez sur **Gérer**.

    Une boîte de dialogue s'affiche et présente la progression de ce processus de gestion. Surveillez la progression pour vérifier si le processus aboutit.

    Une fois le processus terminé, la boîte de dialogue affiche le nombre de dispositifs dans le châssis et l'état du châssis.

    Remarque : Certaines données d'inventaire sont collectées une fois le processus de gestion terminé. Le châssis possède l'état En attente jusqu'à ce que toutes les données d'inventaire soient collectées. Vous ne pouvez pas exécuter certaines tâches sur un dispositif géré (comme le déploiement d'un modèle de serveur) jusqu'à ce que toutes les données d'inventaire soient collectées pour ce dispositif et que le châssis ne possède plus l'état En attente.

11. Une fois le processus terminé, cliquez sur **OK**.

    Le dispositif est désormais géré par XClarity Administrator, qui interroge automatiquement et régulièrement le dispositif géré afin de collecter des informations à jour, telles que l'inventaire.

Si la gestion n’a pas abouti en raison d’une des conditions d’erreur suivantes, répétez cette procédure en utilisant l'option **Forcer la gestion**.

– Si l'instance de XClarity Administrator a échoué et ne peut pas être récupérée.

  Remarque : Si l'instance de remplacement de XClarity Administrator utilise la même adresse IP que l'instance de XClarity Administrator ayant rencontré une défaillance, vous pouvez gérer à nouveau le dispositif à l'aide du compte et du mot de passe RECOVERY_ID (le cas échéant) et de l'option **Forcer la gestion**.

– Si l'instance XClarity Administrator de gestion a été mise hors tension avant que la gestion des appareils n'ait été annulée.

– Si l'annulation de la gestion des appareils n'a pas été correctement effectuée.

Attention : Les appareils peuvent être géré par une seule instance XClarity Administrator à la fois. La gestion par plusieurs instances de XClarity Administrator n'est pas prise en charge. Si un appareil est géré par une instance de XClarity Administrator, et que vous souhaitez le gérer avec une autre instance de XClarity Administrator, vous devez d'abord annuler la gestion de l'appareil dans l'instance de XClarity Administrator d'origine, puis la gérer avec la nouvelle instance de XClarity Administrator.

12. S'il s'agit d'un nouveau châssis, cliquez sur **Poursuivre avec la configuration de châssis** pour valider et modifier les paramètres du réseau de gestion pour l'ensemble du châssis (comprenant les nœuds de traitement et les commutateurs Flex) et pour configurer les informations du nœud de traitement, le stockage local, les cartes d’E-S, les cibles d'amorçage et les paramètres de microprogramme lors de la création et du déploiement des modèles de serveur. Pour plus d'informations, voir Modification des paramètres IP de gestion pour un châssis et Configuration des serveurs à l’aide de modèles de configuration.

Après avoir terminé

- Reconnaître et gérer d'autres dispositifs.
- Déployer les images du système d'exploitation sur les serveurs qui n'ont pas déjà de système d'exploitation. Pour plus d'informations, voir Installation de systèmes d’exploitation sur des serveurs nus.
- Mettez à jour le microprogramme sur les dispositifs qui ne sont pas en conformité avec les règles actuelles (Mise à jour du microprogramme sur les appareils gérés).
- Ajoutez les dispositifs récemment gérés dans l'armoire appropriée pour refléter l'environnement physique (voir Gestion des armoires).
- Surveillez l'état et les informations détaillées du matériel (voir Affichage de l'état d'un serveur géré).
- Surveillez les événements et alertes (voir Utilisation des événements et Utilisation des alertes).

Affichage de l'état de châssis gérés

Vous pouvez afficher un récapitulatif et un état détaillé pour les châssis gérés et leurs composants installés depuis Lenovo XClarity Administrator.

En savoir plus :

- XClarity Administrator : Inventaire
- XClarity Administrator : Surveillance

À propos de cette tâche

Les icônes d'état suivantes sont utilisées pour indiquer l'état de santé global de l'appareil. Si les certificats ne correspondent pas, la mention « (Non sécurisé) » est ajoutée à l'état de chaque appareil concerné, par exemple Avertissement (Non sécurisé). En cas de problème de connectivité ou si une connexion à l'appareil n'est pas sécurisée, la mention « (Connectivité) » est ajoutée à l'état de chaque appareil concerné, par exemple Avertissement (Connectivité).

- () Critique
- () Avertissement
- () En attente
- () Informations
- () Normal
- () Hors ligne
- () Inconnu

Procédure

Procédez comme suit pour afficher l'état d'un châssis géré.

- Affichez des informations détaillées sur les châssis en cliquant sur le lien **Détails** ou en cliquant sur **Actions → Vues → Détails**.
- Lancez l'interface Web CMM pour le châssis en cliquant sur le lien **Adresse IP** (voir Lancement de l'interface Web CMM pour un châssis).
- Modifiez les informations (telles que le contact, l'emplacement et la description du support) en cliquant sur **Actions → Inventaire → Éditer les propriétés**.
- Modifiez les paramètres IP de gestion pour l'ensemble du châssis, y compris les nœuds de traitement et les commutateurs Flex, en cliquant sur **Actions → Inventaire → Éditer les adresses IP de gestion**.
- Exportez des informations détaillées relatives à un ou plusieurs châssis vers un seul fichier CSV en sélectionnant le châssis, puis en cliquant sur **Actions → Inventaire → Exporter l'inventaire**.

  Remarque : Vous pouvez exporter les données d'inventaire pour un maximum de 60 dispositifs en même temps.

  Conseil : Lors de l'importation d'un fichier CSV dans Microsoft Excel, Excel traite les valeurs textuelles contenant uniquement des numéros sous la forme de valeurs numériques (par exemple, pour des UUID). Formatez chaque cellule sous forme de texte pour résoudre cette erreur.
- Corrigez les problèmes pouvant survenir entre le certificat de sécurité de Lenovo XClarity Administrator et le certificat de sécurité du module CMM dans le châssis en sélectionnant un châssis, puis en cliquant sur **Actions → Sécurité → Résoudre les certificats non sécurisés**.

Affichage des détails d'un châssis géré

Vous pouvez afficher les informations détaillées sur les châssis gérés depuis Lenovo XClarity Administrator, notamment sur les niveaux de microprogramme, les adresses IP et l'identificateur unique universel (UUID).

En savoir plus :

- XClarity Administrator : Inventaire
- XClarity Administrator : Surveillance

À propos de cette tâche

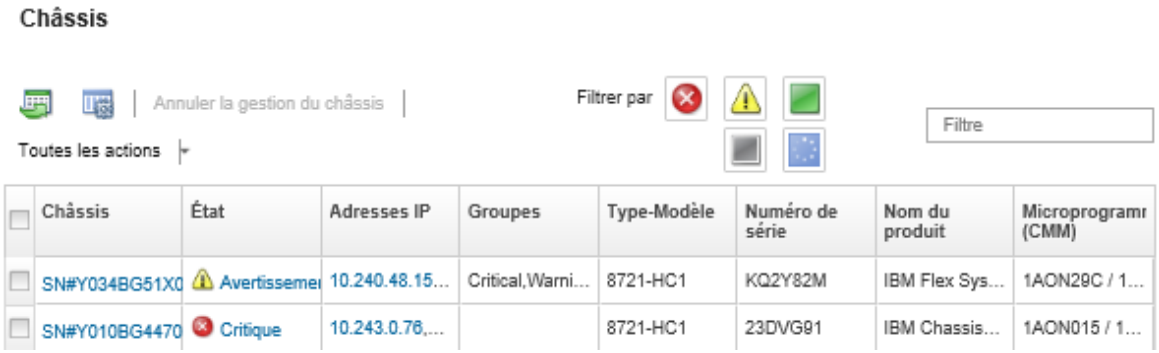
La température d'air au niveau du système est mesurée par un détecteur physique situé à l'avant du serveur. Cette température représente la température d'air entrant du serveur. Notez que la température d'air signalée par XClarity Administrator et celle communiquée par le module CMM peuvent être différentes si elles sont capturées à des moments différents.

Procédure

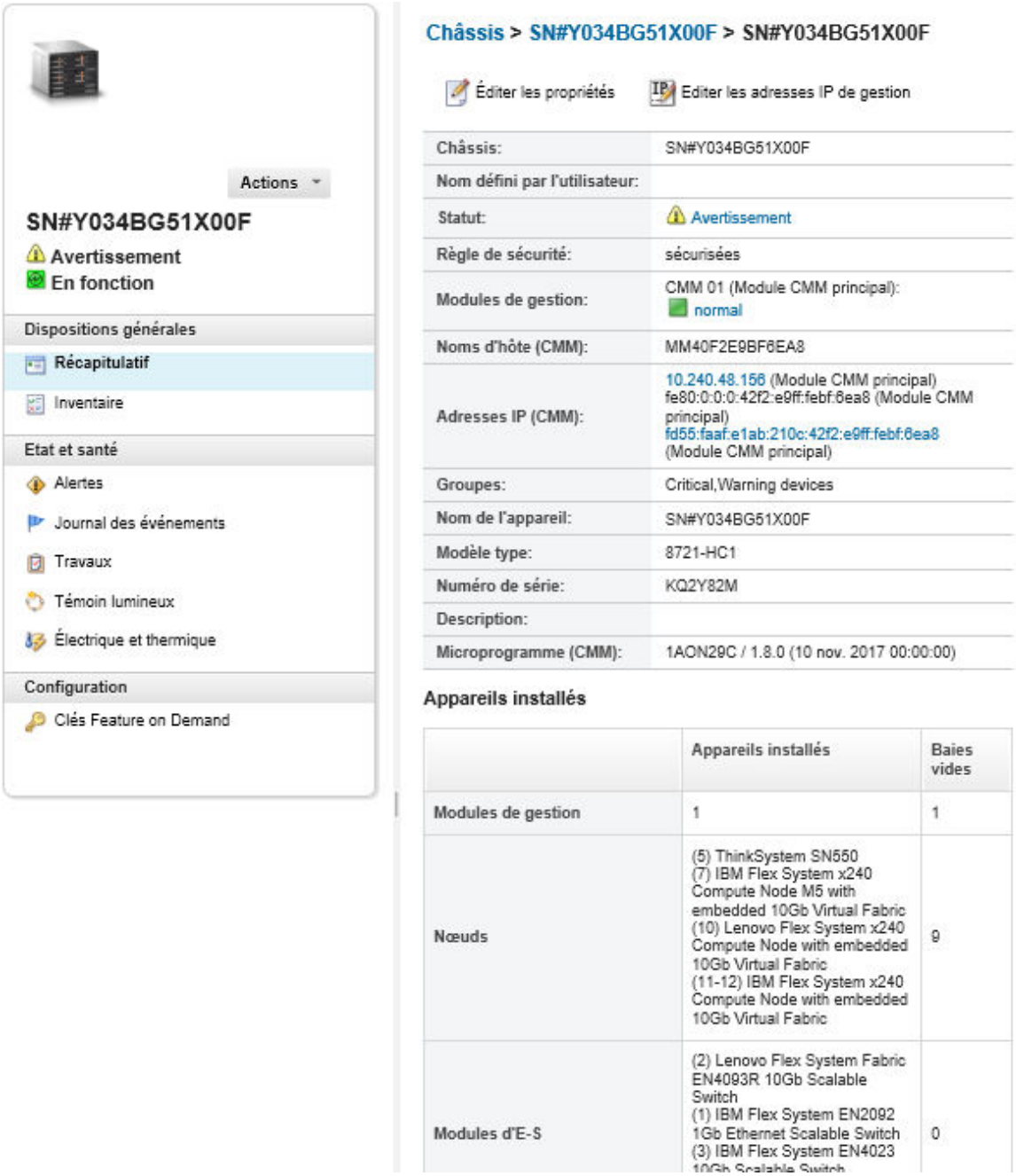
Procédez comme suit pour afficher les détails d'un châssis géré.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Châssis**. La page Châssis s'affiche avec une vue tabulaire de tous les châssis gérés.

Vous pouvez trier les colonnes du tableau pour trouver plus facilement le châssis que vous souhaitez gérer. En outre, vous pouvez entrer du texte (comme un nom de châssis ou une adresse IP) dans le champ **Filtre** pour filtrer davantage les châssis affichés.



Etape 2. Cliquez sur le nom du châssis dans la colonne **Châssis**. La page de récapitulatif de l'état de ce châssis s'affiche et présente les propriétés du châssis et les composants installés dans le châssis.



Etape 3. Exécutez une ou plusieurs des actions suivantes :

- Cliquez sur **Récapitulatif** pour afficher un récapitulatif du châssis, y compris les informations système et les composants installés (voir Affichage de l'état de châssis gérés).
- Cliquez sur **Détails d'inventaire** pour afficher des détails sur les composants de châssis, y compris :
  - Les niveaux de microprogramme pour tous les composants du châssis.
  - Les détails du module CMM, tels que le nom d'hôte, l'adresse IPv4, l'adresse IPv6 et les adresses MAC.
  - Détails des actifs du châssis et du module CMM installé dans le châssis, notamment le nom, l'identificateur unique universel (UUID) et l'emplacement.

- Cliquez sur **Alertes** pour afficher la liste des alertes actuelles du châssis (voir Utilisation des alertes).
- Cliquez sur **Journal des événements** pour afficher la liste des événements du châssis (voir Surveillance des événements dans le journal des événements).
- Cliquez sur **Travaux** pour afficher la liste des travaux associés au châssis (voir Surveillance des travaux).
- Cliquez sur **Light path** pour afficher l'état actuel des voyants de châssis, comme Emplacement, Erreur et Informations. Cela revient à regarder le panneau frontal du châssis.
- Cliquez sur **Électrique et thermique** pour afficher des détails sur l'alimentation et la ventilation.

  Conseil : utilisez le bouton d'actualisation de votre navigateur Web pour collecter les dernières données électriques et thermiques. La collecte de données peut prendre plusieurs minutes.
- Cliquez sur **Clés Feature on Demand** pour accéder à des informations nécessaires pour commander une clé Feature on Demand et d'autres informations sans agent (voir Affichage des clés Features on Demand (FoD)).

Après avoir terminé

En plus d'afficher le récapitulatif et des informations détaillées relatives à un châssis, vous pouvez effectuer les actions suivantes :

- Afficher un châssis dans la vue graphique d'armoire ou de châssis en cliquant sur **Actions → Vues → Afficher dans la vue Armoire** ou **Actions → Vues → Afficher dans la vue Châssis**.
- Lancez l'interface Web CMM en cliquant sur le lien **Adresse IP** (voir Lancement de l'interface Web CMM pour un châssis).
- Modifiez les informations (telles que le contact du support, l'emplacement et la description) en cliquant sur **Éditer les propriétés** (voir Modification des propriétés système pour un châssis).
- Modifiez les paramètres IP de gestion pour l'ensemble du châssis, y compris les nœuds de traitement et les commutateurs Flex, en cliquant sur **Toutes les actions → Inventaire → Éditer les adresses IP de gestion** (voir Modification des paramètres IP de gestion pour un châssis).
- Exporter des informations détaillées sur les châssis dans un fichier CSV en cliquant sur **Actions → Inventaire → Exporter l'inventaire**.

  Remarques :

  – Pour plus d'informations sur les données d'inventaire dans le fichier CSV, voir GET /chassis/*<UUID_list>* dans la documentation en ligne de XClarity Administrator.

  – Lors de l'importation d'un fichier CSV dans Microsoft Excel, Excel traite les valeurs textuelles contenant uniquement des numéros sous la forme de valeurs numériques (par exemple, pour des UUID). Formatez chaque cellule sous forme de texte pour résoudre cette erreur.
- Annuler la gestion d'un châssis (voir Désactivation de la gestion d'un châssis).
- Activer ou désactiver les modifications de règles de pare-feu sur un châssis qui limitent les demandes entrantes à celles provenant de XClarity Administrator en sélectionnant le châssis et en cliquant sur **Actions → Sécurité → Activer l'encapsulage** ou **Actions → Sécurité → Désactiver l'encapsulage**.

  Le paramètre d'encapsulage global est désactivé par défaut. Une fois désactivé, le mode d'encapsulage de dispositif est défini sur « normal » et les règles de pare-feu ne sont pas modifiées dans le cadre du processus de gestion.

  Le paramètre d'encapsulage global est désactivé par défaut. Une fois désactivé, le mode d'encapsulage de dispositif est défini sur « normal » et les règles de pare-feu ne sont pas modifiées dans le cadre du processus de gestion.

Lorsque le paramètre global d'encapsulage est activé et que le dispositif prend en charge l'encapsulage, XClarity Administrator communique avec le dispositif pendant le processus de gestion pour remplacer le mode d'encapsulage de dispositif par « encapsulationLite » et modifier les règles de pare-feu sur le dispositif afin de limiter les demandes entrantes à celles de XClarity Administrator.

Attention : Si l'encapsulage est activé et que XClarity Administrator n'est plus disponible avant l'annulation de la gestion d'un dispositif, des mesures doivent être prises pour désactiver l'encapsulage afin d'établir la communication avec le dispositif. Pour les procédures de récupération, voir le fichier lenovoMgrAlert.mib et Reprise de la gestion avec un module CMM après une défaillance du serveur de gestion.

- Corrigez les problèmes pouvant survenir entre le certificat de sécurité de XClarity Administrator et le certificat de sécurité du CMM dans le châssis en sélectionnant un châssis, puis en cliquant sur **Actions → Sécurité → Résoudre les certificats non sécurisés** (voir Résolution d'un certificat du serveur non sécurisé).

Sauvegarde et restauration des données de configuration CMM

Lenovo XClarity Administrator n'inclut pas de fonctions de sauvegarde intégrées pour les données de configuration CMM. À la place, utilisez les fonctions de sauvegarde qui sont disponibles pour votre module CMM géré.

Utilisez l'interface Web ou l'interface de ligne de commande (CLI) de gestion pour sauvegarder et restaurer le module CMM.

- Sauvegarder les données de configuration CMM
  - Dans l'interface Web de gestion, cliquez sur **Gestion du module de gestion → Configuration → Configuration de sauvegarde**. Pour plus d'informations, voir Sauvegarde d'une configuration CMM via l'interface web dans la documentation en ligne Flex Systems.
  - Dans l'interface CLI, utilisez la commande `write`. Pour plus d'informations, voir Commande CMM write dans la documentation en ligne Flex Systems
- Restaurer les données de configuration CMM
  - Dans l'interface Web de gestion, cliquez sur **Gestion du module de gestion → Configuration → Restaurer la configuration à partir du fichier**. Pour plus d'informations, voir Restauration d'une configuration CMM via l'interface du site web dans la documentation en ligne Flex Systems.
  - Dans l'interface CLI, utilisez la commande `read`. Pour plus d'informations, voir Commande CMM read dans la documentation enligne Flex Systems.

Remarque : Conseil : Des informations supplémentaires relatives à la sauvegarde et la restauration des composants du châssis sont disponibles dans le Guide des bonnes pratiques de sauvegarde et de restauration PureFlex et Flex System.

Lancement de l'interface Web CMM pour un châssis

Vous pouvez lancer l'interface Web CMM pour un châssis spécifique à partir de Lenovo XClarity Administrator.

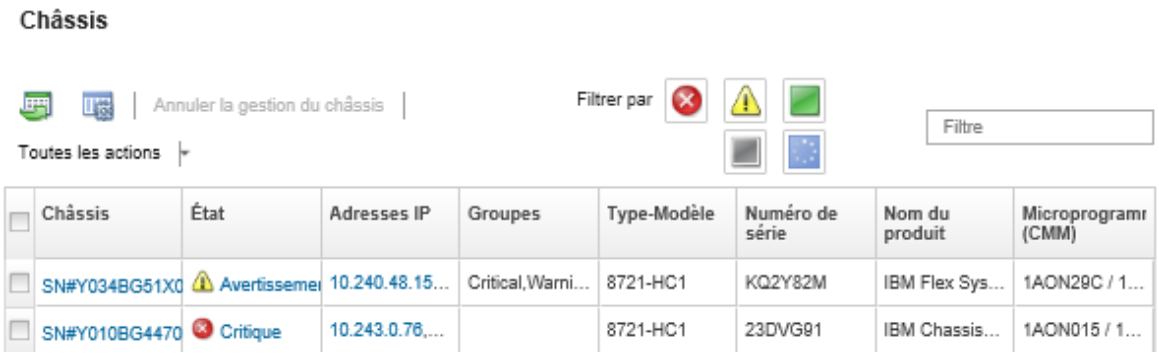
Procédure

Procédez comme suit pour lancer une interface Web CMM.

Remarque : Le lancement de cette interface Web CMM à partir de XClarity Administrator à l'aide du navigateur Web Safari n'est pas pris en charge.

Etape 1. Dans la barre de menu XClarity Administrator, cliquez sur **Matériel → Châssis** pour afficher la page Châssis.

Vous pouvez trier les colonnes du tableau pour trouver plus facilement le châssis que vous souhaitez gérer. En outre, vous pouvez entrer du texte (comme un nom de châssis ou une adresse IP) dans le champ **Filtre** pour filtrer davantage les châssis affichés.



Etape 2. Cliquez sur le lien du châssis dans la colonne **Châssis**. La page de récapitulatif de l'état de ce châssis est affichée.

Etape 3. Cliquez sur **Toutes les actions → Lancer → Interface Web de gestion**. L'interface Web CMM est démarrée.

Conseil : vous pouvez également cliquer sur l'adresse IP pour lancer le module CMM.

Etape 4. Connectez-vous à l'interface Web CMM à l'aide de vos données d'identification utilisateur XClarity Administrator.

Modification des propriétés système pour un châssis

Vous pouvez modifier les propriétés système d'un châssis spécifique.

Procédure

Procédez comme suit pour modifier les propriétés système :

Etape 1. Dans la barre de menu Lenovo XClarity Administrator, cliquez sur **Matériel → Châssis** pour afficher la page Châssis.

Etape 2. Sélectionnez le châssis à mettre à jour.

Etape 3. Cliquez sur **Toutes les actions → Inventaire → Éditer les propriétés** pour afficher la boîte de dialogue Éditer.

Etape 4. Modifiez les informations suivantes, si nécessaire.
- Nom du serveur
- Contact pour support technique
- Description

Remarque : Les propriétés d'emplacement, de pièce, d'armoire et d'unité d'armoire la plus basse sont mises à jour par XClarity Administrator lorsque vous ajoutez ou retirez des appareils dans une armoire dans l'interface Web (voir Gestion des armoires).

Etape 5. Cliquez sur **Enregistrer**.

Remarque : Si vous modifiez ces propriétés, vous devrez peut-être attendre quelques instants avant que les modifications n'apparaissent dans l'interface Web XClarity Administrator.

Modification des paramètres IP de gestion pour un châssis

Vous pouvez modifier les paramètres IP de gestion pour l'ensemble du châssis, y compris les nœuds de traitement, les dispositifs de stockage et Commutateurs Flex.

Procédure

Procédez comme suit pour modifier les paramètres IP de gestion.

Etape 1. Dans la barre de menu Lenovo XClarity Administrator, cliquez sur **Matériel → Châssis** pour afficher la page Châssis.

Etape 2. Sélectionnez le châssis.

Etape 3. Cliquez sur **Toutes les actions → Inventaire → Éditer les adresses IP de gestion** pour afficher la page des paramètres IP du châssis et des composants.

Etape 4. Modifiez les paramètres globaux suivants, si nécessaire.

- Choisissez d'activer ou de désactiver les adresses IPv4.

  Si vous activez les adresses IPv4, indiquez les paramètres suivants. Les paramètres globaux IPv4 sont appliqués à un composant lorsque son adresse IPv4 est mise à jour.
  - (Facultatif) Choisissez d'obtenir les adresses IP à l'aide d'adresses IP affectées de manière statique.
  - Spécifiez le masque de sous-réseau et l'adresse de passerelle.
- Spécifiez les paramètres suivants pour les adresses IPv6. Les paramètres globaux IPv6 sont appliqués à un composant lorsque son adresse IPv6 est mise à jour.
  - (Facultatif) Choisissez d'obtenir les adresses IP à l'aide d'adresses IP affectées de manière statique.

    Si des adresses IP statiques sont utilisées, vous pouvez également choisir d'utiliser la configuration automatique des adresses IP sans état et la configuration des adresses IP avec état.
  - Spécifiez la longueur de préfixe et l'adresse de passerelle.
- Choisissez d'activer ou de désactiver des serveurs DNS.

  Si vous activez les serveurs DNS :
  - Choisissez la préférence de recherche du serveur DNS.
  - Entrez les adresses IP à utiliser pour l'ordre de recherche DNS.
  - Entrez le nom de domaine.

Etape 5. Modifiez les paramètres IP CMM suivants.

- Entrez le nom d'hôte et l'adresse IP du CMM.
- Cliquez sur **Générer automatiquement des adresses IP** pour créer des adresses IP pour les nœuds de traitement, les dispositifs de stockage et Commutateurs Flex avec l'adresse IP CMM comme point de départ.

Etape 6. Entrez le nom d'hôte et les adresses IP pour chaque nœud de traitement dans le châssis

Etape 7. Entrez le nom d'hôte et les adresses IP pour chaque dispositif de stockage dans le châssis.

Etape 8. Entrez les adresses IP pour chaque Commutateur Flex dans le châssis.

Etape 9. Cliquez sur **Enregistrer**. Une boîte de dialogue s'affiche avec un récapitulatif des paramètres réseau.

Etape 10. Cliquez sur **Appliquer**.

Tous les composants existants dans le châssis sont mis à jour avec les paramètres globaux spécifiés. Lorsque la mise à jour est terminée, la boîte de dialogue affiche les paramètres qui ont été modifiés.

Remarque : Si vous modifiez ces informations, vous devrez peut-être attendre quelques instants avant que les informations s'affichent dans l'interface Lenovo XClarity Administrator.

Etape 11. Cliquez sur **Fermer**.

Configuration du basculement CMM

Lorsque vous installez un deuxième CMM dans un châssis, il est automatiquement configuré en tant que module CMM de secours par défaut. Si le module CMM principal échoue, l'adresse IP du module CMM de secours passe à la même adresse IP que celle utilisée pour le module CMM principal, et le module CMM de secours reprend la gestion du châssis. Cependant, vous pouvez effectuer une configuration plus avancée du basculement à partir de l'interface Web du contrôleur de gestion pour le châssis.

À propos de cette tâche

Par exemple, vous pouvez choisir de :

- Désactiver l'interface réseau pour le module CMM de secours afin d'éviter le basculement.
- Activer l'interface réseau pour le module CMM de secours et autoriser la permutation des adresses IP entre les deux modules CMM pendant le basculement.
- Activer l'interface réseau pour le module CMM de secours et empêcher la permutation des adresses IP entre les deux modules CMM pendant le basculement.

Pour plus d'informations sur les fonctions de basculement avancé de module CMM, voir Commande advfailover dans la documentation en ligne du module CMM.

Procédure

Pour activer l'adresse IP permutable des modules CMM principal et de secours, procédez comme suit.

Etape 1. Dans l'interface Web du contrôleur de gestion pour le châssis, cliquez sur **Gestion du module de gestion → Réseau → Ethernet** pour afficher la page de configuration Ethernet.

Etape 2. Sélectionnez **IPv4** ou **IPv6** pour votre système.

Etape 3. Sous **Configurer une adresse IP**, sélectionnez l'option permettant d'utiliser une adresse IP statique. Répétez l'opération pour l'autre protocole.

Etape 4. Cliquez sur **Gestion du module de gestion → Propriétés → Basculement avancé** et activez l'option de basculement avancé.

Etape 5. Sélectionnez **Échanger l'adresse IP du module de gestion**.

Etape 6. Exécutez les scénarios de test pour vérifier que le basculement fonctionne correctement et que Lenovo XClarity Administrator peut se connecter aux modules CMM principal et de sauvegarde.

Redémarrage d'un module CMM

Vous pouvez redémarrer un module Chassis Management Module (CMM) à partir de Lenovo XClarity Administrator.

Procédure

Procédez comme suit pour redémarrer un châssis.

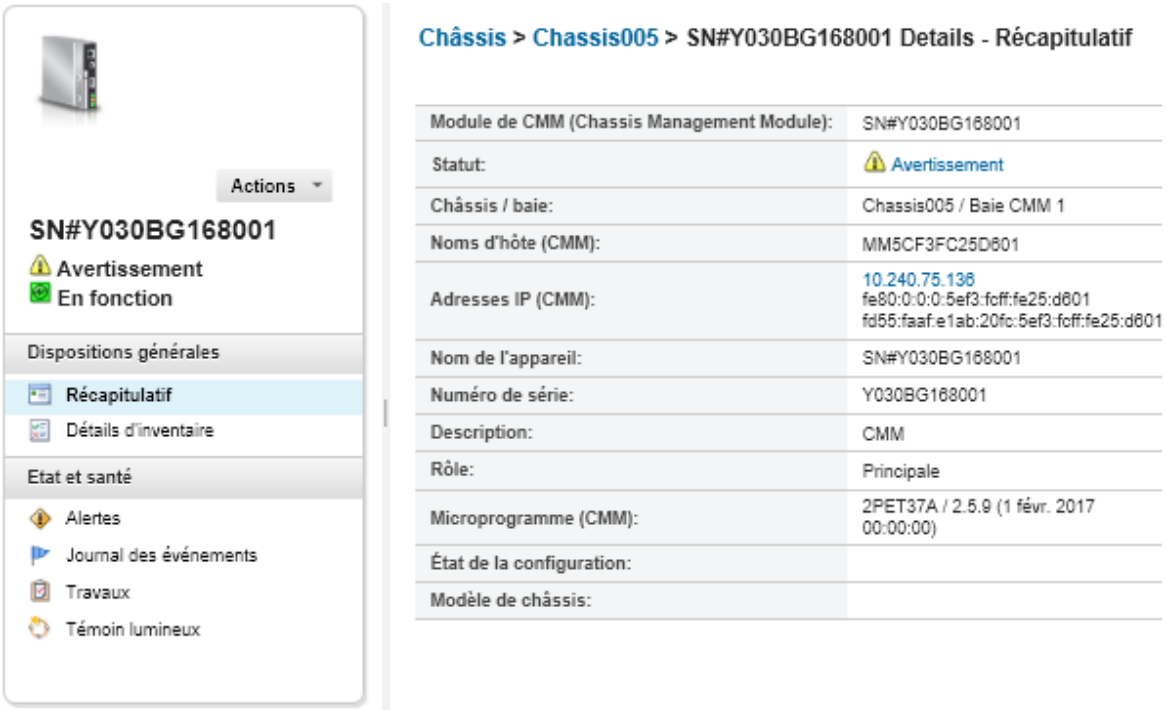
Remarque : Une fois le module CMM redémarré, toutes les connexions réseau existantes au module CMM seront temporairement perdues.

Etape 1. Dans le menu XClarity Administrator, cliquez sur **Matériel → Châssis**. La page Châssis s'affiche avec une vue tabulaire de tous les châssis gérés.

Etape 2. Cliquez sur le nom du châssis dans la colonne **Châssis** pour afficher la vue graphique du châssis.

Etape 3. Cliquez sur le graphique du module CMM pour l'afficher sur la page Récapitulatif CMM.

Conseil : vous pouvez également cliquer sur **Vue tabulaire**, puis cliquer sur le nom du module CMM dans la colonne **Nom** pour afficher la page Récapitulatif CMM.



Etape 4. Cliquez **Actions → Actions d'alimentation → Redémarrer**.

Etape 5. Cliquez sur **Redémarrer immédiatement**.

L'exécution de cette opération peut durer quelques minutes et vous devrez peut-être actualiser la page pour afficher les résultats.

Réinstallation virtuelle d'un module CMM

Vous pouvez simuler le retrait et la réinstallation d'un module Chassis Management Module (CMM) dans un châssis,

À propos de cette tâche

Au cours de la réinstallation virtuelle, toutes les connexions réseau existantes au module CMM sont perdues et l'état d'alimentation du module CMM change.

Attention : Avant d'effectuer une réinstallation virtuelle, assurez-vous d'avoir sauvegardé toutes les données utilisateur sur le module CMM.

Procédure

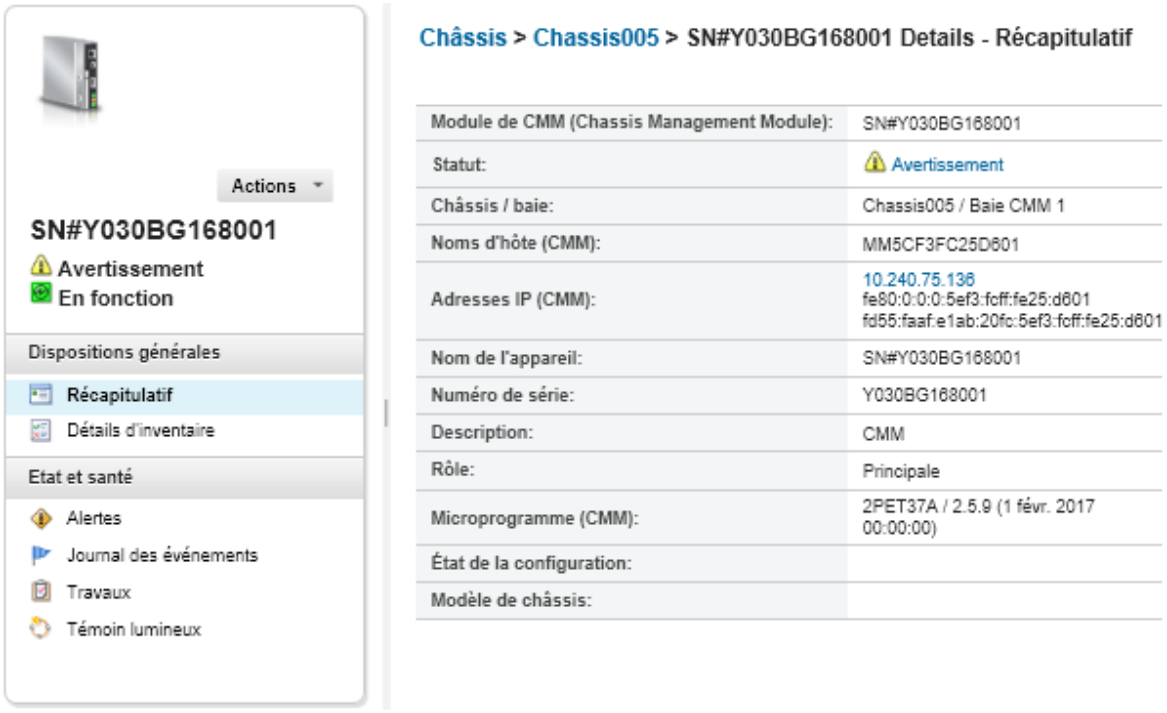
Procédez comme suit pour réinstaller virtuellement un module CMM.

Etape 1. Dans le menu Lenovo XClarity Administrator, cliquez sur **Matériel → Châssis**. La page Châssis s'affiche avec une vue tabulaire de tous les châssis gérés.

Etape 2. Cliquez sur le nom du châssis dans la colonne **Châssis** pour afficher la vue graphique du châssis.

Etape 3. Cliquez sur le graphique du module CMM pour l'afficher sur la page Récapitulatif CMM.

Conseil : vous pouvez également cliquer sur **Vue tabulaire**, puis cliquer sur le nom du module CMM dans la colonne **Nom** pour afficher la page Récapitulatif CMM.



Etape 4. Cliquez sur **Actions → Service → Réinstallation virtuelle**.

Etape 5. Cliquez sur **Réinstallation virtuelle**.

Résolution de données d'identification expirées ou non valides pour un châssis

Lorsqu'une des données d'identification stockées expirent ou deviennent inopérantes sur un appareil, le statut de cet appareil apparaît comme « Hors ligne. »

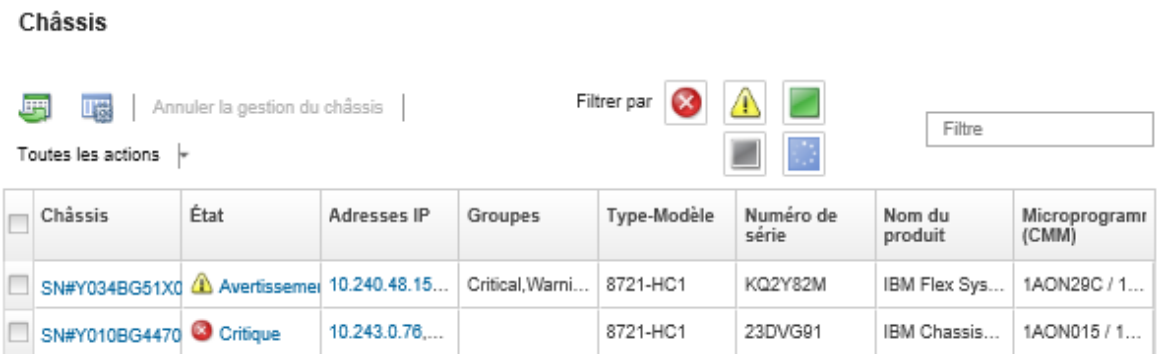
Procédure

Pour résoudre des données d'identification expirées ou non valides pour un châssis.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Matériel → Châssis**. La page Châssis s'affiche avec une vue tabulaire de tous les châssis gérés.

Etape 2. Cliquez sur l'en-tête de colonne **Alimentation** pour grouper tous les châssis hors ligne en haut de la table.

Vous pouvez trier les colonnes du tableau pour trouver plus facilement le châssis que vous souhaitez gérer. En outre, vous pouvez entrer du texte (comme un nom de châssis ou une adresse IP) dans le champ **Filtre** pour filtrer davantage les châssis affichés.



Etape 3. Sélectionnez le châssis à résoudre.

Etape 4. Cliquez sur **Toutes les actions → Sécurité → Éditer les données d'identification stockées**.

Etape 5. Changez le mot de passe des données d'identification stockées ou sélectionnez d'autres données d'identification stockées à utiliser pour cet appareil géré.

Remarque : Si vous avez géré plusieurs appareils à l'aide des mêmes données d'identification stockées et si vous modifiez le mot de passe des données d'identification stockées, ce changement de mot de passe affecte tous les dispositifs qui utilisent actuellement les données d'identification stockées.

Reprise de la gestion avec un module CMM après une défaillance du serveur de gestion

Si un châssis est géré par Lenovo XClarity Administrator et que XClarity Administrator rencontre une défaillance, vous pouvez restaurer les fonctions de gestion et les comptes utilisateur locaux pour un module Module CMM jusqu'à ce que le nœud de gestion soit restauré ou remplacé.

Procédure

Suivez l'une des procédures suivantes pour restaurer la gestion sur un module CMM.

- Si l'instance de remplacement de XClarity Administrator utilise la même adresse IP que l'instance de XClarity Administrator ayant rencontré une défaillance, gérez à nouveau le dispositif à l'aide du compte et du mot de passe RECOVERY_ID et de l'option **Forcer la gestion** (voir Gestion des châssis).
- Réinitialisez le module CMM aux paramètres d'usine par défaut en enfonçant un trombone pendant au moins 10 secondes dans le bouton de réinitialisation sur le module CMM. Pour plus d'informations sur la réinitialisation du module CMM, avec notamment des consignes importantes, voir Réinitialisation CMM dans la documentation enligne Flex Systems.
- Restaurez la configuration du module CMM comme suit :
  1. Via une session SSH, ouvrez une interface de ligne de commande de gestion pour le châssis et connectez-vous avec le compte `RECOVERY_ID`.

     Remarque : Le mot de passe du compte `RECOVERY_ID` a été défini lorsque vous avez sélectionné le châssis pour la gestion sur la page du domaine de gestion. Pour plus d'informations sur la gestion de compte centrale, voir Gestion des châssis.

     Si vous utilisez le compte `RECOVERY_ID` pour la première fois afin de vous connecter au Module CMM, vous devez modifier le mot de passe.
  2. Lorsque vous y êtes invité, entrez le nouveau mot de passe du compte `RECOVERY_ID`.
  3. Restaurez la configuration du module CMM en effectuant l'une des étapes suivantes :
     - Si vous exécutez une version de microprogramme du module CMM de juin 2015 ou ultérieure, exécutez la commande suivante :

`read -f unmanage -T mm[p]`
Pour plus d'informations, voir le document Commande read dans la documentation en ligne du module CMM.

– Si vous exécutez une version de microprogramme du module CMM antérieure à juin 2015, exécutez les commandes suivantes dans l'ordre indiqué :

  a. `env -T mm[p]`
  b. `sslcfg -client disabled -tc1 remove`
  c. `accseccfg -am local`
  d. `ldapcfg -i1 -p1 -rd "" -usa "" -gsa "" -lpa ""`
  e. `ntp -en disabled -i 0.0.0.0 -v3en disabled`
  f. `cimsub -clear all`
  g. `fsmcm -off`

     La commande `fsmcm` désactive la gestion du compte utilisateur XClarity Administrator et vous permet d'utiliser des comptes utilisateur Module CMM locaux pour vous authentifier sur le Module CMM et sur tout processeur de gestion installé dans le châssis.

     Après l'exécution de la commande `fsmcm -off`, le compte `RECOVERY_ID` est supprimé du registre d'utilisateurs du Module CMM. Lorsque vous exécutez la commande `fsmcm -off`, la session CLI Module CMM se termine. Vous pouvez maintenant vous authentifier auprès du module Module CMM et des autres composants du châssis à l'aide des données d'identification du module Module CMM locales, et utiliser ces dernières pour accéder à l'interface Web CMM ou à l'interface de ligne de commande du module Module CMM jusqu'à ce que le mode de gestion des utilisateurs soit restauré par XClarity Administrator.

     Pour plus d'informations, voir le document Commande fsmcm dans la documentation en ligne du module CMM.

Après la restauration ou le remplacement de XClarity Administrator, vous pouvez gérer à nouveau le châssis (voir Gestion des châssis). Toutes les informations sur le châssis (comme les paramètres réseau) sont conservées.

Désactivation de la gestion d'un châssis

Vous pouvez retirer un châssis de la gestion par Lenovo XClarity Administrator. Ce processus est appelé *annulation de la gestion.* Lorsque la gestion d'un châssis est annulée, vous pouvez vous connecter au module CMM du châssis à l'aide des comptes utilisateur CMM locaux.

Avant de commencer

Vous pouvez activer XClarity Administrator pour annuler automatiquement la gestion des appareils qui sont hors ligne pendant une durée spécifique. Cette option est désactivée par défaut. Pour activer l'annulation de la gestion automatique des appareils hors ligne, cliquez sur **Matériel → Reconnaître et gérer de nouveaux appareils** dans le menu XClarity Administrator, puis cliquez sur **Éditer** en regard de **Annuler la gestion des appareils hors ligne correspond à : Désactivé**. Ensuite, sélectionnez **Activer l'option Annuler la gestion des appareils hors ligne** et définissez l'intervalle de temps. Par défaut, la gestion des appareils est annulée lorsque ceux-ci sont hors ligne pendant 24 heures.

Avant d'annuler la gestion d'un châssis, vérifiez qu'il n'existe pas de travaux actifs en cours d'exécution sur les dispositifs installés dans le châssis.

Lorsque l'Appel vers Lenovo est activé dans XClarity Administrator, l'Appel vers Lenovo est désactivé sur tous les châssis et serveurs gérés afin d'éviter de générer des enregistrements de problème en double. Si vous prévoyez de cesser d'utiliser XClarity Administrator pour gérer vos appareils, vous pouvez réactiver

l'Appel vers Lenovo sur tous les appareils gérés à partir de XClarity Administrator au lieu de réactiver ultérieurement l'Appel vers Lenovo pour chaque appareil géré individuel (voir Réactivation de l'appel vers Lenovo sur tous les appareils gérés dans la documentation en ligne de XClarity Administrator).

À propos de cette tâche

Lorsque vous annulez la gestion d'un châssis, XClarity Administrator exécute les actions suivantes :

- Efface la configuration utilisée pour la gestion centralisée des utilisateurs.
- Supprime le certificat de sécurité CMM à partir du fichier de clés certifiées XClarity Administrator.
- Si Encapsulation est activé sur le dispositif, il configure les règles de pare-feu des dispositifs sur les paramètres avant la gestion du dispositif.
- Supprime l'accès au serveur NTP à partir du module CMM.
- Supprime les souscriptions CIM sur le module CMM à partir de la configuration XClarity Administrator de sorte que XClarity Administrator ne reçoit plus d'événements à partir de ce châssis.

Lorsque vous avez annulé la gestion d'un châssis, XClarity Administrator conserve certaines informations sur le châssis. Ces informations sont réappliquées lorsque vous gérez à nouveau le même châssis.

Lorsque vous annulez la gestion d'un châssis, des événements envoyés à partir des composants du châssis sont ignorés. Vous pouvez conserver ces événements en transmettant les événements dans un référentiel externe, tel qu'un syslog (voir Acheminement des événements).

Astuce : Tous les appareils de démonstration qui sont éventuellement ajoutés lors de la configuration initiale sont des nœuds dans un châssis. Pour annuler la gestion des appareils de démonstration, annulez la gestion du châssis à l'aide de l'option **Forcer l'annulation de la gestion, même si l'appareil est inaccessible**.

Procédure

Pour annuler la gestion d'un châssis, procédez comme suit :

Etape 1. Dans la barre de menu XClarity Administrator, cliquez sur **Matériel → Châssis** pour afficher la page Châssis.

Etape 2. Sélectionnez un ou plusieurs châssis des listes de châssis gérés.

Etape 3. Cliquez sur **Annuler la gestion du châssis**. Le dialogue Annuler la gestion s'affiche.

Etape 4. **Facultatif :** sélectionnez **Forcer l'annulation de la gestion, même si l'appareil est inaccessible**.

Important : Lors de l'annulation de la gestion du matériel de démonstration, veillez à sélectionner cette option.

Etape 5. Cliquez sur **Annuler la gestion**.La boîte de dialogue Annuler la gestion affiche la progression de chaque étape dans le processus d'annulation de gestion.

Etape 6. Une fois le processus d'annulation de gestion terminé, cliquez sur **OK**.

Après avoir terminé

Lorsque le processus d'annulation de gestion est terminé, vous pouvez vous connecter au module CMM à l'aide des comptes utilisateur CMM locaux. Si vous ne vous souvenez pas des noms d'utilisateur ou des mots de passe des comptes utilisateur CMM locaux, réinitialisez le module CMM sur les paramètres d'usine par défaut afin de vous connecter au module CMM. Pour plus d'informations sur la réinitialisation du module CMM aux paramètres d'usine par défaut, voir Réinitialisation CMM dans la documentation enligne Flex Systems dans la documentation produit CMM.

Restauration d'un châssis dont la gestion n'a pas été correctement annulée

Si la gestion d'un châssis n'a pas été correctement annulée, vous devez restaurer ce châssis pour pouvoir le gérer à nouveau.

Procédure

Suivez l'une des procédures suivantes pour restaurer la gestion sur un module CMM.

- Si l'instance de remplacement de XClarity Administrator utilise la même adresse IP que l'instance de XClarity Administrator ayant rencontré une défaillance, gérez à nouveau le dispositif à l'aide du compte et du mot de passe RECOVERY_ID et de l'option **Forcer la gestion** (voir Gestion des châssis).
- Réinitialisez le module CMM aux paramètres d'usine par défaut en enfonçant un trombone pendant au moins 10 secondes dans le bouton de réinitialisation sur le module CMM. Pour plus d'informations sur la réinitialisation du module CMM, avec notamment des consignes importantes, voir Réinitialisation CMM dans la documentation enligne Flex Systems.
- Restaurez la configuration du module CMM comme suit :
  1. Via une session SSH, ouvrez une interface de ligne de commande de gestion pour le châssis et connectez-vous avec le compte `RECOVERY_ID`.

     Remarque : Le mot de passe du compte `RECOVERY_ID` a été défini lorsque vous avez sélectionné le châssis pour la gestion sur la page du domaine de gestion. Pour plus d'informations sur la gestion de compte centrale, voir Gestion des châssis.

     Si vous utilisez le compte `RECOVERY_ID` pour la première fois afin de vous connecter au Module CMM, vous devez modifier le mot de passe.
  2. Lorsque vous y êtes invité, entrez le nouveau mot de passe du compte `RECOVERY_ID`.
  3. Restaurez la configuration du module CMM en effectuant l'une des étapes suivantes :
     - Si vous exécutez une version de microprogramme du module CMM de juin 2015 ou ultérieure, exécutez la commande suivante :
       ```
       read -f unmanage -T mm[p]
       ```
       Pour plus d'informations, voir le document Commande read dans la documentation en ligne du module CMM.
     - Si vous exécutez une version de microprogramme du module CMM antérieure à juin 2015, exécutez les commandes suivantes dans l'ordre indiqué :
       a. `env -T mm[p]`
       b. `sslcfg -client disabled -tc1 remove`
       c. `accseccfg -am local`
       d. `ldapcfg -i1 -p1 -rd "" -usa "" -gsa "" -lpa ""`
       e. `ntp -en disabled -i 0.0.0.0 -v3en disabled`
       f. `cimsub -clear all`
       g. `fsmcm -off`

          La commande `fsmcm` désactive la gestion du compte utilisateur XClarity Administrator et vous permet d'utiliser des comptes utilisateur Module CMM locaux pour vous authentifier sur le Module CMM et sur tout processeur de gestion installé dans le châssis.

          Après l'exécution de la commande `fsmcm -off`, le compte `RECOVERY_ID` est supprimé du registre d'utilisateurs du Module CMM. Lorsque vous exécutez la commande `fsmcm -off`, la session CLI Module CMM se termine. Vous pouvez maintenant vous authentifier auprès du module Module CMM et des autres composants du châssis à l'aide des données d'identification du

module Module CMM locales, et utiliser ces dernières pour accéder à l'interface Web CMM ou à l'interface de ligne de commande du module Module CMM jusqu'à ce que le mode de gestion des utilisateurs soit restauré par XClarity Administrator.

Pour plus d'informations, voir le document Commande fsmcm dans la documentation en ligne du module CMM.

Après la restauration ou le remplacement de XClarity Administrator, vous pouvez gérer à nouveau le châssis (voir Gestion des châssis). Toutes les informations sur le châssis (comme les paramètres réseau) sont conservées.

Chapitre 8. Gestion des serveurs

Lenovo XClarity Administrator peut gérer plusieurs types de systèmes, notamment les serveurs ThinkAgile, ThinkSystem, Converged, Flex System, NeXtScale, System x® et ThinkServer®.

En savoir plus :  XClarity Administrator : Reconnaissance

Avant de commencer

Remarque : Les nœuds de traitement Flex sont automatiquement reconnus et gérés lorsque vous gérez le châssis dans lequel ils se trouvent. Vous ne pouvez pas reconnaître et gérer les nœuds de traitement Flex indépendants du châssis.

Avant de gérer des serveurs, vérifiez que les conditions suivantes sont remplies :

- Consultez les instructions de gestion avant de gérer un dispositif. Pour plus d'informations, voir Considérations relatives à la gestion dans la documentation en ligne XClarity Administrator.
- Certains ports doivent être disponibles pour communiquer avec des appareils. Vérifiez que tous les ports requis sont disponibles avant de tenter de gérer des serveurs. Pour plus d'informations sur les ports, voir Disponibilité de port dans la documentation en ligne de XClarity Administrator.
- Vérifiez que le microprogramme minimal requis est installé sur chaque serveur que vous souhaitez gérer à l'aide de XClarity Administrator. Vous pouvez rechercher les niveaux de microprogramme minimum requis par la Support de XClarity Administrator – Page Web de compatibilité en cliquant sur l'onglet **Compatibilité**, puis en cliquant sur le lien des types d'appareil appropriés.
- Assurez-vous que CIM via HTTPS est activé sur l'appareil.
  1. Connectez-vous à l'interface Web de gestion du serveur avec le compte utilisateur `RECOVERY_ID`.
  2. Cliquez sur **Gestion IMM → Sécurité**.
  3. Cliquez sur l'onglet **CIM Over HTTPS** et vérifiez que **Activer CIM sur HTTPS** est sélectionné.
- Pour les serveurs ThinkSystem SR635 et SR655 :
  - Assurez-vous qu'un système d'exploitation est installé et que le serveur a été démarré sur le SE, qu'un support amorçable a été monté ou efishell au moins une fois, de sorte que XClarity Administrator puisse collecter l'inventaire pour ces serveurs.
  - Assurez-vous que IPMI sur LAN est activée. L'interface IPMI sur réseau local est désactivée par défaut sur ces serveurs et doit être activée manuellement pour que ces derniers puissent être gérés. Pour activer l'interface IPMI sur réseau local à l'aide de TSM, cliquez sur **Paramètres → Configuration IPMI**. Vous devrez peut-être redémarrer le serveur pour activer cette modification.
- Si le certificat de serveur de l'appareil est signé par une autorité de certification externe, assurez-vous que le certificat de l'autorité de certification et tous les certificats intermédiaires sont importés dans leXClarity Administratorfichier de clés certifiées (voir Déploiement de certificats de serveur personnalisé sur des appareils gérés).
- Pour identifier un serveur qui se trouve sur un sous-réseau *différent* de XClarity Administrator, veillez à ce que l'une des conditions suivantes soit remplie :
  - Veillez à activer la transmission SLP multidiffusion sur les commutateurs de la partie supérieure de l'armoire, ainsi que les routeurs de votre environnement. Consultez la documentation fournie avec votre routeur ou commutateur spécifique afin de déterminer si la transmission SLP multidiffusion est activée et de prendre connaissance des procédures permettant de l'activer si elle est désactivée.
  - Si le protocole SLP est désactivé sur le point de terminaison ou sur le réseau, vous pouvez utiliser à la place la méthode de détection DNS en ajoutant manuellement un enregistrement de service

(enregistrement SRV) à votre serveur de noms de domaine (DNS), pour XClarity Administrator par exemple
`_lxca._tcp.labs.lenovo.com  service = 0 0 443 fvt-xhmc3.labs.lenovo.com.`

Activez ensuite la reconnaissance DNS sur la console de gestion de la carte mère à partir de l'interface Web de gestion en cliquant sur **Gestion IMM → Protocole réseau**, sur l'onglet **DNS**, puis en sélectionnant **Utiliser DNS pour reconnaîtreLenovo XClarity Administrator**.

Remarques :

- Le contrôleur de gestion doit exécuter un niveau de microprogramme datant de mai 2017 ou d'une date ultérieure pour prendre en charge la reconnaissance automatique via DNS.
- S'il existe plusieurs instances XClarity Administrator dans votre environnement, le serveur est uniquement reconnu par la première instance à répondre à la demande de reconnaissance. Le serveur n'est pas reconnu par toutes les instances.

- Pour reconnaître et gérer les serveurs ThinkServer, vérifiez que les conditions suivantes sont remplies. Pour plus d'informations, voir Impossible de reconnaître un appareil et Impossible de gérer un appareil dans la documentation en ligne de XClarity Administrator.
  - Le nom d'hôte du serveur doit être configuré à l'aide d'un nom d'hôte ou d'une adresse IP valide si vous voulez que XClarity Administrator reconnaisse automatiquement les serveurs.
  - La configuration réseau doit autoriser le trafic SLP entre XClarity Administrator et le serveur.
  - Protocole SLP monodiffusion est requis.
  - Si vous voulez que XClarity Administrator reconnaisse automatiquement les serveurs ThinkServer, le protocole SLP multidiffusion est requis. De plus, le protocole SLP doit être activé sur ThinkServer System Manager (TSM).
  - Si les serveurs ThinkServer se trouvent sur un réseau autre que XClarity Administrator, vérifiez que ce réseau est configuré pour autoriser le trafic UDP entrant via le port 162 afin que XClarity Administrator puisse recevoir des événements pour ces appareils.
- Pour ThinkAgile, ThinkSystem, Converged, Flex System. NeXtScale et System x, si vous retirez, remplacez ou configurez des adaptateurs sur le serveur, redémarrez le serveur au moins une fois pour mettre à jour les informations relatives au nouvel adaptateur dans le contrôleur de gestion de la carte mère et les rapports XClarity Administrator (Mise sous tension et hors tension d'un serveur).
- Lorsque vous effectuez des actions de gestion sur un serveur, assurez-vous que le serveur est mis hors tension ou mis sous tension sur la configuration BIOS/UEFI ou sur un système d'exploitation en cours d'exécution. (Vous pouvez amorcer la configuration BIOS/UEFI à partir de la page Serveurs dans XClarity Administrator en cliquant sur **Toutes les actions → Actions d'alimentation → Redémarrer sur la configuration BIOS/UEFI**.) Si le serveur est mis sous tension sans système d'exploitation, le contrôleur de gestion réinitialise le serveur en continu pour tenter de trouver un système d'exploitation.
- Vérifiez que tous les paramètres `UEFI_Ethernet_*` et `UEFI_Slot_*` sont activés dans les paramètres UEFI du serveur. Pour vérifier les paramètres, redémarrez le serveur et, lorsque l'invite `<F1> Setup` s'affiche, appuyez sur `F1` pour démarrer l'utilitaire Setup Utility. Accédez à **System Settings → Devices and I/O Ports → Enable/Disable Adapter Option ROM Support**, puis localisez la section **Enable/Disable UEFI Option ROM(s)** pour vérifier que les paramètres sont activés.

  Remarque : Si la fonctionnalité Console distante est prise en charge, vous pouvez également l'utiliser dans l'interface de gestion de la carte mère pour consulter et modifier les paramètres à distance.
- Les serveurs System x3950 X6 doivent être gérés en tant que deux boîtiers 4U, chacun avec son propre contrôleur de gestion de la carte mère.

À propos de cette tâche

XClarity Administrator peut détecter automatiquement des serveurs au format tour et rack dans votre environnement en sondant les dispositifs gérables présents dans le même sous-réseau IP que XClarity Administrator. Pour reconnaître les serveurs au format tour et rack qui se trouvent dans d'autres sous-réseaux, définissez une adresse IP ou une plage d'adresses IP, ou importez les informations à partir d'un tableur.

Important : Pour les serveurs System x3850 et x3950 X6, vous devez gérer chaque serveur dans l'environnement rack évolutif.

Une fois que les serveurs sont gérés par XClarity Administrator, Lenovo XClarity Administrator interroge régulièrement chaque serveur géré afin de collecter des informations, telles que l'inventaire, les données techniques essentielles et l'état. Vous pouvez afficher et surveiller chaque serveur géré et effectuer des tâches de gestion (telles que la configuration des paramètres système, le déploiement d'images du système d'exploitation, ainsi que la mise sous tension et hors tension).

Par défaut, les appareils sont gérés par XClarity Administrator authentification gérée pour la connexion aux appareils. Lors de la gestion de serveurs rack et de châssis Lenovo, vous pouvez choisir d'utiliser l'authentification locale ou l'authentification gérée pour vous connecter aux appareils.

- Lorsque l'*authentification locale* est utilisée pour les serveurs rack, les châssis Lenovo et les commutateurs d'armoire, XClarity Administrator utilise des données d'identification stockées pour l'authentification sur l'appareil. Les *données d'identification stockées* peuvent être un compte utilisateur actif sur l'appareil ou un compte utilisateur dans un serveur Active Directory.

  Vous devez créer des données d’identification stockées dans XClarity Administrator qui correspondent à un compte utilisateur active sur l’appareil ou un compte utilisateur dans un serveur Active Directory avant de gérer l’appareil à l’aide de l’authentification locale (voir Gestion de données d'identification stockées dans la documentation en ligne XClarity Administrator).

  Remarques :

  – Les appareils RackSwitch prennent en charge uniquement les données d'identification stockées pour l'authentification. Les données d'identification utilisateur XClarity Administrator stockées ne sont pas prises en charge.
- L'*authentification gérée* vous permet de gérer et de surveiller plusieurs appareils à l’aide des données d’identification dans le serveur d’authentification XClarity Administrator au lieu des données d’identification locales. Lorsqu'un appareil (autre que des serveurs ThinkServer, System x M4 et des commutateurs) est géré par authentification gérée, XClarity Administrator configure l'appareil géré et ses composants installés afin d'utiliser le serveur d'authentification XClarity Administrator pour la gestion centralisée.

  – Lorsque l’authentification gérée est activée, vous pouvez gérer des appareils à l’aide de saisies manuelles ou de données d’identification stockées (voir Gestion des comptes utilisateur et dans la documentation en ligne de XClarity Administrator).

    Les données d’identification stockées sont utilisées uniquement jusqu’à ce que XClarity Administrator configure les paramètres LDAP sur l’appareil. Ensuite, toute modification apportée aux données d’identification stockées n’a aucun impact sur la gestion ou la surveillance de cet appareil.

    Remarque : Lorsque l’authentification gérée est activée pour un appareil, vous ne pouvez pas modifier les données d’identification stockées pour cet appareil à l’aide de XClarity Administrator.

  – Si un serveur LDAP local ou externe est utilisé comme serveur d'authentification XClarity Administrator, les comptes utilisateur définis dans le serveur d'authentification sont utilisés pour se connecter à XClarity Administrator, aux modules CMM et aux contrôleurs de gestion de la carte mère dans le domaine XClarity Administrator. Les CMM locaux et les comptes utilisateur du contrôleur de gestion sont désactivés.

- Si un fournisseur d'identité SAML 2.0 est utilisé comme serveur d'authentification XClarity Administrator, les comptes SAML ne sont pas accessibles pour les appareils gérés. Cependant, lorsque vous utilisez un fournisseur d'identité SAML et un serveur LDAP ensemble et que le fournisseur d'identité utilise des comptes qui existent dans le serveur LDAP, les comptes utilisateur LDAP peuvent être utilisés pour se connecter à des appareils gérés, tandis que des méthodes d'authentification plus avancées qui sont fournies par SAML 2.0 (comme l'authentification à plusieurs facteurs et la connexion unique) peuvent être utilisées pour la connexion à XClarity Administrator.
- L'authentification unique permet à un utilisateur qui est déjà connecté à XClarity Administrator de se connecter automatiquement au contrôle de gestion de la carte mère. La connexion unique est activée par défaut lorsqu'un serveur ThinkSystem ou ThinkAgile est amené dans la gestion par XClarity Administrator (sauf si le serveur est géré avec des mots de passe CyberArk). Vous pouvez configurer le paramètre global pour activer ou désactiver la connexion unique pour tous les serveurs ThinkSystem et ThinkAgile gérés. L'activation de la connexion unique pour un serveur ThinkSystem et ThinkAgile remplace le paramétrage global pour tous les serveurs ThinkSystem et ThinkAgile (voir).

  Remarque : La connexion unique est automatiquement désactivée lorsque vous faites appel au système de gestion d'identité CyberArk pour vous connecter.
- Lorsque l'authentification gérée est activée pour les serveurs ThinkSystem SR635 et SR655 :
  - Le microprogramme du contrôleur de gestion de la carte mère prend en charge jusqu'à cinq rôles utilisateur LDAP. XClarity Administrator ajoute ces rôles utilisateur LDAP aux serveurs lors de la gestion : **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin** et **lxc-os-admin**.

    Les utilisateurs doivent être affectés à au moins l'un des rôles utilisateur LDAP spécifiés pour pouvoir communiquer avec les serveurs ThinkSystem SR635 et SR655.
  - Le microprogramme du contrôleur de gestion ne prend pas en charge les utilisateurs LDAP dont le nom d'utilisateur est identique à celui de l'utilisateur local du serveur.
- Pour les serveurs ThinkServer et System x M4, le serveur d'authentification XClarity Administrator n'est pas utilisé. À la place, un compte IPMI est créé sur l'appareil avec le préfixe « LXCA_ » suivi d'une chaîne aléatoire. (Les comptes utilisateur IPMI locaux ne sont pas désactivés.) Lorsque vous annulez la gestion d'un serveur ThinkServer, le compte utilisateur « LXCA_ » est désactivé, et le préfixe « LXCA_ » est remplacé par le préfixe « DISABLED_ ». Pour déterminer si un serveur ThinkServer est géré par une autre instance, XClarity Administrator recherche les comptes IPMI ayant le préfixe « LXCA_ ». Si vous choisissez de forcer la gestion d'un serveur ThinkServer géré, tous les comptes IPMI sur l'appareil avec le préfixe « LXCA_ » sont désactivés et renommés. Pensez à supprimer manuellement les comptes IPMI qui ne sont plus utilisés.

  Si vous utilisez des données d'identification saisies manuellement, XClarity Administrator crée automatiquement des données d'identification stockées et utilise ces dernières pour gérer l'appareil.

  Remarques : Lorsque l'authentification gérée est activée pour un appareil, vous ne pouvez pas modifier les données d'identification stockées pour cet appareil à l'aide de XClarity Administrator.
  - Chaque fois que vous gérez un appareil en utilisant des données d'identification saisies manuellement, de nouvelles données d'identification stockées sont créées pour cet appareil, même si d'autres données d'identification stockées ont été créées pour cet appareil lors d'un processus de gestion précédent.
  - Lorsque vous annulez la gestion d'un appareil, XClarity Administrator ne supprime pas les données d'identification stockées qui ont été créées automatiquement pour cet appareil lors du processus de gestion.

Un dispositif peut être géré par une seule instance XClarity Administrator à la fois. La gestion par plusieurs instances de XClarity Administrator n'est pas prise en charge. Si un dispositif est géré par une instance de XClarity Administrator, et que vous souhaitez le gérer avec une autre instance de XClarity Administrator, vous devez d'abord annuler la gestion du dispositif dans l'instance de XClarity Administrator en cours, puis la

gérer avec la nouvelle instance de XClarity Administrator. Si une erreur se produit lors du processus d'annulation de gestion, vous pouvez sélectionner l'option **Forcer la gestion** lors de la gestion sur la nouvelle instance de XClarity Administrator.

Remarque : En analysant le réseau pour rechercher des dispositifs gérables, XClarity Administrator ne sait pas si un dispositif est déjà géré par un autre gestionnaire avant d'avoir tenté de gérer le dispositif.

Remarque : Lorsque vous analysez le réseau pour rechercher des appareils gérables, XClarity Administrator ne sait pas si un appareil ThinkServer est déjà géré. Par conséquent, les appareils ThinkServer gérés peuvent apparaître dans la liste des appareils gérables.

Au cours du processus de gestion, XClarity Administrator exécute les actions suivantes :

- Se connecte au serveur à l'aide des données d'identification fournies.
- Collecte l'inventaire pour chaque serveur.

  Remarque : Certaines données d'inventaire sont collectées une fois le processus de gestion terminé. Vous ne pouvez pas exécuter certaines tâches sur un serveur géré (comme le déploiement d'un modèle de serveur) jusqu'à ce que toutes les données d'inventaire soient collectées pour ce serveur et que le serveur ne soit plus dans l'état En attente.
- Configure les paramètres du serveur NTP afin que tous les appareils gérés utilisent la même configuration de serveur NTP que sur XClarity Administrator.
- (Serveurs System x et NeXtScale uniquement) Affecte la dernière stratégie de conformité du microprogramme modifiée au serveur.
- (Serveurs Lenovo System x et NeXtScale uniquement) Configure éventuellement les règles de pare-feu des appareils afin que seules les demandes entrantes en provenance de XClarity Administrator soient acceptées.
- (Serveurs System x et NeXtScale uniquement) Échange les certificats de sécurité avec le contrôleur de gestion, en copiant le certificat de serveur CIM et le certificat du client LDAP à partir du contrôleur de gestion dans le fichier de clés certifiées XClarity Administrator et en envoyant les certificats du certificat CA XClarity Administrator et les certificats d'approbation LDAP au contrôleur de gestion. Le contrôleur de gestion charge les certificats dans son fichier de clés certifiées afin de pouvoir approuver les connexions aux serveurs LDAP et CIM sur XClarity Administrator.

  Remarque : Si le certificat du serveur CIM ou le certificat du client LDAP n'existe pas, il est créé pendant le processus de gestion.
- Configure l'authentification gérée, le cas échéant. Pour plus d'informations sur l'authentification gérée, voir Gestion du serveur d'authentification.
- Crée le compte utilisateur de récupération (`RECOVERY_ID`), le cas échéant. Pour plus d'informations sur le compte `RECOVERY_ID`, voir Gestion du serveur d'authentification.

Remarque : XClarity Administrator ne modifie pas les paramètres de sécurité ni les paramètres cryptographiques (mode cryptographique et mode utilisé pour les communications sécurisées) lors du processus de gestion. Vous pouvez modifier les paramètres cryptographiques une fois le serveur géré (voir Configuration des paramètres cryptographiques sur le serveur de gestion).

Important : Si vous modifiez l'adresse IP d'un serveur lorsque le serveur est géré par XClarity Administrator, XClarity Administrator reconnaît la nouvelle adresse IP et continue à gérer le serveur. Toutefois, XClarity Administrator ne reconnaît pas le changement d'adresse IP pour certains serveurs. Si XClarity Administrator indique que le serveur est hors ligne après le changement d'adresse IP, gérez à nouveau le serveur à l'aide de l'option **Forcer la gestion**.

Procédure

Pour gérer vos serveurs rack et au format tour à l'aide de XClarity Administrator, suivez l'une des procédures suivantes.

- Détectez et gérez un grand nombre de serveurs rack et au format tour et d'autres appareils à l'aide d'un fichier d'importation en masse (voir Gestion des systèmes dans la documentation en ligne XClarity Administrator).
- Reconnaissez et gérez les serveurs rack et au format tour présents sur le même sous-réseau IP que XClarity Administrator.
  1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Reconnaître et gérer de nouveaux appareils**. La page Reconnaître et gérer de nouveaux appareils s'affiche.

     Vous pouvez trier les colonnes de la table pour faciliter la recherche des serveurs que vous voulez gérer. En outre, vous pouvez saisir un texte (par exemple, un nom ou une adresse IP) dans la zone **Filtre** pour filtrer davantage les serveurs affichés. Vous pouvez modifier les colonnes qui s'affichent et l'ordre de tri par défaut en cliquant sur l'icône **Personnaliser les colonnes** ( ).

  2. Cliquez sur l'icône **Actualiser** ( ) pour reconnaître tous les périphériques gérables dans le domaine XClarity Administrator. La reconnaissance peut prendre plusieurs minutes.
  3. Cliquez sur la case à cocher **Activer l'encapsulage de tous les appareils gérés ultérieurs** afin de modifier les règles de pare-feu sur tous les dispositifs lors du processus de gestion, de sorte que les demandes entrantes sont acceptées uniquement à partir de XClarity Administrator.

L'encapsulage peut être activé ou désactivé sur des dispositifs spécifiques après leur gestion.

Remarque : Lorsque l'interface réseau de gestion est configurée pour utiliser le protocole DHCP (Dynamic Host Configuration Protocol) et que l'encapsulation est activée, la gestion d'un serveur rack peut prendre du temps.

Attention : Si l'encapsulage est activé et que XClarity Administrator n'est plus disponible avant l'annulation de la gestion d'un dispositif, des mesures doivent être prises pour désactiver l'encapsulage afin d'établir la communication avec le dispositif. Pour les procédures de récupération, voir le fichier lenovoMgrAlert.mib et Reprise de la gestion avec un module CMM après une défaillance du serveur de gestion.

4. Sélectionnez un ou plusieurs serveurs à gérer.
5. Cliquez sur **Gérer la sélection**. La boîte de dialogue Gérer s'affiche.
6. Choisissez d'utiliser XClarity Administrator l'authentification gérée ou l'authentification locale pour cet appareil. L'authentification gérée est sélectionnée par défaut. Pour utiliser l'authentification locale, désactivez l'option **Authentification gérée**.
7. Choisissez le type de données d'identification à utiliser pour authentifier l'appareil et indiquez les données d'identification appropriées :
   - **Utiliser des données d'identification saisies manuellement**
     - Spécifiez l'ID utilisateur et le mot de passe pour l'authentification sur le serveur.
     - (Facultatif) Définissez un nouveau mot de passe pour le nom d'utilisateur spécifié si le mot de passe a expiré sur l'appareil.

     Remarque : Pour utiliser les données d'identification saisies manuellement, vous devez sélectionner l'authentification gérée XClarity Administrator.
   - **Utiliser des données d'identification stockées**

     Sélectionnez les données d'identification stockées à utiliser pour cet appareil géré. Vous pouvez créer de nouvelles données d'identification stockées en cliquant sur **Créer nouveau**.
   - **Utiliser un système de gestion d'identité**

     Choisissez le système de gestion d'identité à utiliser avec cet appareil géré. Renseignez ensuite les champs restants, comme l'adresse IP ou le nom d'hôte du serveur géré, le nom d'utilisateur, et (en option) l'ID d'application, le coffre-fort et le dossier.

     Si vous indiquez l'ID d'application, vous devez également indiquer le coffre-fort et le dossier, le cas échéant.

     Si vous n'indiquez pas l'ID d'application, XClarity Administrator utilise alors les chemins d'accès définis lors de la configuration de CyberArk pour identifier les comptes intégrés.

     Remarque : Seuls les serveurs ThinkSystem ou ThinkAgile sont pris en charge. Le système de gestion d'identité doit être configuré dans XClarity Administrator. Le Lenovo XClarity Controller destiné aux serveurs ThinkSystem ou ThinkAgile doit être intégré à CyberArk.

   Il est recommandé d'utiliser un compte administrateur ou superviseur pour gérer l'appareil. Si un compte avec un niveau de droits plus bas est utilisé, la gestion peut échouer, ou la gestion peut aboutir, mais d'autres opérations XClarity Administrator sur l'appareil peuvent échouer (notamment si l'appareil est géré sans authentification gérée).

   Pour plus d'informations sur les données d'identification normales et stockées, voir Gestion des comptes utilisateur, Gestion de données d'identification stockées.
8. Spécifiez le mot de passe de récupération si l'authentification gérée est sélectionnée.

Lorsqu'un mot de passe est spécifié, le compte de récupération (RECOVERY_ID) est créé sur le serveur et tous les comptes utilisateur locaux sont désactivés. En cas de problème avec XClarity Administrator, et s'il cesse de fonctionner pour une raison quelconque, vous *ne pouvez pas* vous connecter au contrôleur de gestion en utilisant des comptes utilisateur normaux. Cependant, vous pouvez vous connecter avec le compte de récupération.

Remarques :

- Le mot de passe de récupération est facultatif si vous choisissez d'utiliser l'authentification locale mais n'est pas autorisé si vous choisissez l'authentification locale.
- Vous pouvez choisir d'utiliser un compte de récupération local ou des données d'identification de récupération stockées. Dans les deux cas, le nom d'utilisateur est toujours RECOVERY_ID.
- Veillez à ce que le mot de passe respecte les règles de sécurité et définies pour les mots de passe sur l'appareil. Les règles de sécurité et de mot de passe peuvent varier.
- Veillez à noter le mot de passe de récupération pour un usage ultérieur.
- Le compte de récupération n'est pas pris en charge pour les serveurs ThinkServer et System x M4.

Pour plus d'informations sur le RECOVERY_ID, voir Gestion du serveur d'authentification.

9. Cliquez sur **Modifier** pour modifier les groupes de rôles qui doivent être affectés aux appareils.

   Remarques :

   - Vous pouvez effectuer votre sélection dans une liste de groupes de rôles affectée à l'utilisateur en cours.
   - Si vous ne modifiez pas les groupes de rôles, les groupes de rôles par défaut sont utilisés. Pour plus d'informations sur les groupes de rôles par défaut, voir Modification des droits par défaut.

10. Cliquez sur **Gérer**.

    Une boîte de dialogue s'affiche et présente la progression de ce processus de gestion. Pour vérifier si le processus aboutit, surveillez la progression.

11. Une fois le processus terminé, cliquez sur **OK**.

    Le dispositif est désormais géré par XClarity Administrator, qui interroge automatiquement et régulièrement le dispositif géré afin de collecter des informations à jour, telles que l'inventaire.

    Si la gestion n'a pas abouti en raison d'une des conditions d'erreur suivantes, répétez cette procédure en utilisant l'option **Forcer la gestion**.

    - Si l'instance de XClarity Administrator a échoué et ne peut pas être récupérée.

      Remarque : Si l'instance de remplacement de XClarity Administrator utilise la même adresse IP que l'instance de XClarity Administrator ayant rencontré une défaillance, vous pouvez gérer à nouveau le dispositif à l'aide du compte et du mot de passe RECOVERY_ID (le cas échéant) et de l'option **Forcer la gestion**.
    - Si l'instance XClarity Administrator de gestion a été mise hors tension avant que la gestion des appareils n'ait été annulée.
    - Si l'annulation de la gestion des appareils n'a pas été correctement effectuée.

    Attention : Les appareils peuvent être géré par une seule instance XClarity Administrator à la fois. La gestion par plusieurs instances de XClarity Administrator n'est pas prise en charge. Si un appareil est géré par une instance de XClarity Administrator, et que vous souhaitez le gérer avec une autre instance de XClarity Administrator, vous devez d'abord annuler la gestion de l'appareil dans l'instance de XClarity Administrator d'origine, puis la gérer avec la nouvelle instance de XClarity Administrator.

- Reconnaissez et gérez les serveurs rack et au format tour qui ne se trouvent pas sur le même sous-réseau IP que XClarity Administrator en spécifiant manuellement des adresses IP.
  1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Reconnaître et gérer de nouveaux appareils**. La page Reconnaître et gérer s'affiche.
  2. Cliquez sur la case à cocher **Activer l'encapsulage de tous les appareils gérés ultérieurs** afin de modifier les règles de pare-feu sur tous les dispositifs lors du processus de gestion, de sorte que les demandes entrantes sont acceptées uniquement à partir de XClarity Administrator.

     L'encapsulage peut être activé ou désactivé sur des dispositifs spécifiques après leur gestion.

     Remarque : Lorsque l'interface réseau de gestion est configurée pour utiliser le protocole DHCP (Dynamic Host Configuration Protocol) et que l'encapsulation est activée, la gestion d'un serveur rack peut prendre du temps.

     Attention : Si l'encapsulage est activé et que XClarity Administrator n'est plus disponible avant l'annulation de la gestion d'un dispositif, des mesures doivent être prises pour désactiver l'encapsulage afin d'établir la communication avec le dispositif. Pour les procédures de récupération, voir le fichier lenovoMgrAlert.mib et Reprise de la gestion avec un module CMM après une défaillance du serveur de gestion.
  3. Sélectionnez **Saisie manuelle**.
  4. Spécifiez les adresses réseau des serveurs à gérer :
     - Cliquez sur **Système unique**, puis entrez un nom de domaine d'adresse IP unique, ou un nom de domaine complet (FQDN).

       Remarque : Pour indiquer un nom FQDN, vérifiez qu'un nom de domaine valide est spécifié sur la page Accès réseau (voir Configuration de l'accès réseau).
     - Cliquez sur **Plusieurs systèmes** et entrez une plage d'adresses IP. Pour ajouter une autre plage, cliquez sur l'icône **Ajouter** (). Pour supprimer une plage, cliquez sur l'icône **Supprimer** ().
  5. Cliquez sur **OK**. La boîte de dialogue Gérer s'affiche
  6. Choisissez d'utiliser XClarity Administrator l'authentification gérée ou l'authentification locale pour cet appareil. L'authentification gérée est sélectionnée par défaut. Pour utiliser l'authentification locale, désactivez l'option **Authentification gérée**.
  7. Choisissez le type de données d'identification à utiliser pour authentifier l'appareil et indiquez les données d'identification appropriées :
     - **Utiliser des données d'identification saisies manuellement**
       - Spécifiez l'ID utilisateur et le mot de passe pour l'authentification sur le serveur.
       - (Facultatif) Définissez un nouveau mot de passe pour le nom d'utilisateur spécifié si le mot de passe a expiré sur l'appareil.

       Remarque : Pour utiliser les données d'identification saisies manuellement, vous devez sélectionner l'authentification gérée XClarity Administrator.
     - **Utiliser des données d'identification stockées**

       Sélectionnez les données d'identification stockées à utiliser pour cet appareil géré. Vous pouvez créer de nouvelles données d'identification stockées en cliquant sur **Créer nouveau**.
     - **Utiliser un système de gestion d'identité**

       Choisissez le système de gestion d'identité à utiliser avec cet appareil géré. Renseignez ensuite les champs restants, comme l'adresse IP ou le nom d'hôte du serveur géré, le nom d'utilisateur, et (en option) l'ID d'application, le coffre-fort et le dossier.

Si vous indiquez l'ID d'application, vous devez également indiquer le coffre-fort et le dossier, le cas échéant.

Si vous n'indiquez pas l'ID d'application, XClarity Administrator utilise alors les chemins d'accès définis lors de la configuration de CyberArk pour identifier les comptes intégrés.

Remarque : Seuls les serveurs ThinkSystem ou ThinkAgile sont pris en charge. Le système de gestion d'identité doit être configuré dans XClarity Administrator. Le Lenovo XClarity Controller destiné aux serveurs ThinkSystem ou ThinkAgile doit être intégré à CyberArk.

Il est recommandé d'utiliser un compte administrateur ou superviseur pour gérer l'appareil. Si un compte avec un niveau de droits plus bas est utilisé, la gestion peut échouer, ou la gestion peut aboutir, mais d'autres opérations XClarity Administrator sur l'appareil peuvent échouer (notamment si l'appareil est géré sans authentification gérée).

Pour plus d'informations sur les données d'identification normales et stockées, voir Gestion des comptes utilisateur, Gestion de données d'identification stockées.

8. Spécifiez le mot de passe de récupération si l'authentification gérée est sélectionnée.

   Lorsqu'un mot de passe est spécifié, le compte de récupération (`RECOVERY_ID`) est créé sur le serveur et tous les comptes utilisateur locaux sont désactivés. En cas de problème avec XClarity Administrator, et s'il cesse de fonctionner pour une raison quelconque, vous *ne pouvez pas* vous connecter au contrôleur de gestion en utilisant des comptes utilisateur normaux. Cependant, vous pouvez vous connecter avec le compte de récupération.

   Remarques :

   - Le mot de passe de récupération est facultatif si vous choisissez d'utiliser l'authentification locale mais n'est pas autorisé si vous choisissez l'authentification locale.
   - Vous pouvez choisir d'utiliser un compte de récupération local ou des données d'identification de récupération stockées. Dans les deux cas, le nom d'utilisateur est toujours `RECOVERY_ID`.
   - Veillez à ce que le mot de passe respecte les règles de sécurité et définies pour les mots de passe sur l'appareil. Les règles de sécurité et de mot de passe peuvent varier.
   - Veillez à noter le mot de passe de récupération pour un usage ultérieur.
   - Le compte de récupération n'est pas pris en charge pour les serveurs ThinkServer et System x M4.

   Pour plus d'informations sur le RECOVERY_ID, voir Gestion du serveur d'authentification.

9. Cliquez sur **Modifier** pour modifier les groupes de rôles qui doivent être affectés aux appareils.

   Remarques :

   - Vous pouvez effectuer votre sélection dans une liste de groupes de rôles affectée à l'utilisateur en cours.
   - Si vous ne modifiez pas les groupes de rôles, les groupes de rôles par défaut sont utilisés. Pour plus d'informations sur les groupes de rôles par défaut, voir Modification des droits par défaut.

10. Cliquez sur **Gérer**.

    Une boîte de dialogue s'affiche et présente la progression de ce processus de gestion. Pour vérifier si le processus aboutit, surveillez la progression.

11. Une fois le processus terminé, cliquez sur **OK**.

    Le dispositif est désormais géré par XClarity Administrator, qui interroge automatiquement et régulièrement le dispositif géré afin de collecter des informations à jour, telles que l'inventaire.

    Si la gestion n'a pas abouti en raison d'une des conditions d'erreur suivantes, répétez cette procédure en utilisant l'option **Forcer la gestion**.

- Si l'instance de XClarity Administrator a échoué et ne peut pas être récupérée.

  Remarque : Si l'instance de remplacement de XClarity Administrator utilise la même adresse IP que l'instance de XClarity Administrator ayant rencontré une défaillance, vous pouvez gérer à nouveau le dispositif à l'aide du compte et du mot de passe RECOVERY_ID (le cas échéant) et de l'option **Forcer la gestion**.
- Si l'instance XClarity Administrator de gestion a été mise hors tension avant que la gestion des appareils n'ait été annulée.
- Si l'annulation de la gestion des appareils n'a pas été correctement effectuée.

Attention : Les appareils peuvent être géré par une seule instance XClarity Administrator à la fois. La gestion par plusieurs instances de XClarity Administrator n'est pas prise en charge. Si un appareil est géré par une instance de XClarity Administrator, et que vous souhaitez le gérer avec une autre instance de XClarity Administrator, vous devez d'abord annuler la gestion de l'appareil dans l'instance de XClarity Administrator d'origine, puis la gérer avec la nouvelle instance de XClarity Administrator.

Après avoir terminé

- Reconnaître et gérer d'autres dispositifs.
- Configurez les informations système, le stockage local, les cartes d'E-S, les rubriques relatives à l'amorçage et les paramètres de microprogramme en créant et en déployant des modèles de serveur (voir Configuration des serveurs à l'aide de modèles de configuration).
- Déployez des images de système d'exploitation pour les serveurs sur lesquels aucun système d'exploitation n'est encore installé (voir Installation de systèmes d'exploitation sur des serveurs nus).
- Mettez à jour le microprogramme sur les dispositifs qui ne sont pas en conformité avec les stratégies actuelles (voir Mise à jour du microprogramme sur les appareils gérés).
- Ajoutez les dispositifs dans l'armoire appropriée pour refléter l'environnement physique (voir Gestion des armoires).
- Surveillez l'état et les informations détaillées du matériel (voir Affichage de l'état d'un serveur géré).
- Surveillez les événements et alertes (voir Utilisation des événements et Utilisation des alertes).
- Effacez le journal des événements système (SEL) d'un serveur en cliquant sur **Matériel → Serveurs** depuis la barre de menus de XClarity Administrator, en sélectionnant le serveur, puis en cliquant sur **Toutes les actions → Sécurité → Effacer le journal des événements système (SEL)**.Cette action n'est prise en charge que pour les serveurs ThinkSystem et ThinkAgile.
- Résoudre les données d'identification stockées qui ont expiré ou sont non valides (voir Gestion de données d'identification stockées).
- Activez ou désactivez la connexion unique pour tous les serveurs ThinkSystem et ThinkAgile gérés en cliquant sur **Administration → Sécurité** depuis la barre de menus de XClarity Administrator, en cliquant sur **Sessions actives**, puis en activant ou désactivant **Connexion unique**.
- Désactiver ou activer la connexion unique pour les serveurs ThinkSystem et ThinkAgile gérés.
  - Pour tous les serveurs ThinkSystem et ThinkAgile gérés (globalement), cliquer sur **Administration → Sécurité** à partir de la barre de menu XClarity Administrator, puis cliquer sur **Sessions actives**, puis activer ou désactiver **Connexion unique**.
  - Pour un serveur ThinkSystem et ThinkAgile spécifique, cliquer sur **Matériel → Serveur** dans la barre de menus XClarity Administrator, puis cliquer sur **Toutes les actions → Sécurité → Activer connexion unique** ou**Toutes les actions → Sécurité → Désactiver connexion unique**.

Remarque : L'authentification unique permet à un utilisateur qui est déjà connecté à XClarity Administrator de se connecter automatiquement au contrôle de gestion de la carte mère. La connexion unique est activée par défaut lorsqu'un serveur ThinkSystem ou ThinkAgile est amené dans la gestion par

XClarity Administrator (sauf si le serveur est géré avec des mots de passe CyberArk). Vous pouvez configurer le paramètre global pour activer ou désactiver la connexion unique pour tous les serveurs ThinkSystem et ThinkAgile gérés. L'activation de la connexion unique pour un serveur ThinkSystem et ThinkAgile remplace le paramétrage global pour tous les serveurs ThinkSystem et ThinkAgile .

Affichage de l'état d'un serveur géré

Vous pouvez afficher un récapitulatif et un état détaillé pour les serveurs gérés et leurs composants installés à partir de Lenovo XClarity Administrator.

En savoir plus :

- XClarity Administrator : Inventaire
- XClarity Administrator : Surveillance

À propos de cette tâche

Les icônes d'état suivantes sont utilisées pour indiquer l'état de santé global de l'appareil. Si les certificats ne correspondent pas, la mention « (Non sécurisé) » est ajoutée à l'état de chaque appareil concerné, par exemple Avertissement (Non sécurisé). En cas de problème de connectivité ou si une connexion à l'appareil n'est pas sécurisée, la mention « (Connectivité) » est ajoutée à l'état de chaque appareil concerné, par exemple Avertissement (Connectivité).

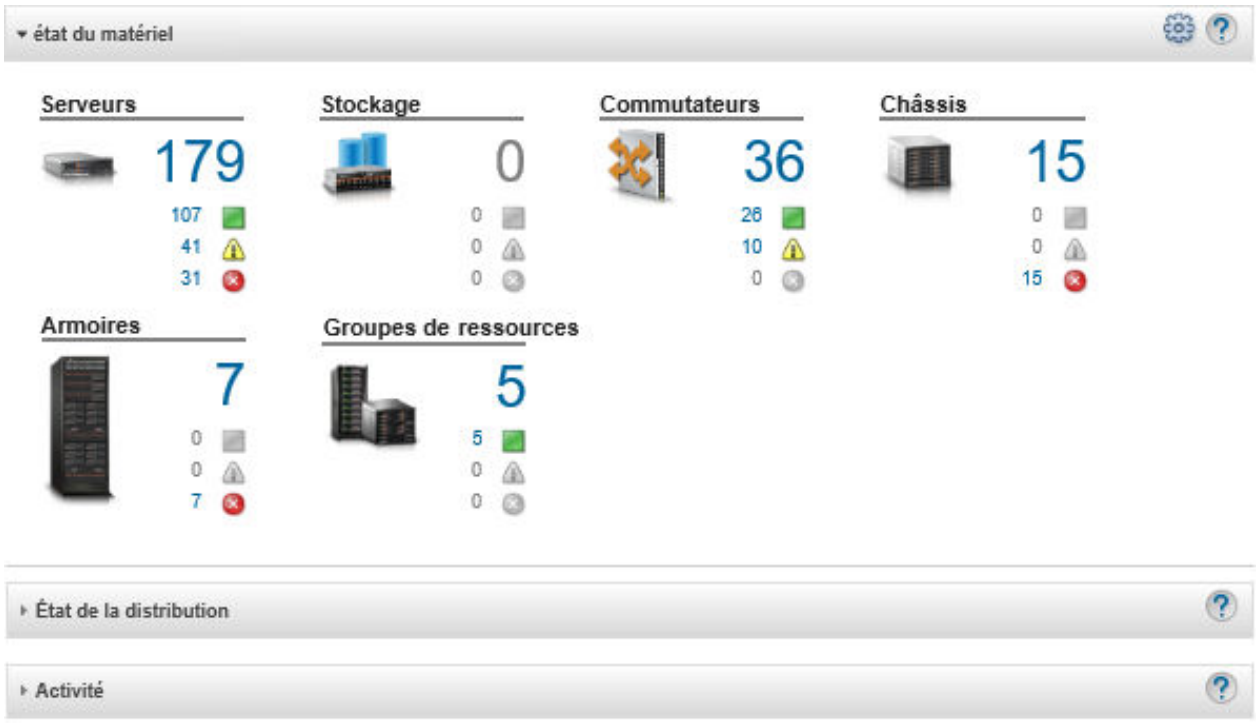
- ( ) Critique
- ( ) Avertissement
- ( ) En attente
- ( ) Informations
- ( ) Normal
- ( ) Hors ligne
- ( ) Inconnu

Un appareil peut se trouver dans l'un des états d'alimentation suivants :
- En fonction
- Hors fonction
- Arrêter
- veille
- Mettre en veille prolongée
- Unknown

Procédure

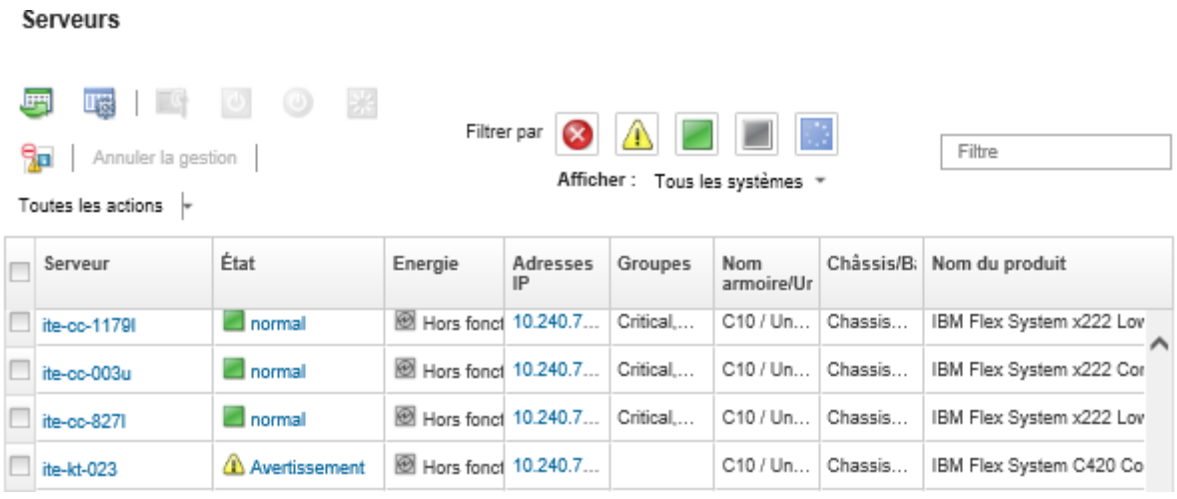
Pour afficher l'état d'un serveur géré, exécutez une ou plusieurs des actions suivantes.

- Dans la barre de menus de XClarity Administrator, cliquez sur **Tableau de bord**. La page Tableau de bord affiche la présentation et l'état de tous les appareils et d'autres ressources.



- Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Serveurs**. La page Serveurs qui s'affiche présente une vue tabulaire de tous les serveurs gérés (serveurs rack, serveurs au format tour et nœuds de traitement).

  Vous pouvez trier les colonnes du tableau afin de faciliter la recherche de serveurs spécifiques. En outre, vous pouvez sélectionner un type de système dans la liste déroulante **Tous les systèmes**, saisir un texte (par exemple, un nom ou une adresse IP) dans la zone **Filtre**, puis cliquer sur les icônes d'état pour afficher uniquement les serveurs qui répondent aux critères sélectionnés.



  Depuis cette page, vous pouvez effectuer les actions suivantes :

  – Afficher des informations détaillées sur le serveur et ses composants (voir Affichage des détails d'un serveur géré).
  – Afficher un serveur dans la vue graphique Armoire ou Châssis en cliquant sur **Toutes les actions → Vues → Afficher dans la vue Armoire** ou sur **Toutes les actions → Vues → Afficher dans la vue Châssis**.

- Lancer l'interface Web du contrôleur de gestion pour le serveur en cliquant sur le lien **Adresse IP** (voir Lancement de l'interface du contrôleur de gestion pour un serveur).
- Gérer à distance le serveur (voir Utilisation du contrôle à distance pour gérer des serveurs Converged, Flex System, NeXtScale et System x).
- Mettre le serveur sous tension et hors tension (voir Mise sous tension et hors tension d'un serveur).
- Modifier des informations système en sélectionnant un serveur, puis en cliquant sur **Toutes les actions → Inventaire → Éditer les propriétés**.
- Actualiser l'inventaire en sélectionnant un serveur et en cliquant sur **Toutes les actions → Inventaire → Actualiser l'inventaire**.
- Exporter des informations détaillées relatives à un ou plusieurs serveurs vers un seul fichier CSV en sélectionnant les serveurs, puis en cliquant sur **Toutes les actions → Inventaire → Exporter l'inventaire**.

  Remarque : Vous pouvez exporter les données d'inventaire pour un maximum de 60 dispositifs en même temps.

  Conseil : Lors de l'importation d'un fichier CSV dans Microsoft Excel, Excel traite les valeurs textuelles contenant uniquement des numéros sous la forme de valeurs numériques (par exemple, pour des UUID). Formatez chaque cellule sous forme de texte pour résoudre cette erreur.
- Annuler la gestion d'un serveur (voir Annulation de la gestion d'un serveur rack ou au format tour).
- Réinitialiser les adaptateurs de stockage local à leur valeur par défaut en cliquant sur **Toutes les actions → Service → Réinitialiser le stockage local aux valeurs par défaut**.
- Modifiez l'état du voyant de localisation sur un serveur en le faisant passer à Allumé, Éteint ou clignotant en sélectionnant le serveur et en cliquant sur **Toutes les actions → Service → Basculer l'état du voyant de localisation**, en sélectionnant l'état puis en cliquant sur **Appliquer**.
  - Le basculement du voyant de localisation pour les serveurs ThinkSystem SR635 et SR655 n'est pas pris en charge.
  - Le voyant de localisation situé sur les serveurs ThinkServer peut être allumé ou éteint. Le clignotement n'est pas pris en charge.
- Réinstaller virtuellement le serveur (voir Réinstallation virtuelle d'un serveur dans un châssis Flex System).
- Exclure les événements qui ne vous intéressent pas de toutes les pages sur lesquelles des événements sont affichés en cliquant sur l'icône **Exclure des événements** () (voir Exclusion d'événements).
- Redémarrer le serveur à l'aide d'une interruption non masquable (NMI) en cliquant sur **Toutes les actions → Service → Déclencher NMI**.
- Activer ou désactiver les modifications de règles de pare-feu sur un serveur qui limitent les demandes entrantes à celles provenant de XClarity Administrator en sélectionnant le serveur, puis en cliquant sur **Toutes les actions → Sécurité → Activer Encapsulation** ou **Toutes les actions → Sécurité → DésactiverEncapsulation**.Le paramètre d'encapsulage global est désactivé par défaut. Une fois désactivé, le mode d'encapsulage de dispositif est défini sur « normal » et les règles de pare-feu ne sont pas modifiées dans le cadre du processus de gestion.

  Lorsque le paramètre global d'encapsulage est activé et que le dispositif prend en charge l'encapsulage, XClarity Administrator communique avec le dispositif pendant le processus de gestion pour remplacer le mode d'encapsulage de dispositif par « encapsulationLite » et modifier les règles de pare-feu sur le dispositif afin de limiter les demandes entrantes à celles de XClarity Administrator.

  Attention : Si l'encapsulage est activé et que XClarity Administrator n'est plus disponible avant l'annulation de la gestion d'un dispositif, des mesures doivent être prises pour désactiver l'encapsulage afin d'établir la communication avec le dispositif. Pour les procédures de récupération,

voir le fichier lenovoMgrAlert.mib et Reprise de la gestion avec un module CMM après une défaillance du serveur de gestion.

- (Serveurs Converged, Flex System, NeXtScale et System x et ThinkSystem uniquement) Corriger les problèmes pouvant survenir entre le certificat de sécurité XClarity Administrator et le certificat de sécurité du contrôleur de gestion de la carte mère sur le serveur en sélectionnant un serveur et en cliquant sur **Toutes les actions → Sécurité → Résoudre les certificats non sécurisés**(voir Résolution d'un certificat du serveur non sécurisé).
- Résoudre les données d'identification expirées ou non valides pour un appareil du groupe (voir Résolution de données d'identification expirées ou non valides pour un serveur).
- Ajouter ou retirer un serveur d'un groupe de ressources statique en cliquant sur **Toutes les actions → Groupes → Ajouter au groupe** ou sur **Toutes les actions → Groupes → Retirer du groupe**.

Affichage des détails d'un serveur géré

Vous pouvez afficher des informations détaillées relatives aux serveurs gérés à partir de Lenovo XClarity Administrator, notamment les niveaux de microprogramme, le nom du serveur et l'identificateur unique universel (UUID).

En savoir plus :

- XClarity Administrator : Inventaire
- XClarity Administrator : Surveillance

À propos de cette tâche

L'utilisation de l'unité centrale mesure l'implantation permanente dans l'état C agrégé. Elle est mesurée sous la forme d'un pourcentage de l'implantation permanente dans l'état C0 utilisée et maximale, par seconde.

L'utilisation de la mémoire mesure les volumes en lecture/écriture regroupés de tous les canaux de mémoire. Cela est calculé sous la forme d'un pourcentage de la bande passante de mémoire utilisée et maximale disponible, par seconde.

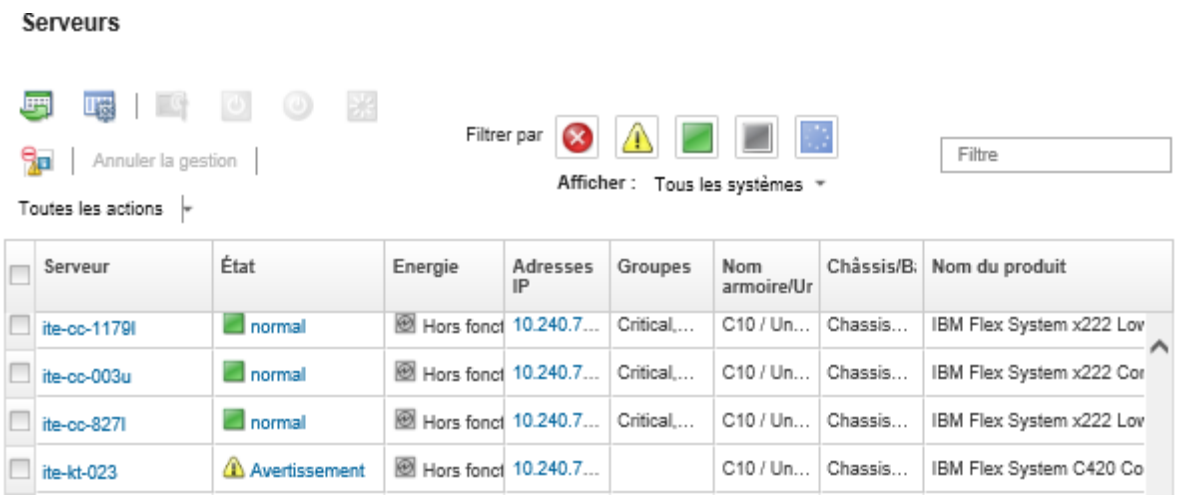
La température d'air au niveau du système est mesurée par un détecteur physique situé à l'avant du serveur. Cette température représente la température d'air entrant du serveur. Notez que la température d'air signalée par XClarity Administrator et celle communiquée par le module CMM peuvent être différentes si elles sont capturées à des moments différents.

Procédure

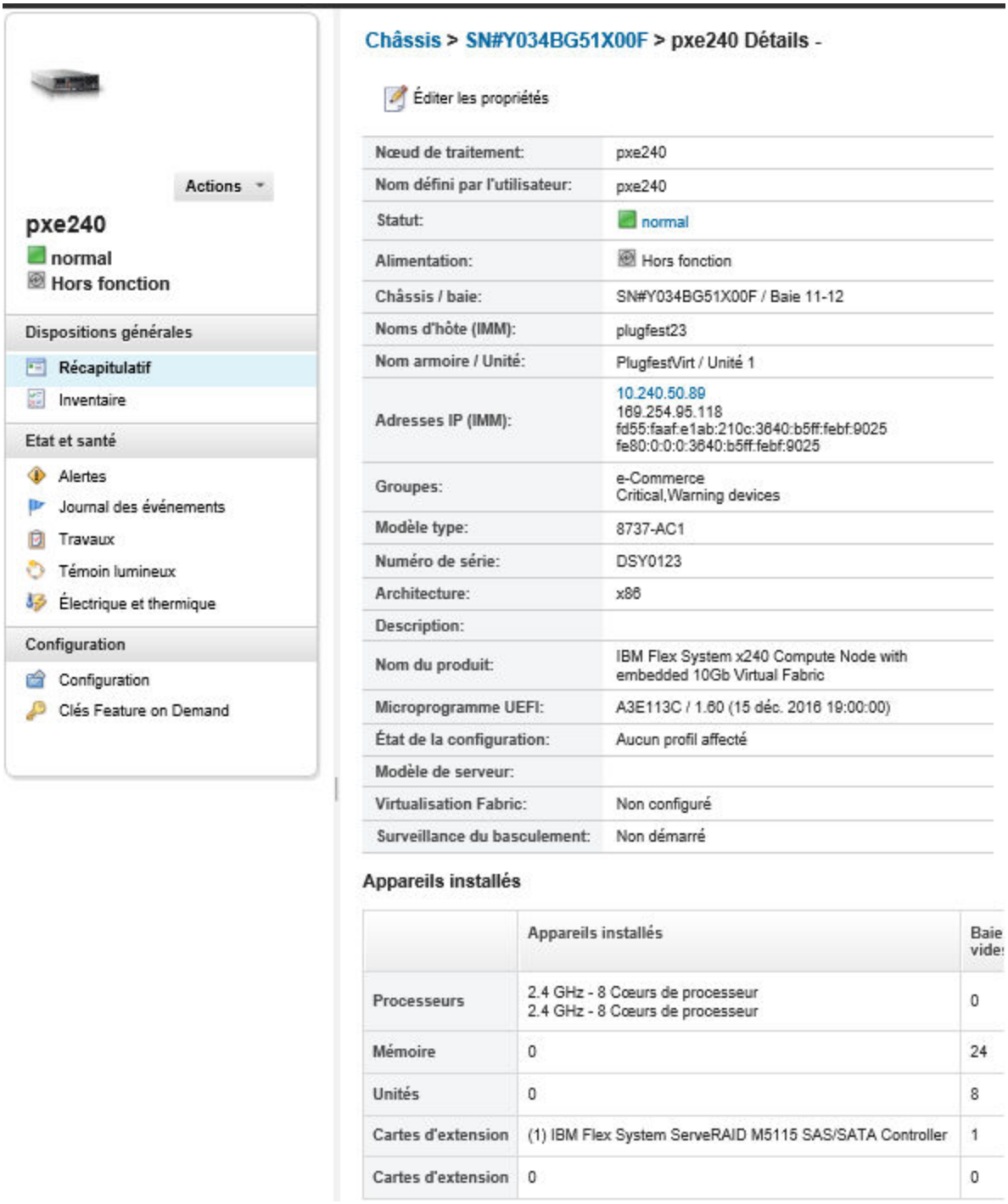
Pour afficher les détails d'un serveur géré, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Serveurs**. La page Serveurs s'affiche avec une vue tabulaire de tous les serveurs gérés (serveurs rack et nœuds de traitement).

Vous pouvez trier les colonnes de la table pour faciliter la recherche des serveurs spécifiques. En outre, vous pouvez sélectionner un type de système dans la liste déroulante **Tous les systèmes** et saisir un texte (par exemple, un nom de système ou une adresse IP) dans la zone **Filtre** pour filtrer davantage l'affichage des serveurs.



Etape 2. Cliquez sur le lien du serveur dans la colonne **Serveur**. La page de récapitulatif de l'état de ce serveur s'affiche et présente les propriétés du serveur ainsi qu'une liste des composants installés sur ce serveur.



Remarque : Pour les serveurs System x et NeXtScale, l'adresse de réseau local via USB est répertoriée sur cette page. Toutefois, vous ne pouvez pas modifier cette adresse à partir de XClarity Administrator. Vous devez à la place utiliser l'interface du contrôleur de gestion de la carte mère du serveur. Pour plus d'informations, voir « Accès au module IMM2 à l'aide de l'interface de réseau local via USB » dans la documentation produit du serveur. La documentation produit de votre serveur est disponible dans la Documentation en ligne de BladeCenter.

Etape 3. Exécutez une ou plusieurs des actions suivantes :

- Cliquez sur **Récapitulatif** pour afficher un récapitulatif du serveur, notamment les informations système et les composants installés (voir Affichage de l'état d'un serveur géré).

- Cliquez sur **Détails d'inventaire** pour afficher des détails sur les composants serveur, notamment :
  - Les niveaux de microprogramme pour le serveur et le contrôleur de gestion.
  - Les détails relatifs au réseau du module de gestion, tels que le nom d'hôte, l'adresse IPv4, l'adresse IPv6 et les adresses MAC.
  - Les détails des actifs, notamment le nom du serveur, l'identificateur unique universel (UUID) et l'emplacement.
  - Les détails relatifs aux composants, notamment les UC, la mémoire, les unités et les cartes d'extension.

  Remarques :

  - Toutes les adresses IP pour le serveur sont répertoriées. L'adresse IP du port du contrôleur de gestion est répertoriée en premier. Si l'adresse IP du contrôleur de gestion est disponible, elle est utilisée pour la connexion au serveur.
  - Si des données ne sont pas disponibles pour une carte spécifique, certaines zones de la carte (telles que le nom du produit) peuvent être vides.
  - Si une nouvelle carte a été installée sur le serveur, ce dernier doit être réamorcé pour que la carte apparaisse dans l'inventaire.
  - Pour certaines cartes d'extension, les informations Feature on Demand s'affichent sous le nom de l'appareil.
  - Vous pouvez passer la souris sur les liens figurant dans la colonne Type afin d'obtenir plus d'informations au sujet des composants spécifiques, tels que la mémoire Intel Optain DCPMM.
- Cliquez sur **Alertes** pour afficher la liste des alertes actuelles de ce serveur (voir Utilisation des alertes).

  Remarque : Vous pouvez définir des préférences de seuil pour le déclenchement d'une alerte et d'un événement lorsqu'une certaine valeur, comme la durée de vie d'un disque SSD sur un serveur ThinkSystem ou ThinkServer dépasse un niveau d'avertissement ou critique (voir Définition des préférences de seuil pour la génération d'alertes et d'événements).
- Cliquez sur **Journal des événements** pour afficher la liste des événements de ce serveur (voir Surveillance des événements dans le journal des événements).
- Cliquez sur **Travaux** pour afficher la liste des travaux associés au serveur (voir Surveillance des travaux).
- Cliquez sur **Light Path** pour afficher l'état actuel des voyants du serveur, comme Emplacement, Erreur et Informations. Cela revient à regarder le panneau frontal du serveur.
- Cliquez sur **Électrique et thermique** pour afficher les détails relatifs à l'utilisation de l'alimentation et la température de l'air.

  Conseil : utilisez le bouton d'actualisation de votre navigateur Web pour collecter les dernières données électriques et thermiques. La collecte de données peut prendre plusieurs minutes.
- Cliquez sur **Configuration** pour afficher des informations sur la configuration actuelle du serveur (par exemple, stockage local, cartes d'E-S, paramètres d'amorçage SAN et paramètres de microprogramme), ainsi que sa conformité avec le modèle de configuration attribué (voir Configuration des serveurs à l'aide de modèles de configuration).
- Cliquez sur **Clés Feature on Demand** pour afficher la liste des clés Feature on Demand actuellement installées sur le serveur géré (voir Affichage des clés Features on Demand (FoD)).

Après avoir terminé

En plus d'afficher un récapitulatif et des informations détaillées relatives à un serveur, vous pouvez effectuer les actions suivantes :

- Vérifiez l'armoire ou le châssis associé au serveur en cliquant sur le nom de l'armoire et du châssis, dans la page Récapitulatif.
- Afficher un serveur sélectionné dans la vue graphique Armoire ou Châssis en cliquant sur **Toutes les actions → Vues → Afficher dans la vue Armoire** ou sur **Toutes les actions → Vues → Afficher dans la vue Châssis**.
- Lancer l'interface Web du contrôleur de gestion pour le serveur sélectionné en cliquant sur le lien **Adresse IP** (voir Lancement de l'interface du contrôleur de gestion pour un serveur).
- Accéder à distance à un serveur (voir Utilisation du contrôle à distance pour gérer des serveurs Converged, Flex System, NeXtScale et System x).
- Mettre un serveur sélectionné sous tension et hors tension (voir Mise sous tension et hors tension d'un serveur).
- Modifier des informations système d'un serveur sélectionné en cliquant sur **Éditer les propriétés**.
- Actualiser l'inventaire d'un serveur sélectionné en cliquant sur **Actions → Inventaire → Actualiser l'inventaire**.
- Exporter des informations détaillées relatives aux serveurs dans un fichier CSV en cliquant sur **Actions → Inventaire → Exporter l'inventaire**.

  Remarques :

  – Pour plus d'informations sur les données d'inventaire dans le fichier CSV, voir GET /nodes/<*UUID_list*> dans la documentation en ligne de XClarity Administrator.

  – Lors de l'importation d'un fichier CSV dans Microsoft Excel, Excel traite les valeurs textuelles contenant uniquement des numéros sous la forme de valeurs numériques (par exemple, pour des UUID). Formatez chaque cellule sous forme de texte pour résoudre cette erreur.
- Exclure les événements qui ne vous intéressent pas de toutes les pages sur lesquelles des événements sont affichés en cliquant sur **Actions → Réinitialisation de service → Exclure des événements** (voir Exclusion d'événements).
- Redémarrer un serveur sélectionné à l'aide d'une interruption non masquable (NMI) en cliquant sur **Actions → Service → Déclencher NMI**.
- Modifier l'état du voyant de localisation sur un serveur sélectionné en le faisant passer à allumé, éteint ou clignotant, pour cela cliquer sur **Actions → Service → Basculer l'état du voyant de localisation**, en sélectionnant l'état, puis en cliquant sur **Appliquer**.

  Remarques :
  – Le basculement du voyant de localisation pour les serveurs ThinkSystem SR635 et SR655 n'est pas pris en charge.
  – Le voyant de localisation situé sur les serveurs ThinkServer peut être allumé ou éteint. Le clignotement n'est pas pris en charge.
- Désactivez ou activez la connexion unique pour un serveur ThinkSystem et ThinkAgile sélectionné en cliquant sur **Toutes les actions → Sécurité → Activer la connexion unique** ou **Toutes les actions → Sécurité → Désactiver la connexion unique**.

  L'authentification unique permet à un utilisateur qui est déjà connecté à XClarity Administrator de se connecter automatiquement au contrôle de gestion de la carte mère. La connexion unique est activée par défaut lorsqu'un serveur ThinkSystem ou ThinkAgile est amené dans la gestion par XClarity Administrator (sauf si le serveur est géré avec des mots de passe CyberArk). Vous pouvez configurer le paramètre global pour activer ou désactiver la connexion unique pour tous les serveurs ThinkSystem et ThinkAgile gérés. L'activation de la connexion unique pour un serveur ThinkSystem et ThinkAgile remplace le paramétrage global pour tous les serveurs ThinkSystem et ThinkAgile .

Remarque : La connexion unique est automatiquement désactivée lorsque vous faites appel au système de gestion d'identité CyberArk pour vous connecter.

- Activer ou désactiver les modifications de règles de pare-feu sur un serveur sélectionné qui limitent les demandes entrantes à celles de XClarity Administrator en cliquant sur **Actions → Sécurité → Activer l'encapsulage** ou **Actions → Sécurité → Désactiver l'encapsulage**. Le paramètre d'encapsulage global est désactivé par défaut. Une fois désactivé, le mode d'encapsulage de dispositif est défini sur « normal » et les règles de pare-feu ne sont pas modifiées dans le cadre du processus de gestion.

  Lorsque le paramètre global d'encapsulage est activé et que le dispositif prend en charge l'encapsulage, XClarity Administrator communique avec le dispositif pendant le processus de gestion pour remplacer le mode d'encapsulage de dispositif par « encapsulationLite » et modifier les règles de pare-feu sur le dispositif afin de limiter les demandes entrantes à celles de XClarity Administrator.

  Attention : Si l'encapsulage est activé et que XClarity Administrator n'est plus disponible avant l'annulation de la gestion d'un dispositif, des mesures doivent être prises pour désactiver l'encapsulage afin d'établir la communication avec le dispositif. Pour les procédures de récupération, voir le fichier lenovoMgrAlert.mib et Reprise de la gestion avec un module CMM après une défaillance du serveur de gestion.
- (Serveurs non ThinkServer uniquement) Corriger les problèmes pouvant survenir entre le certificat de sécurité Lenovo XClarity Administrator et le certificat de sécurité de ce contrôleur de gestion sur le serveur sélectionné en cliquant sur **Actions → Sécurité → Résoudre les certificats non sécurisés** (voir Résolution d'un certificat du serveur non sécurisé).

Sauvegarde et restauration des données de configuration de serveur

Lenovo XClarity Administrator n'inclut pas de fonctions de sauvegarde intégrées pour les données de configuration de serveur. À la place, utilisez les fonctions de sauvegarde qui sont disponibles pour votre serveur géré.

- **Serveurs Converged, Flex System, System x, ThinkSystem et NeXtScale**
  - Sauvegarde des données de configuration de serveur

    Utilisez l'interface Web ou l'interface CLI de gestion pour sauvegarder le microprogramme.

    - Dans l'interface Web IMM, cliquez sur **Gestion IMM → Configuration IMM**.
    - Dans l'interface CLI, utilisez la commande `backup`.

    Pour plus d'informations sur la sauvegarde des serveurs via le module IMM, voir la Documentation en ligne d'Integrated Management Module II.

    Utilisez les outils fournis par le système d'exploitation pour sauvegarder les applications qui s'exécutent sur le serveur. Pour plus d'informations, voir la documentation fournie avec le système d'exploitation.

    Pour les dispositifs de traitement Flex System, assurez-vous de sauvegarder les paramètres des options installées sur les nœuds de traitement. Vous pouvez sauvegarder tous les paramètres des nœuds de traitement, notamment les paramètres des options, à l'aide de l'utilitaire ASU (Advanced Setup Utility). Pour plus d'informations sur ASU, voir Site Web de l'utilitaire ASU (Advanced Settings Utility).
  - Restauration des données de configuration serveur

    Utilisez l'interface Web ou l'interface CLI de gestion pour restaurer le microprogramme. Pour plus d'informations sur la restauration des serveurs via le module BMC, voir Documentation en ligne d'Integrated Management Module II.

Pour restaurer le logiciel installé sur le serveur, utilisez la documentation fournie avec le système d'exploitation et toutes les applications en cours d'exécution sur le serveur.

- Dans l'interface Web IMM, cliquez sur **Gestion IMM → Configuration IMM**.
- Dans l'interface CLI, utilisez la commande `restore`.

Remarque : Conseil : Des informations supplémentaires relatives à la sauvegarde et la restauration des composants du châssis sont disponibles dans le Guide des bonnes pratiques de sauvegarde et de restauration PureFlex et Flex System.

- **Serveurs ThinkServer**Les procédures de restauration sont différentes suivant le type de serveurs ThinkServer. Pour plus d'informations sur la restauration de l'appareil, consultez la documentation produit fournie avec votre serveur.

Activation de System Guard

System Guard surveille les divergences de l'inventaire matériel pour les serveurs ThinkSystem équipés de XCC2.

À propos de cette tâche

L'inventaire surveillé inclut les processeurs, la mémoire, les adaptateurs PCI, les unités de disque, la carte mère et les cartes mezzanine. Les modifications des niveaux de microprogramme et des paramètres de configuration ne sont pas détectées.

Lorsque System Guard est activé, un instantané de l'inventaire matériel est pris comme référence fiable pour chaque appareil sélectionné. Lorsqu'un appareil est redémarré, le contrôleur de gestion de la carte mère de l'appareil collecte la configuration système actuelle et la compare à l'instantané. Lorsqu'un écart est détecté pour un ou plusieurs composants, System Guard déclenche un événement. Si un écart est détecté pour un processeur ou un élément de mémoire, System Guard déclenche un événement et empêche éventuellement le serveur de s'amorcer dans le système d'exploitation.

Procédure

Pour activer System Guard sur un serveur serveurs avec XCC2 supplémentaire, procédez comme suit.

Etape 1. Dans le menu XClarity Administrator, cliquez sur **Matériel → Serveurs**. La page Serveurs qui s'affiche présente une vue tabulaire de tous les serveurs gérés.

Etape 2. Sélectionnez un ou plusieurs serveurs avec XCC2.

Etape 3. Cliquez sur **Toutes les actions → Sécurité → Activer System Guard** pour afficher la boîte de dialogue Activer System Guard.

Etape 4. Choisissez l'action à entreprendre lorsque System Guard est activé, qu'une modification d'inventaire est détectée et que le serveur devient non conforme.

- **Activer, conserver le comportement par défaut du système**. Le comportement actuel est utilisé. . Le comportement par défaut consiste à générer un événement.
- **Activer, empêcher l'amorçage SE en cas de non conformité**. Un événement est déclenché. Si vous tentez un amorçage dans le système d'exploitation, vous recevez un avertissement indiquant que System Guard a détecté des modifications de configuration au niveau des processeurs ou de la mémoire. Dans ce cas, vous êtes invité à vous connecter au contrôleur de gestion de la carte mère si les modifications sont inattendues ; sinon, vous pouvez poursuivre le processus d'amorçage ou d'arrêt. Si vous ne répondez pas dans les 5 minutes, le serveur est arrêté par défaut.
- **Activer, générer un événement en cas de non conformité**. Un événement est déclenché mais aucune autre action n'est entreprise.

Etape 5. Cliquez sur **Appliquer**.

Une tâche est créée pour créer des instantanés d'inventaire pour le serveur sélectionné. Vous pouvez surveiller la progression de la tâche à partir du journal des travaux. Dans le menu XClarity Administrator, cliquez sur **Surveillance → Travaux**. Pour plus d'informations sur le journal des travaux, voir Surveillance des travaux.

Après avoir terminé

Pour désactiver System Guard sur les serveurs sélectionnés, cliquez sur **Toutes les actions → Sécurité → Désactiver System Guard**, puis cliquez sur **Appliquer**.

Effacement sécurisé des données d'unité

Lenovo XClarity Administrator peut effacer de manière sécurisée les données de toutes les unités de certains serveurs ThinkSystem et ThinkAgile exécutant la version 22B ou une version ultérieure. Cette opération réécrit de manière permanente chaque unité en remplissant l'intégralité de l'unité avec un zéro binaire, un chiffre un binaire ou des données aléatoires, ce qui rend difficile la détection de ce qui a été enregistré sur l'unité.

Attention :

- Cette opération efface de manière *permanente* et *irréversible* toutes les données des unités.
- Une fois le travail soumis, il n'est pas possible de l'annuler.

Avant de commencer

Vous devez disposer de droits **lxc-supervisor** pour effacer les données de l'unité.

Assurez-vous que le mot de passe UEFI admin n'est pas défini sur les serveurs gérés à effacer. Si le mot de passe UEFI admin est défini sur un serveur, les unités de ces serveurs ne sont pas effacées.

Par défaut, vous pouvez effacer de manière sécurisée les données de jusqu'à trois serveurs à la fois. Vous pouvez configurer le nombre de serveurs autorisés à la fois en cliquant sur **Administration → Préférences de l'inventaire**, puis en définissant **Nombre maximal de serveurs pouvant être effacés dans un lot** pour obtenir la valeur souhaitée. Vous pouvez choisir un nombre parmi les `3 - 100` serveurs.

Un seul travail d'effacement sécurisé est autorisé à la fois. Vous devez attendre que le travail en cours se termine avant de démarrer un autre travail d'effacement sécurisé.

L'effacement d'unités très volumineuses peut prendre plusieurs heures.

Vous ne pouvez pas effacer de manière sécurisée les volumes SSD SATA connectés à des contrôleurs RAID Marvell. Suivez plutôt les recommandations suivantes.

- Pour des disques SSD SATA 7 mm, connectez des contrôleurs Broadcom RAID afin de procéder à un effacement sécurisé.
- Pour les disques SSD M.2 SATA, connectez des contrôleurs Marvell non-RAID (par exemple, un kit d'activation à 2 baies ThinkSystem M.2 SATA/NVMe) afin de procéder à un effacement sécurisé.

À propos de cette tâche

Vous pouvez effacer les données des unités ci-après.
- NVMe
- SAS

- SAS HBA
- SAS RAID
- SATA
- Dispositifs de stockage branchés de manière externe
  - Lenovo Storage D1212 (MT 4587)
  - Lenovo Storage D1224 (MT 4587)
  - Lenovo Storage D3284 (MT 6413)

L'opération d'effacement sécurisé crée une entrée dans le journal d'audit. Vous pouvez réacheminer ces événements à l'aide de la fonction d'acheminement d'événement (voir Acheminement des événements vers syslog, un gestionnaire SNMP distant, un e-mail et d'autres services d'événement).

Pour résoudre les problèmes relatifs aux effacements sécurisés, voir Impossible d'effacer les données d'une unité bloquée de manière sécurisée et Impossible d'effacer de manière sécurisée les volumes SSD SATA une fois connectés à Marvell RAID dans la documentation en ligne de XClarity Administrator.

Procédure

Procédez comme suit pour effacer de manière sécurisée toutes les unités sur des serveurs gérés spécifiques.

Etape 1. Dans le menu XClarity Administrator, cliquez sur **Matériel → Serveurs**. La page Serveurs qui s'affiche présente une vue tabulaire de tous les serveurs gérés.

Etape 2. Sélectionnez le serveur.

Etape 3. Cliquez sur **Toutes les actions → Service → Effacement sécurisé de disque dur (HDD/SSD)**.

Etape 4. Saisissez votre mot de passe superviseur afin de confirmer que vous souhaitez bien effacer toutes les unités des serveurs sélectionnés

Etape 5. Cliquez sur **Effacer**.

Si vous choisissez d'exécuter un effacement d'unité de masse sur plus de trois serveurs, vous êtes invité(e) à saisir votre ID utilisateur, ainsi que votre mot de passe. Saisissez les mêmes données d'identification que celles utilisées pour vous connecter à XClarity Administrator.

Une travail est créé pour effectuer cette opération. Vous pouvez surveiller la progression des travaux en cliquant sur **Surveillance → Travaux** dans le menu XClarity Administrator. Si le travail ne s'est pas achevé avec succès, cliquez sur le lien Travail pour afficher des détails sur le travail (voir Surveillance des travaux).

Utilisation du contrôle à distance

À partir de l'interface Web de Lenovo XClarity Administrator, vous pouvez ouvrir une session de contrôle à distance à un serveur géré comme si vous opériez depuis une console locale. Vous pouvez utiliser la session de contrôle à distance pour effectuer des opérations, comme la mise sous tension ou hors tension du serveur et le montage d'une unité réseau ou locale de façon logique.

Pour lancer une session de contrôle à distance pour un appareil, vous devez disposer des privilèges **lxc-supervisor**, **lxc-admin**, **lxc-security-admin**, **lxc-fw-admin**, **lxc-os-admin**, **lxc-hw-admin**, **lxc-service-admin** ou **lxc-hw-manager**.

Utilisation du contrôle à distance pour gérer des serveurs ThinkSystem ou ThinkAgile

À partir de l'interface Web de Lenovo XClarity Administrator, vous pouvez ouvrir une session de contrôle à distance sur un serveur ThinkSystem ou ThinkAgile géré comme si vous opériez depuis une console locale.

Vous pouvez utiliser la session de contrôle à distance pour effectuer des opérations d'alimentation, monter une unité réseau ou locale de façon logique.

Avant de commencer

L'encapsulage doit être désactivée sur le serveur.

L'ouverture d'une session de contrôle à distance avec un serveur requiert que celui-ci soit à l'état En ligne ou Normal. Si l'état d'accès d'un serveur est tout autre, la session de contrôle à distance ne peut pas se connecter à ce serveur. Pour plus d'informations sur l'affichage de l'état du serveur, voir Affichage des détails d'un serveur géré.

Passez en revue les éléments suivants concernant les serveurs ThinkSystem SR635 et SR655.
- Le microprogramme du contrôleur de gestion de la carte mère v2.94 ou ultérieure est nécessaire.
- Le mode mono-utilisateur n'est pas pris en charge; seul le mode multi-utilisateur l'est.
- Internet Explorer 11 n'est pas pris en charge.
- Vous ne pouvez pas mettre sous tension et hors tension un serveur à partir d'une session de contrôle à distance.

À propos de cette tâche

Vous pouvez lancer une session de contrôle à distance sur un seul serveur ThinkSystem ou ThinkAgile à partir de XClarity Administrator.

Pour plus d'informations sur l'utilisation des fonctions de console distante et de support éloigné, voir la documentation sur le serveur ThinkSystem ou ThinkAgile.

Remarque : Pour les serveurs ThinkSystem et ThinkAgile, il n'est pas nécessaire d'utiliser Java Runtime Environment (JRE) avec la prise en charge de Java WebStart.

Procédure

Pour ouvrir une session de contrôle à distance avec un serveur spécifique, procédez comme suit :

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Serveurs**. La page Serveurs qui s'affiche présente une vue tabulaire de tous les serveurs gérés (serveurs rack et nœuds de traitement).

Vous pouvez trier les colonnes du tableau afin de faciliter la recherche de serveurs spécifiques. En outre, vous pouvez sélectionner un type de système dans la liste déroulante **Tous les systèmes** et saisir un texte (par exemple, un nom ou une adresse IP) dans la zone **Filtre** pour filtrer davantage l'affichage des serveurs.

Etape 2. Sélectionnez le serveur avec lequel vous souhaitez ouvrir une session de contrôle à distance.

Etape 3. Cliquez sur l'icône **Contrôle à distance** ().

Etape 4. Acceptez tous les avertissements de sécurité provenant de votre navigateur Web.

Après avoir terminé

Si la session de contrôle à distance ne s'ouvre pas correctement, voir Problèmes liés au contrôle à distance dans la documentation en ligne de XClarity Administrator.

Utilisation du contrôle à distance pour gérer des serveurs ThinkServer et NeXtScale sd350 M5

À partir de l'interface Web de Lenovo XClarity Administrator, vous pouvez ouvrir une session de contrôle à distance pour gérer des serveurs ThinkServer et NeXtScale sd350 M5 comme si vous opériez depuis une console locale. Vous pouvez utiliser la session de contrôle à distance pour effectuer des opérations d'alimentation et de réinitialisation, monter une unité réseau ou locale de façon logique sur le serveur et réaliser des captures d'écran et enregistrer des vidéos.

Avant de commencer

- Le contrôle à distance de ces serveurs requiert un environnement Java Runtime (JRE) avec la prise en charge de Java WebStart installé côté client. Un JDK en source ouverte est fortement recommandé. Si vous utilisez le JRE ou le JDK d'un fournisseur, assurez-vous qu'il est correctement sous licence pour un usage commercial. Les environnements JRE suivants sont pris en charge.
  - Oracle JRE 7 (voir Site Web de téléchargement d'Oracle Java)

    Attention :
    - Java 7 requiert au minimum une prise en charge TLSv1.2 (voir Configuration des paramètres cryptographiques sur le serveur de gestion).
    - La prise en charge de Java 7 sera obsolète ultérieurement.
  - Oracle JRE 8, qui nécessite une licence payante (voir Site Web de téléchargement d'Oracle Java)
  - Adoptium OpenJDK 8 avec le plug-in IcedTea-Web v1.8 (voir Site Web Adoptium OpenJDK)
  - Amazon Corretto 8 (voir Site Web de téléchargement Amazon Corretto 8)

  Java WebStart n'est pas inclus dans les modules d'installation OpenJDK ou Coretto et doit être installé séparément. IcedTea-Web ou OpenWebStart peut être utilisé avec la licence GNU GPLV2 (voir Site Web de téléchargement IcedTea-OpenJDK et Site Web OpenWebStart).
- Le contrôle à distance requiert l'installation d'une clé Features on Demand (FoD) pour la mise à niveau de ThinkServer System Manager Premium sur les serveurs ThinkServer. Pour plus d'informations sur les clés FoD installées sur vos serveurs, voir Affichage des clés Features on Demand (FoD) .

À propos de cette tâche

Vous pouvez lancer une session de contrôle à distance sur un seul serveur ThinkServer à partir de XClarity Administrator.

L'ouverture d'une session de contrôle à distance avec un serveur requiert que celui-ci soit à l'état En ligne ou Normal. Si l'état d'accès d'un serveur est tout autre, la session de contrôle à distance ne peut pas se connecter à ce serveur. Pour plus d'informations sur l'affichage de l'état du serveur, voir Affichage des détails d'un serveur géré.

Pour plus d'informations sur l'utilisation des fonctions de console distante et de support distant ThinkServer, voir la documentation sur le serveur ThinkServer.

Procédure

Pour ouvrir une session de contrôle à distance avec un serveur spécifique, procédez comme suit :

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Serveurs**. La page Serveurs qui s'affiche présente une vue tabulaire de tous les serveurs gérés (serveurs rack et nœuds de traitement).

Vous pouvez trier les colonnes du tableau afin de faciliter la recherche de serveurs spécifiques. En outre, vous pouvez sélectionner un type de système dans la liste déroulante **Tous les systèmes** et saisir un texte (par exemple, un nom ou une adresse IP) dans la zone **Filtre** pour filtrer davantage l'affichage des serveurs.

Etape 2. Sélectionnez le serveur avec lequel vous souhaitez ouvrir une session de contrôle à distance.

Etape 3. Cliquez sur l'icône **Contrôle à distance** ().

Etape 4. Acceptez tous les avertissements de sécurité provenant de votre navigateur Web.

Après avoir terminé

Si la session de contrôle à distance ne s'ouvre pas correctement, voir Problèmes liés au contrôle à distance dans la documentation en ligne de XClarity Administrator.

Utilisation du contrôle à distance pour gérer des serveurs Converged, Flex System, NeXtScale et System x

À partir de l'interface Web de Lenovo XClarity Administrator, vous pouvez ouvrir une session de contrôle à distance pour gérer des serveurs Converged, Flex System, NeXtScale et System x comme si vous opériez depuis une console locale.

Avant de commencer

En savoir plus :  XClarity Administrator : Contrôle à distance

- Le contrôle à distance de ces serveurs requiert un environnement Java Runtime (JRE) avec la prise en charge de Java WebStart installé côté client. Un JDK en source ouverte est fortement recommandé. Si vous utilisez le JRE ou le JDK d'un fournisseur, assurez-vous qu'il est correctement sous licence pour un usage commercial. Les environnements JRE suivants sont pris en charge.
  - Oracle JRE 7 (voir Site Web de téléchargement d'Oracle Java)

    Attention :
    - Java 7 requiert au minimum une prise en charge TLSv1.2 (voir Configuration des paramètres cryptographiques sur le serveur de gestion).
    - La prise en charge de Java 7 sera obsolète ultérieurement.
  - Oracle JRE 8, qui nécessite une licence payante (voir Site Web de téléchargement d'Oracle Java)
  - Adoptium OpenJDK 8 avec le plug-in IcedTea-Web v1.8 (voir Site Web Adoptium OpenJDK)
  - Amazon Corretto 8 (voir Site Web de téléchargement Amazon Corretto 8)

  Java WebStart n'est pas inclus dans les modules d'installation OpenJDK ou Coretto et doit être installé séparément. IcedTea-Web ou OpenWebStart peut être utilisé avec la licence GNU GPLV2 (voir Site Web de téléchargement IcedTea-OpenJDK et Site Web OpenWebStart).
- Vous pouvez lancer une session de contrôle à distance sur des serveurs exécutant les systèmes d'exploitation suivants (32 bits ou 64 bits) :
  - Microsoft Windows 7
  - Microsoft Windows 8
  - Microsoft Windows 10
- Le contrôle à distance nécessite l'installation d'une clé Features on Demand (FoD) de présence à distance sur les serveurs Converged, NeXtScale et System x. Si la clé FoD n'est pas détectée sur un serveur, le message `Clé d'activation manquante` apparaît pour ce serveur dans la session de contrôle à distance lors de l'affichage de la liste des serveurs disponibles. Vous pouvez déterminer si la présence à distance est activée, désactivée ou non installée sur un serveur depuis la page Serveurs (voir Affichage de l'état d'un serveur géré). Pour plus d'informations sur les clés FoD installées sur vos serveurs, voir Affichage des clés Features on Demand (FoD).
- Le compte utilisateur utilisé pour démarrer la session de contrôle à distance doit être un compte utilisateur valide ayant été défini dans le serveur d'authentification de XClarity Administrator. Le compte utilisateur doit également disposer des droits d'utilisateur suffisants pour accéder à un serveur et le gérer.

- Prenez connaissance des remarques concernant la sécurité, les performances et le clavier avant d'ouvrir une session de contrôle à distance. Pour plus d'informations sur ces remarques, voir Considérations relatives au contrôle à distance.
- La boîte de dialogue Contrôle à distance utilise les paramètres d'environnement local et de langue d'affichage qui sont définis pour le système d'exploitation installé sur votre système local.Si votre système local s'exécute sous Windows, voir le Site Web Java pour connaître la procédure de modification du paramètre d'environnement local. Pour modifier la langue d'affichage, installez une copie localisée de Windows ou installez un module linguistique à partir du Site Web Windows.

À propos de cette tâche

Vous pouvez démarrer plusieurs sessions de contrôle à distance à partir de Lenovo XClarity Administrator. Chaque session peut gérer plusieurs serveurs.

L'ouverture d'une session de contrôle à distance avec un serveur requiert que celui-ci soit à l'état En ligne ou Normal. Si l'état d'accès d'un serveur est tout autre, la session de contrôle à distance ne peut pas se connecter à ce serveur. Pour plus d'informations sur l'affichage de l'état du serveur, voir Affichage des détails d'un serveur géré.

Vous pouvez ouvrir une session de contrôle à distance non ciblée en cliquant sur **Distribution → Contrôle à distance** dans la barre de menus de Lenovo XClarity Administrator. Acceptez ensuite tous les avertissements de sécurité provenant de votre navigateur Web.

Remarque : Pour les nœuds de traitement Flex System x280, x480 et x880, vous ne pouvez démarrer une session de contrôle à distance qu'avec le nœud principal. Si vous tentez de démarrer une session de contrôle à distance avec un nœud qui n'est pas le nœud principal d'un système multinœud, le contrôle à distance démarre, mais aucune vidéo ne s'affiche.

Procédure

Procédez comme suit pour ouvrir une session de contrôle à distance avec un serveur Converged, Flex System, NeXtScale et System x spécifique.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Serveurs**. La page Serveurs qui s'affiche présente une vue tabulaire de tous les serveurs gérés (serveurs rack et nœuds de traitement).

Vous pouvez trier les colonnes du tableau afin de faciliter la recherche de serveurs spécifiques. En outre, vous pouvez sélectionner un type de système dans la liste déroulante **Tous les systèmes** et saisir un texte (par exemple, un nom ou une adresse IP) dans la zone **Filtre** pour filtrer davantage l'affichage des serveurs.

Etape 2. Sélectionnez le serveur avec lequel vous souhaitez ouvrir une session de contrôle à distance.

Etape 3. Cliquez sur l'icône **Contrôle à distance** ().

Etape 4. Acceptez tous les avertissements de sécurité provenant de votre navigateur Web.

Etape 5. Vous pouvez éventuellement choisir d'enregistrer l'icône de contrôle à distance sur votre bureau. Vous pouvez utiliser cette icône pour lancer une session de contrôle à distance sans vous connecter à l'interface Web de XClarity Administrator.

Etape 6. Lorsque vous y êtes invité, sélectionnez l'un des modes de connexion suivants :

- **Mode mono-utilisateur**. Établit une session de contrôle à distance exclusive avec le serveur. Toutes les autres sessions de contrôle à distance avec ce serveur sont bloquées jusqu'à ce que vous vous déconnectiez de celui-ci. Cette option n'est disponible que si aucune autre session de contrôle à distance n'est établie avec le serveur.

- **Mode multi-utilisateur**. Permet d'établir plusieurs sessions de contrôle à distance avec le même serveur. XClarity Administrator prend en charge jusqu'à six sessions de contrôle à distance simultanées avec un serveur.

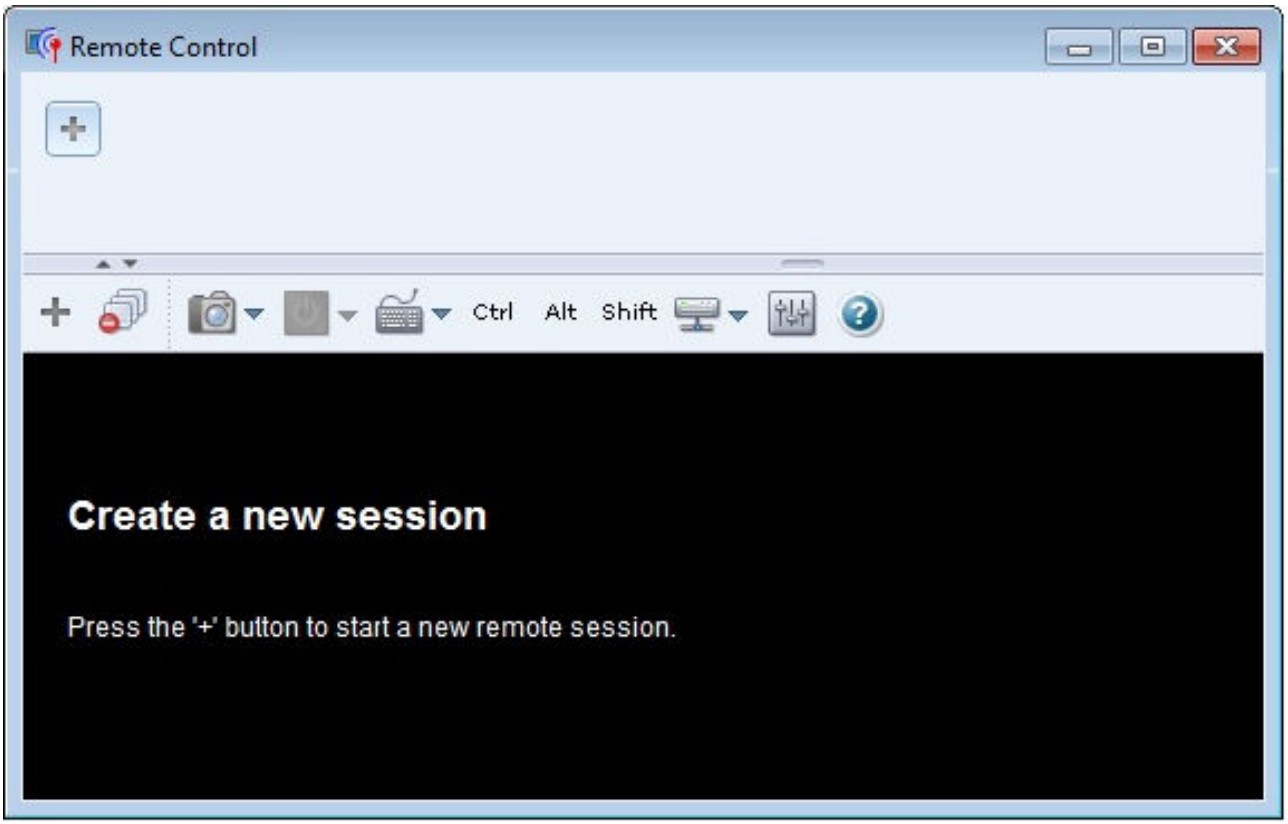
Etape 7. Lorsque vous y êtes invité, indiquez si vous souhaitez enregistrer un raccourci vers la session de contrôle à distance sur votre système local.

Si vous enregistrez le raccourci, vous pouvez ensuite l'utiliser pour ouvrir une session de contrôle à distance avec le serveur spécifié sans avoir à le faire à partir de l'interface Web de XClarity Administrator. Toutefois, votre système local doit avoir accès à XClarity Administrator pour valider le compte utilisateur à l'aide du serveur d'authentification de XClarity Administrator.

Le raccourci contient un lien qui ouvre une session de contrôle à distance vide à laquelle vous pouvez ajouter manuellement des serveurs.

Résultats

La fenêtre Contrôle à distance s'affiche.



La zone des miniatures contient les miniatures de toutes les sessions de serveur gérées par le biais de la session de contrôle à distance.

Vous pouvez afficher plusieurs de sessions de serveur et passer de l'une à l'autre en cliquant sur une miniature, qui affiche alors la console de serveur dans la zone de session vidéo. Si vous accédez à plus de serveurs que ne peut en contenir la zone des miniatures, cliquez sur l'icône **Défiler vers la droite** ( ) et sur l'icône **Défiler vers la gauche** ( ) pour accéder aux autres miniatures de serveur. Cliquez sur l'icône **Toutes les sessions** ( ) pour afficher la liste de toutes les sessions de serveur ouvertes.

À partir de la zone des miniatures, cliquez sur l'icône **Ajouter un serveur** () pour ajouter un nouveau serveur à la liste de serveurs que vous gérez. Pour plus d'informations sur l'ajout d'une session, voir Ajout d'une console de serveur à une session de contrôle à distance. Sur la page Miniature, vous pouvez choisir si la zone des miniatures doit s'afficher, ainsi que la fréquence d'actualisation des miniatures. Pour plus d'informations sur les paramètres de miniature, voir Définition de préférences de contrôle à distance.

Après avoir terminé

Si la session de contrôle à distance ne s'ouvre pas correctement, voir Problèmes liés au contrôle à distance dans la documentation en ligne de XClarity Administrator.

La boîte de dialogue Contrôle à distance vous permet d'effectuer les actions suivantes :

- Ajouter une session avec d'autres serveurs à la session de contrôle à distance en cours (voir Ajout d'une console de serveur à une session de contrôle à distance).
- Masquer ou afficher la zone des miniatures en cliquant sur l'icône **Activer les miniatures** ().
- Afficher la session de contrôle à distance en mode fenêtre ou en mode plein écran en cliquant sur l'icône **Écran** (), puis en cliquant sur **Activer le plein écran** ou **Désactiver le plein écran**.
- Utiliser les touches Ctrl, Alt et Maj dans une session de contrôle à distance (voir Utilisation des touches Ctrl, Alt et Maj).
- Définir des séquences de touches personnalisées, appelées touches de fonction (voir Définition de touches de fonction).
- Effectuer une capture d'écran de la session de serveur sélectionnée et l'enregistrer dans différents formats en cliquant sur l'icône **Écran** (), puis en cliquant sur **Capture d'écran**.
- Monter un support distant (par exemple, un dispositif de CD, DVD ou USB, une image de disque ou une image de CD (ISO)) sur le serveur sélectionné ou déplacer un support monté vers un autre serveur (voir Montage ou déplacement d'un support distant).
- Télécharger des images vers un serveur à partir d'un support distant (voir Téléchargement d'une image sur le serveur).
- Mettre le serveur sous tension ou hors tension à partir d'une console distante (voir Mise sous tension et hors tension d'un serveur à partir d'une session de contrôle à distance).
- Modifier les préférences de contrôle à distance (voir Définition de préférences de contrôle à distance).

Considérations relatives au contrôle à distance

Prenez connaissance des remarques sur la sécurité, les performances et le clavier qui s'appliquent dans le cadre de l'accès aux serveurs gérés à l'aide d'une session de contrôle à distance.

Remarques liées à la sécurité

Le compte utilisateur utilisé pour démarrer la session de contrôle à distance doit être un compte utilisateur valide ayant été défini dans le serveur d'authentification de Lenovo XClarity Administrator. Le compte utilisateur doit également disposer des droits d'utilisateur suffisants pour accéder à un serveur et le gérer.

Par défaut, plusieurs sessions de contrôle à distance peuvent être établies avec serveur. Toutefois, lorsque vous démarrez une session de contrôle à distance, vous avez la possibilité de démarrer la session en mode mono-utilisateur, ce qui établit une session exclusive avec le serveur. Toutes les autres sessions de contrôle à distance avec ce serveur sont bloquées jusqu'à ce que vous vous déconnectiez de celui-ci.

Remarque : Cette option n'est disponible que si aucune autre session de contrôle à distance n'est actuellement établie avec le serveur.

Pour utiliser la forme FIPS (Federal Information Processing Standard) 140, vous devez l'activer manuellement en procédant comme suit sur le système local :

1. Recherchez le nom du fournisseur cryptographique certifié FIPS 140 qui est installé sur le système local.

   Astuce : Pour plus d'informations sur la conformité avec la norme FIPS 140, voir le Site Web FIPS 140 Mode conforme pour SunJSSE.
2. Éditez le fichier `$(java.home)/lib/security/java.security`.
3. Modifiez la ligne contenant `com.sun.net.ssl.internal.ssl.Provider` en y ajoutant le nom du fournisseur cryptographique certifié FIPS 140. Par exemple, remplacez :
   `security.provider.4=com.sun.net.ssl.internal.ssl.Provider`
   par :
   `security.provider.4=com.sun.net.ssl.internal.ssl.Provider SunPKCS11-NSS`

Remarques sur les performances

Si une session de contrôle à distance ralentit ou ne répond plus, fermez toutes les sessions multimédia à distance et vidéo que vous avez établies avec le serveur sélectionné afin de réduire le nombre de connexions de serveur ouvertes. En outre, vous pouvez augmenter les performances en modifiant les préférences suivantes. Pour plus d'informations, voir Définition de préférences de contrôle à distance.

- **KVM**
  - Réduisez le pourcentage de bande passante vidéo qui est utilisée par l'application. La qualité de l'image de la session de contrôle à distance sera réduite.
  - Réduisez le pourcentage de cadres qui sont actualisés par l'application. La fréquence d'actualisation de la session de contrôle à distance sera réduite.
- **Miniatures**
  - Réduisez l'intervalle d'actualisation des miniatures. L'application va actualiser les miniatures à un rythme plus lent.
  - Désactivez complètement l'affichage des miniatures.

La taille de la fenêtre de session de contrôle à distance et le nombre de sessions actives peuvent avoir une incidence sur les ressources du poste de travail, telles que la mémoire et la bande passante du réseau, ce qui peut affecter les performances. La session de contrôle à distance utilise une limite logicielle de 32 sessions ouvertes. Si plus de 32 sessions sont ouvertes, il se peut que les performances soient considérablement dégradées et que la session de contrôle à distance ne réponde plus. Vous pourrez constater une dégradation des performances avec moins de 32 sessions ouvertes si les ressources, y compris la bande passante de réseau et la mémoire locale, ne sont pas suffisantes.

Remarques sur le clavier

La session de contrôle à distance prend en charge les types de clavier suivants :

- 105 touches (belge)
- Portugais (Brésil)
- Chinois
- 105 touches (français)
- 105 touches (allemand)
- 105 touches (italien)
- 109 touches (japonais)
- Coréen
- Portugais
- Russe
- 105 touches (espagnol)
- 105 touches (suisse)
- 105 touches (anglais)

- 104 touches (américain)

Pour plus d'informations sur les préférences de clavier, voir Définition de préférences de contrôle à distance.

Ajout d'une console de serveur à une session de contrôle à distance

Vous pouvez ajouter une ou plusieurs consoles de serveur à la session de contrôle à distance en cours.

Procédure

Pour ajouter une ou plusieurs consoles de serveur à la session de contrôle à distance en cours, procédez comme suit.

Etape 1. Dans la fenêtre Contrôle à distance, cliquez sur l'icône **Nouvelle session** ().

Une boîte de dialogue s'affiche avec la liste des châssis et serveurs rack disponibles qui sont gérés par Lenovo XClarity Administrator et que votre compte utilisateur est autorisé à gérer.

Conseil : Si la liste ne contient aucun serveur, voir Problèmes liés au contrôle à distance dans la documentation en ligne de XClarity Administrator pour savoir comment résoudre le problème.

Etape 2. Sélectionnez un ou plusieurs serveurs auxquels vous souhaitez établir une connexion.

Vous pouvez filtrer l'affichage des serveurs en sélectionnant un type de système dans la liste déroulante **Type** et en saisissant un texte (par exemple, un nom de système ou un nom de boîtier) dans la zone **Filtre**.

Vous pouvez choisir **Sélectionner tout** pour sélectionner tous les serveurs de la liste.

Etape 3. **Facultatif :** Sélectionnez **Mode mono-utilisateur** pour ouvrir une session exclusive avec chaque serveur sélectionné.

Si vous sélectionnez cette option, toutes les autres sessions de contrôle à distance avec les serveurs sélectionnés sont bloquées jusqu'à ce que vous vous déconnectiez de ces serveurs. Cette option n'est disponible que si aucune autre session de contrôle à distance n'est établie avec les serveurs sélectionnés.

Si vous ne sélectionnez pas cette option, le mode multi-utilisateurs est utilisé par défaut.

Etape 4. Cliquez sur **Connecter**.

Mise sous tension et hors tension d'un serveur à partir d'une session de contrôle à distance

Vous pouvez mettre sous tension et hors tension un serveur à partir d'une session de contrôle à distance.

Procédure

Procédez comme suit pour mettre sous tension et hors tension un serveur.

Etape 1. Dans la fenêtre Contrôle à distance, cliquez sur la miniature correspondant au serveur que vous souhaitez mettre sous tension ou hors tension.

Etape 2. Cliquez sur l'icône **Alimentation** (), puis sur l'une des actions d'alimentation suivantes :
- **Mettre sous tension**
- **Mettre hors tension normalement**
- **Mettre hors tension immédiatement**
- **Redémarrer normalement**
- **Redémarrer immédiatement**
- **Déclencher NMI**

- **Redémarrer sur la configuration système** (serveurs Lenovo Converged, Flex System, NeXtScale et System x uniquement)

Astuce : L'icône **Alimentation** est verte si le serveur est sous tension.

Définition de touches de fonction

Vous pouvez définir vos propres séquences de touches personnalisées, appelées *touches de fonction*, pour la session de contrôle à distance en cours.

Avant de commencer

Pour afficher la liste actuelle des définitions des touches de fonction, cliquez sur l'icône **Clavier** ().

Les définitions des touches de fonction sont stockées sur le système à partir duquel vous avez démarré la session de contrôle à distance. Par conséquent, si vous lancez la session de contrôle à distance à partir d'un autre système, vous devez les redéfinir.

Vous pouvez choisir d'exporter des paramètres utilisateur (ce qui inclut les touches de fonction) à partir de l'onglet **Paramètres utilisateur** de la boîte de dialogue Préférences. Pour plus d'informations, voir Importation et exportation de paramètres utilisateur.

Remarque : Si vous utilisez un clavier international et que vous définissez des touches de fonction impliquant la touche AltGr, vérifiez que le type du système d'exploitation installé sur le poste de travail que vous utilisez pour appeler l'application de contrôle à distance est identique au type du système d'exploitation qui est installé sur le serveur auquel vous accédez à distance. Par exemple, si le serveur s'exécute sous Linux, prenez soin d'appeler la session de contrôle à distance à partir d'un poste de travail qui s'exécute sous Linux.

Procédure

Procédez comme suit pour ajouter une touche de fonction.

Etape 1. Dans la fenêtre Contrôle à distance, cliquez sur l'icône **Clavier** (), puis sur **Ajouter une touche de fonction**. L'onglet **Programmateur de touche de fonction** de la boîte de dialogue Préférence s'affiche.

Etape 2. Cliquez sur **Nouveau**.

Etape 3. Saisissez la séquence de touches que vous souhaitez à définir.

Etape 4. Cliquez sur **OK**. La nouvelle touche de fonction est ajoutée à la liste de touches de fonction.

Utilisation des touches Ctrl, Alt et Maj

Certains systèmes d'exploitation interceptent certaines touches au lieu de les transmettre au serveur distant. Vous pouvez utiliser les touches rémanentes pour envoyer des frappes directement au serveur que vous gérez.

Procédure

Pour envoyer une combinaison de touches avec Ctrl ou Alt, cliquez sur le bouton **Ctrl** ou **Alt** dans la barre d'outils, placez le curseur dans la zone de session vidéo et appuyez sur une touche du clavier.

Par exemple, pour envoyer la combinaison de touches Ctrl+Alt+Suppr, procédez de la manière suivante :

1. Cliquez sur **Ctrl** dans la barre d'outils.
2. Cliquez sur **Alt** dans la barre d'outils.
3. Cliquez avec le bouton gauche de la souris à un endroit quelconque de la zone de session vidéo.

4. Appuyez sur la touche Suppr du clavier.

Remarque : Si le mode capture de la souris est activé, appuyez sur la touche Alt située à gauche du clavier pour déplacer le curseur en dehors de la zone de session vidéo. Le mode capture de la souris est désactivé par défaut, mais vous pouvez l'activer à partir de la page Barre d'outils (voir Définition de préférences de contrôle à distance).

Lorsque vous cliquez sur **Ctrl**, **Alt** ou **Maj** dans la barre d'outils pour rendre la touche active, celle-ci reste active jusqu'à ce que vous appuyiez sur une touche du clavier ou cliquiez à nouveau sur le bouton.

Montage ou déplacement d'un support distant

Vous pouvez utiliser la fonction de support distant pour monter un support distant (par exemple, un dispositif de CD, DVD ou USB, une image de disque ou une image de CD (ISO)) du système local sur le serveur sélectionné. Vous pouvez également télécharger une image vers le stockage local disponible sur le contrôleur de gestion de la carte mère.

Avant de commencer

Un seul utilisateur à la fois peut monter et télécharger des données vers le stockage local disponible sur le contrôleur de gestion. Les autres utilisateurs sont empêchés d'accéder au stockage local disponible sur le contrôleur de gestion lorsqu'il est en cours de montage ou que des données sont en cours de téléchargement vers le stockage local.

Sur un serveur exécutant le système d'exploitation Linux, le montage de plusieurs images ISO n'est pas pris en charge.

Procédure

Procédez comme suit pour monter ou déplacer un support distant.

Etape 1. Dans la fenêtre Contrôle à distance, cliquez sur l'icône **Support distant** ().

Etape 2. Cliquez sur l'une des actions suivantes :

- **Monter un support éloigné**

  Cette action met à disposition du serveur sélectionné les ressources de stockage locales. Une ressource de stockage ne peut être montée sur un seul serveur à la fois dans une même session de contrôle à distance.

  Lorsque vous cliquez sur **Monter un support éloigné**, les options suivantes sont disponibles :

  - **Sélectionner une image à monter**. L'image est disponible pour le serveur sélectionné jusqu'à ce que vous démontiez l'appareil ou que vous fermiez la session de contrôle à distance. Plusieurs images peuvent être montées sur un même serveur et chaque image peut être montée sur plusieurs serveurs.
  - **Sélectionner un appareil, par exemple, une unité de CD, DVD, ou USB, qui doit être montée**. L'appareil est disponible pour le serveur sélectionné jusqu'à ce que vous démontiez l'unité ou que vous fermiez la session de contrôle à distance. Plusieurs appareils peuvent être montés sur un même serveur, mais chaque appareil ne peut être monté que sur un seul serveur à la fois.

    Remarque : Si vous sélectionnez une unité, veillez à la démonter avant de retirer le support de l'unité.
  - **Télécharger l'image vers le module IMM**. Utilisez cette option pour stocker une image dans le stockage local disponible sur le contrôleur de gestion pour le serveur sélectionné.

L'image reste sur le contrôleur de gestion même si vous mettez fin à la session de contrôle à distance ou si le serveur est redémarré.

Environ 50 Mo de données peuvent être stockés sur le contrôleur de gestion.

Vous pouvez télécharger plusieurs images vers le contrôleur de gestion, à condition que l'espace total utilisé pour l'ensemble de ces images soit inférieur à 50 Mo.

Chaque image qui est chargée sur le contrôleur de gestion est automatiquement montée sur le serveur. Une fois que vous avez téléchargé une image sur le contrôleur de gestion, vous pouvez déplacer cette image sur le contrôleur de gestion d'un autre serveur. Lorsque vous déplacez l'image, l'image précédemment téléchargée est retirée sur le serveur actuel et téléchargée sur un serveur sélectionné.

- **Déplacer un support éloigné**

  Cette action déplace une ressource de stockage déjà montée d'un serveur à un autre.

  Procédez comme suit pour mettre une ressource à disposition d'un serveur :

  1. Sélectionnez une ou plusieurs ressources.
  2. Cliquez sur **Ajouter** pour déplacer les ressources vers la liste **Ressources sélectionnées**.
  3. Cliquez sur **Monter** pour monter les ressources en vue de leur utilisation par le serveur. La session de contrôle à distance définit un appareil pour la ressource et mappe cet appareil à un point de montage sur le serveur sélectionné. Vous avez la possibilité de protéger le support monté contre l'écriture.

Téléchargement d'une image sur le serveur

Vous pouvez également télécharger une image vers le stockage local disponible sur le contrôleur de gestion de la carte mère du serveur sélectionné.

À propos de cette tâche

L'image reste sur le contrôleur de gestion même si vous mettez fin à la session de contrôle à distance ou si le serveur est redémarré.

Environ 50 Mo de données peuvent être stockés sur le contrôleur de gestion.

Vous pouvez télécharger plusieurs images vers le contrôleur de gestion, à condition que l'espace total utilisé pour l'ensemble de ces images soit inférieur à 50 Mo.

Chaque image qui est chargée sur le contrôleur de gestion est automatiquement montée sur le serveur. Une fois que vous avez téléchargé une image sur le contrôleur de gestion, vous pouvez déplacer cette image sur le contrôleur de gestion d'un autre serveur. Lorsque vous déplacez l'image, l'image précédemment téléchargée est retirée sur le serveur actuel et téléchargée sur un serveur sélectionné.

Procédure

Procédez comme suit pour télécharger une image vers le serveur.

Etape 1. Dans la fenêtre Contrôle à distance, cliquez sur l'icône **Support distant** ().

Etape 2. Cliquez sur **Monter un support éloigné**.

Etape 3. Cliquez sur **Télécharger l'image vers le module IMM**.

Importation et exportation de paramètres utilisateur

Vous pouvez choisir d'importer ou d'exporter des paramètres utilisateur pour la session de contrôle à distance en cours.

À propos de cette tâche

Lorsque vous exportez des paramètres utilisateur, tous les paramètres utilisateur de la session de contrôle à distance en cours sont stockées dans un fichier de propriétés sur votre système local. Vous pouvez copier ce fichier de propriétés sur un autre système et importer ces paramètres dans l'application de contrôle à distance pour les utiliser.

Procédure

Procédez comme suit pour importer ou exporter des paramètres utilisateur pour la session de contrôle à distance en cours.

Etape 1. Dans la fenêtre Contrôle à distance, cliquez sur l'icône **Préférence** ().

Etape 2. Cliquez sur l'onglet **Paramètres utilisateur**.

Etape 3. Cliquez sur **Importer** pour importer des paramètres à partir d'un fichier exporté ou cliquez sur **Exporter** pour enregistrer tous les paramètres utilisateur en cours dans un fichier de propriétés sur le système local.

Définition de préférences de contrôle à distance

Vous pouvez modifier les paramètres de préférence de la session de contrôle à distance en cours.

Procédure

Procédez comme suit pour modifier les préférences de contrôle à distance.

Etape 1. Pour modifier les paramètres de contrôle à distance, cliquez sur l'icône **Préférences** (). Toutes ces modifications prennent effet immédiatement.

- **KVM**
  - **Pourcentage de bande passante vidéo**. L'augmentation de la bande passante améliore la qualité visuelle de la session de contrôle à distance, mais peut affecter ses performances.
  - **Pourcentage de trames actualisées**. L'augmentation du pourcentage d'actualisation des images accroît la fréquence de mise à jour de la session de contrôle à distance, mais peut affecter ses performances.
  - **Type de clavier**. Sélectionnez le type de clavier utilisé pour la session de contrôle à distance. Le type de clavier que vous sélectionnez doit correspondre aux paramètres de clavier définis dans le système local, ainsi qu'aux paramètres de clavier définis sur l'hôte distant.

    Remarque : Si vous sélectionnez un clavier international et que vous devez utiliser des combinaisons de touches impliquant la touche AltGr, vérifiez que le type du système d'exploitation installé sur le poste de travail que vous utilisez pour appeler la session de contrôle à distance est identique au type du système d'exploitation qui est installé sur le serveur auquel vous souhaitez accéder à distance. Par exemple, si le serveur s'exécute sous Linux, prenez soin d'appeler l'application de contrôle à distance à partir d'un poste de travail qui s'exécute sous Linux.
  - **Dimensionner l'image à la fenêtre**. Sélectionnez cette option pour adapter l'image vidéo qui est reçue de la part du serveur à la taille de la zone de session vidéo.
- **Sécurité**
  - **Préférer les connexions en mode mono-utilisateur**. Indiquez si les connexions en mode mono-utilisateur correspondent à la sélection par défaut lorsque vous vous connectez à un serveur. Lorsqu'une connexion est établie en mode mono-utilisateur, un seul utilisateur à la fois peut être connecté au serveur. Si cette case n'est pas cochée, le comportement par défaut consiste à se connecter au serveur en mode multi-utilisateurs.

- **Exiger des connexions de tunnellisation (sécurisées)**. Sélectionnez cette option pour accéder à un serveur via le nœud de gestion. Vous pouvez utiliser cette option pour accéder à un serveur à partir d'un client qui n'est pas sur le même réseau que lui.

  Remarque : L'application de contrôle à distance tente toujours de se connecter directement au serveur à partir du système local sur lequel le contrôle à distance a été lancé. Si vous sélectionnez cette option, l'application de contrôle à distance accède au serveur via Lenovo XClarity Administrator si le poste de travail client n'arrive pas à y accéder directement.

- **Barre d'outils**

  Remarque : Cliquez sur **Restaurer les valeurs par défaut** pour restaurer la valeur par défaut de tous les paramètres répertoriés sur cette page.

  - **Epingler la barre d'outils à la fenêtre**. Par défaut, la barre d'outils est masquée au-dessus de la fenêtre de session de contrôle à distance et n'apparaît que lorsque vous la survolez avec le pointeur de votre souris. Si vous sélectionnez cette option, la barre d'outils est épinglée à la fenêtre et apparaît toujours entre le panneau des miniatures et la fenêtre de session de contrôle à distance.
  - **Afficher les touches du clavier**. Indiquez si vous souhaitez afficher les icônes des touches du clavier (Maj, Verr Num et Arrêt Défil) dans la barre d'outils.
  - **Afficher le contrôle d'alimentation**. Indiquez si vous souhaitez afficher les options de contrôle de l'alimentation dans la barre d'outils.
  - **Afficher les touches rémanentes**. Indiquez si vous souhaitez afficher les icônes des touches rémanentes (Ctrl, Alt et Suppr) dans la barre d'outils.
  - **Masquer le pointeur de souris local**. Indiquez si le pointeur de souris local doit apparaître lorsque vous placez le curseur dans la session de serveur qui est affichée dans la zone de session vidéo.
  - **Activer le mode capture avec la souris**. Par défaut, le mode capture de la souris est désactivé. Cela signifie que vous pouvez librement déplacer le curseur à l'intérieur et à l'extérieur de la zone de session vidéo. Si vous activez le mode capture avec la souris, vous devez appuyer sur la touche Alt située dans la partie gauche du clavier pour pouvoir déplacer le curseur hors de la zone de session vidéo. Si le mode capture de la souris est activé, vous pouvez choisir d'utiliser les touches Ctrl+Alt pour quitter ce mode. Le comportement par défaut est d'utiliser la touche Alt située sur la partie gauche du clavier.
  - **Spécifier l'opacité d'arrière-plan de la barre d'outils**. La réduction du pourcentage d'opacité permet de visualiser une plus grande partie de la zone de session vidéo en arrière-plan de la barre d'outils.

    Remarque : Cette option n'est disponible que lorsque la barre d'outils n'est pas épinglée à la fenêtre.

- **Miniatures**
  - **Afficher les miniatures**. Sélectionnez cette option pour afficher la zone des miniatures dans la session de contrôle à distance.
  - **Spécifier un intervalle d'actualisation des miniatures**. La réduction de l'intervalle d'actualisation augmente la fréquence de mise à jour des miniatures de serveur.
- **Dispositions générales**
  - **Mode débogage**. Indiquez si vous souhaitez mettre en place le mode débogage pour l'application de contrôle à distance. Ces paramètres déterminent la granularité des événements qui sont consignés dans les fichiers journaux. Par défaut, seuls les événements

graves sont consignés. Pour plus d'informations sur l'emplacement des fichiers journaux, voir Affichage des journaux et des traces de contrôle à distance.

- **Hériter des paramètres d'apparence du système**. Ce paramètre modifie la présentation pour la faire correspondre aux schémas de couleurs configurés pour le serveur local (fonctionnant sous Windows). Ces paramètres ne prennent effet qu'au redémarrage de l'application de console à distance.
- C**réer une icône de bureau**. Ce paramètre crée une icône de bureau sur votre système local pour que vous puissiez démarrer l'application de contrôle à distance directement depuis votre système. Vous devez toujours avoir accès au logiciel de gestion depuis votre système.
- **Synchroniser avec le serveur de gestion**. Ce paramètre garantit que les données du serveur qui s'affichent dans l'application de contrôle à distance correspondent aux données du serveur qui s'affichent dans le logiciel de gestion.

Affichage des journaux et des traces de contrôle à distance

Lorsque vous démarrez une session de contrôle à distance, des fichiers journaux sont créés. Les types des événements consignés dans ces fichiers varient en fonction du mode débogage, lequel est défini sur l'onglet **Général** de la boîte de dialogue Préférences. Vous pouvez utiliser ces fichiers journaux pour résoudre des problèmes.

Procédure

Les fichiers journaux de contrôle à distance sont stockés aux emplacements suivants.

Système d'exploitation	Répertoire du fichier journal
Windows 7 et 8	`%USERPROFILE%\lenovo\remoteaccess` Par exemple : `C:\Users\win_user\lenovo\remoteaccess`

Pour plus d'informations sur la collecte des fichiers de diagnostic et sur l'envoi de ces fichiers à Lenovo Support, voir Utilisation du service et support dans la documentation en ligne de Lenovo XClarity Administrator.

Gestion de l'accès aux systèmes d'exploitation sur les serveurs gérés

Vous pouvez gérer l'accès aux systèmes d'exploitation sur les serveurs gérés.

Avant de commencer

Vous devez disposer de droits **lxc-os-admin**, **lxc-supervisor**, **lxc-admin** ou **lxc-hw-admin** pour gérer et déployer des pilotes de périphérique SE et pour effectuer des actions d'alimentation sur des serveur gérés à partir de pages Mises à joue de pilote Windows.

À propos de cette tâche

Avant que Lenovo XClarity Administrator puisse mettre à jour les pilotes de périphérique SE sur un système géré, vous devez fournir des informations pour accéder au système d'exploitation hôte, notamment l'adresse IP SE et les données d'identification administrateur stockées pour l'accès au système d'exploitation hôte. Pour plus d'informations sur la mise à jour des pilotes de périphérique SE, voir Mise à jour des pilotes de périphérique Windows sur des serveurs gérés.

XClarity Administrator utilise des informations d'identification stockées pour s'authentifier auprès du système d'exploitation hôte. Pour plus d'informations sur la création de données d'identification stockées dans XClarity Administrator, voir Gestion de données d'identification stockées.

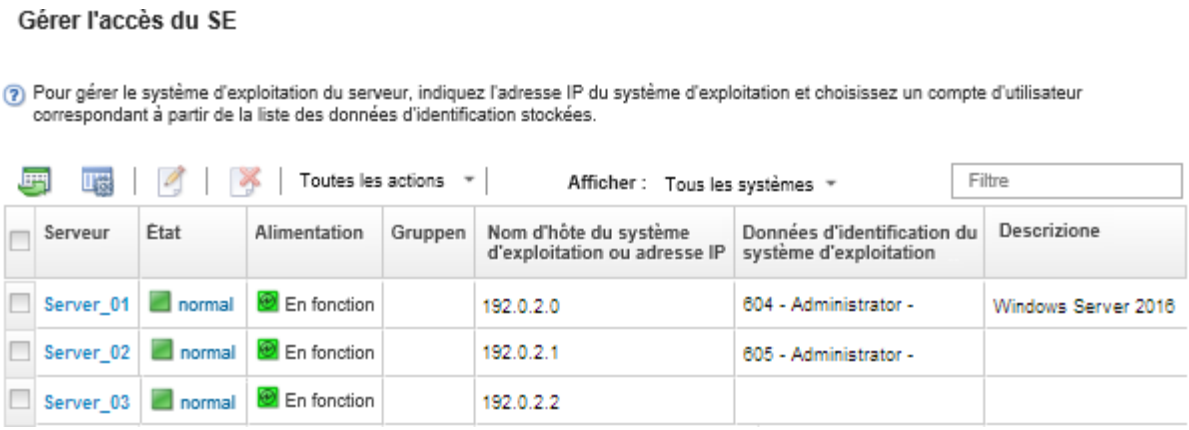
Conseil : XClarity Administrator ne valide pas automatiquement les informations que vous spécifiez sur cette page.

Procédure

Procédez comme suit pour modifier les propriétés du système d'exploitation.

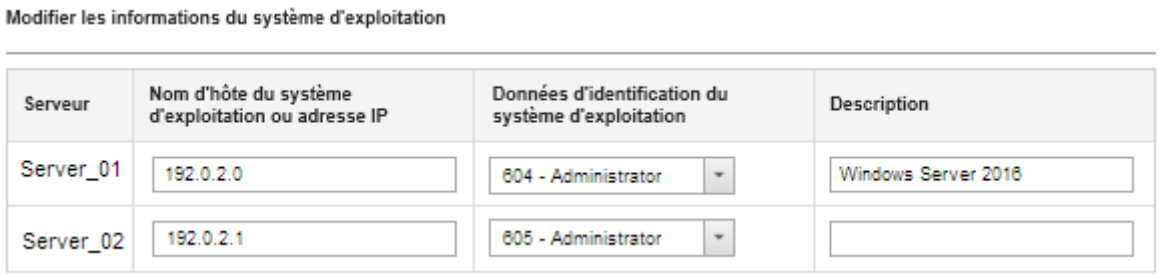
Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Gérer l'accès SE** pour afficher la page Gérer l'accès SE.

Vous pouvez trier les colonnes de la table pour faciliter la recherche des serveurs spécifiques. En outre, vous pouvez sélectionner un type de système dans la liste déroulante **Tous les systèmes** et saisir un texte (par exemple, un nom de système ou une adresse IP) dans la zone **Filtre** pour filtrer davantage l'affichage des serveurs.



Etape 2. Sélectionnez les serveurs à mettre à jour.

Etape 3. Cliquez sur l'icône **Éditer les informations SE**( ) pour afficher la boîte de dialogue Éditer les informations SE.



Etape 4. Pour chaque serveur cible, indiquez les informations suivantes :
- Adresse IP ou nom d'hôte du système d'exploitation hôte
- (Facultatif) Données d'identification stockées pour l'accès au système d'exploitation hôte
- (Facultatif) Description du système d'exploitation hôte

Etape 5. Cliquez sur **Enregistrer**.

Après avoir terminé

Vous pouvez effectuer les actions suivantes pour gérer l'accès au système d'exploitation.

- Effacez les informations relatives au système d'exploitation (adresse IP, données d'identification et description) en sélectionnant le serveur, puis en cliquant sur l'icône **Supprimer les informations SE** ( ).

- Testez l'authentification sur les serveurs Windows en cliquant sur **Distribution → Mises à jour de pilote Windows : Appliquer**, en sélectionnant le serveur cible, puis en cliquant sur **Vérifier l'authentification**.
- Pour afficher des informations sur le déploiement du système d'exploitation sur un serveur spécifique, pointez sur le nom du serveur.

  Remarque : Les informations de déploiement sont disponibles uniquement pour les systèmes d'exploitation qui ont été déployés par l'instance XClarity Administrator. Les informations de déploiement ne sont pas disponibles pour les déploiements défaillants et les déploiements qui ont été effectués par d'autres moyens, notamment une autre instance de XClarity Administrator.

Affichage des clés Features on Demand (FoD)

Vous pouvez afficher la liste des clés Features on Demand (FoD) actuellement installées sur les serveurs gérés.

À propos de cette tâche

Vous ne pouvez pas acheter, installer ou gérer la clé Features on Demand (FoD) à partir de l'interface Web de Lenovo XClarity Administrator. Pour plus d'informations sur l'acquisition et l'installation de clés Features on Demand (FoD), voir Features on Demand (FoD) dans la documentation en ligne de XClarity Administrator.

Procédure

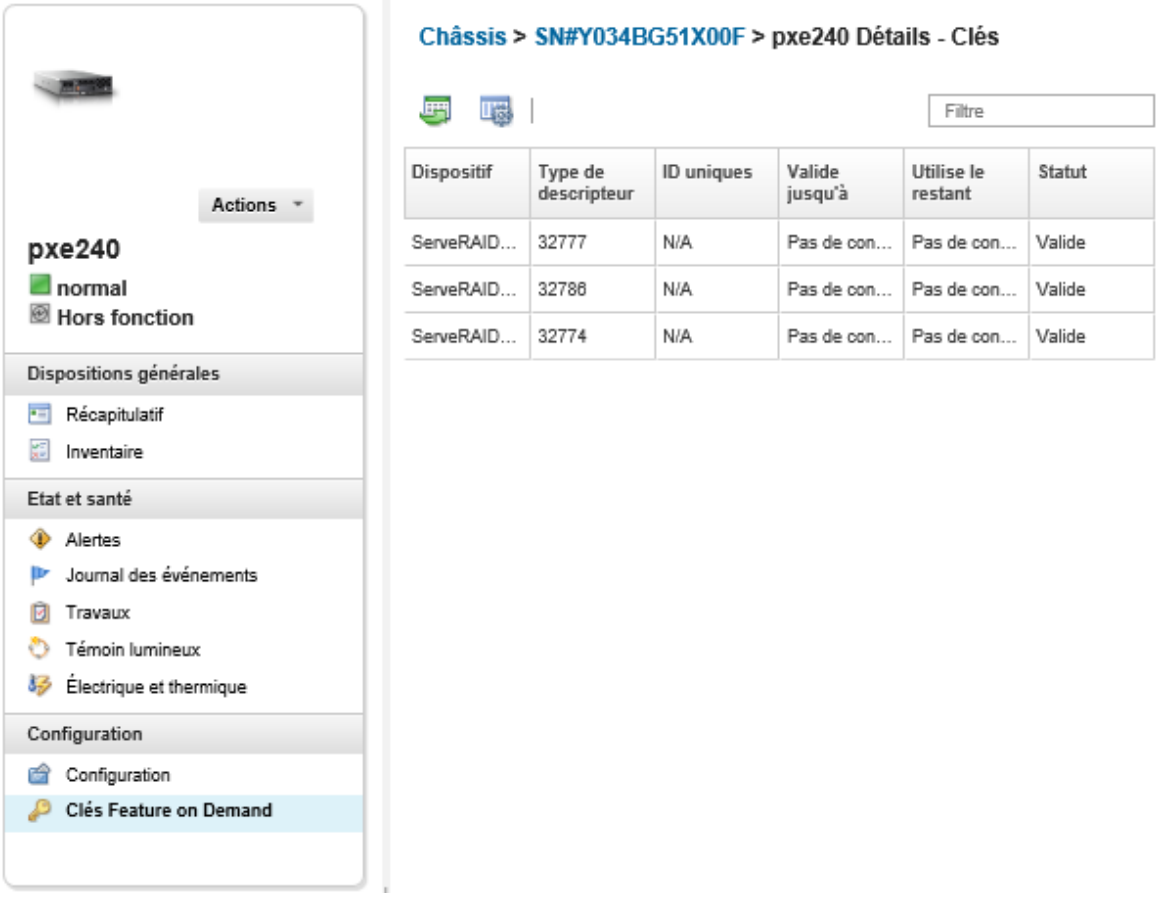
Procédez comme suit pour afficher une liste des clés FoD installées sur un serveur géré spécifique.

Etape 1. Dans le menu XClarity Administrator, cliquez sur **Matériel → Serveurs**. La page Serveurs qui s'affiche présente une vue tabulaire de tous les serveurs gérés (serveurs rack, serveurs au format tour et nœuds de traitement).

Etape 2. Cliquez sur le nom du serveur dans la colonne **Serveur**. La page de récapitulatif de l'état de ce serveur s'affiche et présente les propriétés du serveur ainsi qu'une liste des composants installés sur ce serveur.

Etape 3. Cliquez sur **Détails d'inventaire** sous Général dans le panneau de navigation de gauche et développez chaque section de composant matériel afin d'afficher les ID FoD uniques pour ces composants.

Etape 4. Cliquez sur Clés **Features on Demand (FoD)** sous Configuration dans le panneau de navigation de gauche pour afficher des informations sur toutes les clés FoD installées sur le serveur.



Gestion de l'alimentation et de la température

Vous pouvez surveiller et gérer la consommation d'énergie et la température de serveurs Converged, NeXtScale, System x et ThinkServer, et améliorer l'efficacité énergétique à l'aide de Lenovo XClarity Energy Manager.

En savoir plus : Lenovo XClarity Energy Manager

À propos de cette tâche

XClarity Administrator est une interface utilisateur autonome que vous pouvez utiliser pour surveiller et gérer la consommation d'énergie et la température des serveurs pris en charge, notamment par les opérations suivantes :

- Surveillance de la consommation d'énergie, en estimant la demande en énergie, puis en réaffectant l'énergie aux serveurs en fonction des besoins.
- Surveillance de la température et des capacités de refroidissement des serveurs.
- Envoi de notifications lorsque certains événements se produisent ou lorsque des seuils sont dépassés.
- Utilisation de stratégies pour limiter la quantité d'énergie qu'un appareil consomme.
- Optimisation de l'efficacité énergétique en surveillant les températures d'entrée en temps réel, en identifiant les serveurs peu utilisés en fonction des données sur l'alimentation hors bande, en mesurant des plages de puissances des différents modèles de serveur et en évaluant la façon dont les serveurs s'adaptent aux nouvelles charges de travail en fonction de la disponibilité des ressources.

- En réduisant la consommation électrique à un niveau minimal pour prolonger la durée de service lors d'un événement lié à l'alimentation de secours (tel qu'une coupure d'alimentation du centre de données).

Pour plus d'informations sur le téléchargement, l'installation et l'utilisation de XClarity Administrator, voir le Site Web Lenovo XClarity Energy Manager.

Mise sous tension et hors tension d'un serveur

Vous pouvez mettre sous tension et hors tension un serveur à partir de Lenovo XClarity Administrator.

Avant de commencer

- Pour Red Hat® Enterprise Linux (RHEL) versions 7 et suivantes, le redémarrage du système d'exploitation à partir d'un mode graphique interrompt le serveur par défaut. Avant d'effectuer les actions **Redémarrer normalement** ou **Redémarrer immédiatement** depuis XClarity Administrator, vous devez configurer manuellement le système d'exploitation afin de modifier le comportement du bouton d'alimentation pour la mise hors tension. Pour des instructions détaillées, voir Guide d'administration et de migration des données Red Hat : Modification du comportement lors de l'utilisation du bouton d'alimentation dans le mode cible graphique.
- Pour SUSE Linux Enterprise Server (SLES), la mise hors tension du système d'exploitation requiert la saisie du mot de passe racine dans la session SLES. Pour pouvoir effectuer les actions **Mettre hors tension normalement** ou **Mettre hors tension immédiatement** à partir de XClarity Administrator, vous devez mettre le serveur sous tension manuellement à l'aide de l'interface SLES locale et sélectionner l'option **Remember authorization** lorsque vous entrez le mot de passe, ou vérifier votre stratégie de sécurité pour voir si l'authentification obligatoire peut être désactivée.
- Une fois activée, l'option d'amorçage Wake on LAN peut affecter les opérations XClarity Administrator qui mettent le serveur hors tension, notamment les mises à jour du microprogramme si votre réseau comprend un client Wake on LAN qui émet des commandes « Wake on Magic Packet ».
- L'action d'alimentation **Redémarrer sur la configuration système** redémarre le serveur, puis ouvre l'utilitaire de configuration BIOS/UEFI dans une session de contrôle à distance plutôt que dans un amorçage normal du système d'exploitation.
- Les actions d'alimentation **Mettre hors tension normalement** et **Mettre hors tension immédiatement** dépendent des configurations du système d'exploitation installé sur l'appareil et fonctionnent uniquement si le système d'exploitation est configuré pour les prendre en charge.
- Vous pouvez redémarrer l'appareil avec une interruption non masquable (NMI) en cliquant sur **Toutes les actions → Service → Déclencher NMI**.

Procédure

Pour mettre un serveur sous tension ou hors tension, procédez comme suit.

Etape 1. Dans le menu XClarity Administrator, cliquez sur **Matériel → Serveurs**. La page Serveurs s'affiche avec une vue tabulaire de tous les serveurs gérés (serveurs rack et nœuds de traitement).

Etape 2. Sélectionnez le serveur.

Etape 3. Cliquez sur **Toutes les actions → Actions d'alimentation**, puis sur l'une des actions d'alimentation suivantes :
- **Mettre sous tension** permet de mettre l'appareil sous tension.
- **Mettre hors tension normalement** permet d'arrêter le système d'exploitation et de mettre l'appareil hors tension.
- **Mettre hors tension immédiatement** permet de mettre l'appareil hors tension.
- **Redémarrer normalement** permet d'arrêter le système d'exploitation et de redémarrer l'appareil.
- **Redémarrer immédiatement** permet de redémarrer l'appareil

- **Redémarrer à la configuration du système** permet de redémarrer l'appareil à la configuration BIOS/UEFI (F1). Cette actions est prise en charge pour les serveurs non ThinkServer qui sont pris en charge sans limitations.
- **Redémarrer le contrôleur de gestion** permet de redémarrer BMC.
- **Redémarrer immédiatement et tenter un amorçage réseau PXE** redémarre le serveur immédiatement et lance le serveur sur le réseau PXE (Preboot Execution Environment). Cette option est prise en charge pour les serveurs Lenovo Flex System, System x et ThinkSystem.

  Remarque : Les paramètres UEFI liés à l'amorçage PXE doivent être configurés sur le serveur.

Réinstallation virtuelle d'un serveur dans un châssis Flex System

Vous pouvez simuler le retrait et la réinsertion d'un serveur dans un châssis Flex System en redémarrant le serveur à l'aide d'une interruption non masquable (NMI).

À propos de cette tâche

Au cours de la réinstallation virtuelle, toutes les connexions réseau existantes au serveur sont perdues et l'état d'alimentation du serveur change. Avant d'effectuer une réinstallation virtuelle, vérifiez que vous avez enregistré toutes les données utilisateur.

Attention :

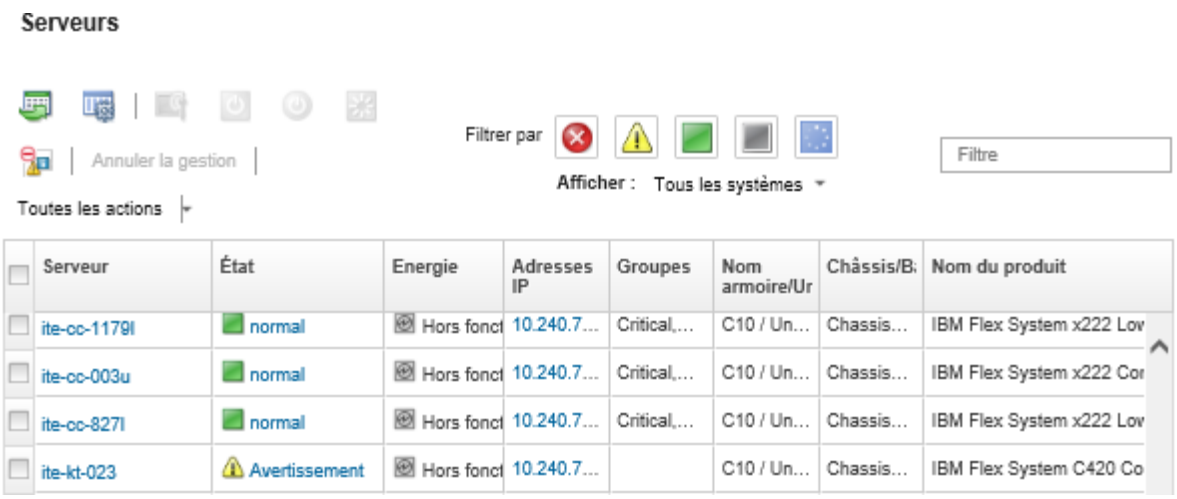
- N'effectuez pas de réinstallation virtuelle si vous n'y êtes pas invité par Lenovo Support.
- Une réinstallation virtuelle peut engendrer la perte de données. Avant de réinstaller le serveur, effectuez les opérations nécessaires pour protéger les données utilisateur.
- Au lieu d'effectuer une réinstallation virtuelle, mettez le serveur hors tension. Pour plus d'informations sur les actions d'alimentation, voir Mise sous tension et hors tension d'un serveur.

Procédure

Pour réinstaller virtuellement un serveur dans un châssis Flex System, procédez comme suit.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Matériel → Serveurs**. La page Serveurs qui s'affiche présente une vue tabulaire de tous les serveurs gérés.

Vous pouvez trier les colonnes du tableau pour trouver plus facilement le serveur que vous souhaitez réinstaller. En outre, vous pouvez sélectionner un type d'appareil dans la liste déroulante **Tous les appareils** et saisir un texte (par exemple, un nom ou une adresse IP) dans la zone **Filtre** pour filtrer davantage l'affichage des serveurs.



Etape 2. Sélectionnez le serveur dans le tableau.

Etape 3. Cliquez sur **Toutes les actions → Service → Réinstallation virtuelle**.

Etape 4. Cliquez sur **Réinstallation virtuelle**.

Lancement de l'interface du contrôleur de gestion pour un serveur

Vous pouvez lancer l'interface Web du contrôleur de gestion pour un serveur spécifique à partir de Lenovo XClarity Administrator.

Avant de commencer

Pour accéder aux serveurs ThinkSystem SR635 SR655 via XClarity Administrator, un utilisateur doit posséder des droits **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin** ou **lxc-os-admin** (voir Gestion du serveur d'authentification).

Lorsque vous utilisez l'authentification unique (SSO), vous pouvez lancer l'interface de gestion des serveurs gérés à partir de XClarity Administrator sans devoir vous connecter. L'authentification unique est prise en charge sur les serveurs ThinkSystem et ThinkAgile (à l'exception des modèles SR635 et SR655). Les serveurs ThinkSystem SR645 et SR665 nécessitent un microprogramme XCC 21A ou une version plus récente.

Pour vous connecter directement au contrôleur de gestion à l'aide de comptes utilisateur LDAP locaux ou externes sans vous connecter à XClarity Administrator, utilisez l'URL `https://{XCC_IP_adderss}/#/login`.

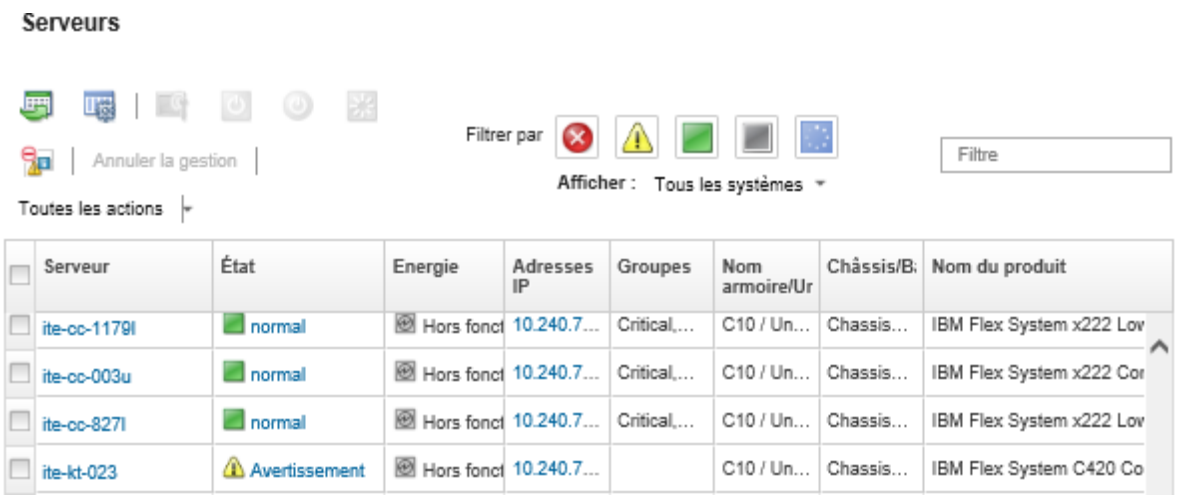
Procédure

Procédez comme suit pour lancer l'interface du contrôleur de gestion pour un serveur.

Remarque : Le lancement d'une interface du contrôleur de gestion à partir de Lenovo XClarity Administrator à l'aide du navigateur Web Safari n'est pas pris en charge.

Etape 1. Dans la barre de menus XClarity Administrator, cliquez sur **Matériel → Serveurs** pour afficher la page Serveurs.

Vous pouvez trier les colonnes du tableau afin de faciliter la recherche de serveurs spécifiques. En outre, vous pouvez sélectionner un type de système dans la liste déroulante **Tous les systèmes** et saisir un texte (par exemple, un nom ou une adresse IP) dans la zone **Filtre** pour filtrer davantage l'affichage des serveurs.



Etape 2. Cliquez sur le lien du serveur dans la colonne **Serveur**. La page de récapitulatif de l'état de ce serveur s'affiche.

Etape 3. Cliquez sur **Toutes les actions → Lancer → Interface Web de gestion**. L'interface Web du contrôleur de gestion du serveur est démarrée.

Conseil : Vous pouvez également cliquer sur l'adresse IP dans la colonne **Adresses IP** pour lancer l'interface du contrôleur de gestion.

Etape 4. Connectez-vous à l'interface du contrôleur de gestion à l'aide de vos données d'identification utilisateur XClarity Administrator.

Après avoir terminé

Pour plus d'informations sur l'utilisation de l'interface du contrôleur de gestion pour un serveur, voir Documentation en ligne d'Integrated Management Module II et Documentation en ligne XClarity Controller.

Modification des propriétés système pour un serveur

Vous pouvez modifier les propriétés système d'un serveur spécifique.

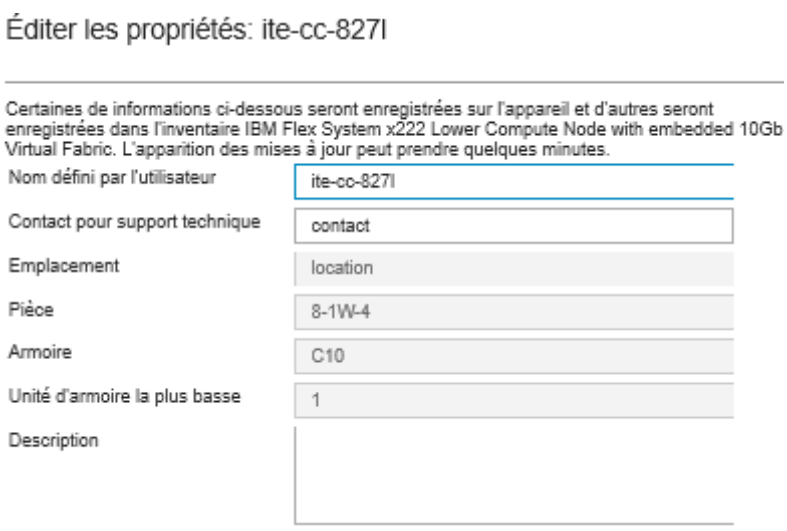
Procédure

Procédez comme suit pour modifier les propriétés système :

Etape 1. Dans la barre de menus Lenovo XClarity Administrator, cliquez sur **Matériel → Serveurs** pour afficher la page Serveurs.

Etape 2. Sélectionnez le serveur à mettre à jour.

Etape 3. Cliquez sur **Toutes les actions → Inventaire → Éditer les propriétés** pour afficher la boîte de dialogue Éditer.



Etape 4. Modifiez les informations suivantes, si nécessaire.
- Nom défini par l'utilisateur pour le serveur
- Contact pour support technique
- Description

Remarque : Les propriétés d'emplacement, de pièce, d'armoire et d'unité d'armoire la plus basse sont mises à jour par XClarity Administrator lorsque vous ajoutez ou retirez des appareils dans une armoire dans l'interface Web (voir Gestion des armoires).

Etape 5. Cliquez sur **Enregistrer**.

Remarque : Si vous modifiez ces propriétés, vous devrez peut-être attendre quelques instants avant que les modifications n'apparaissent dans l'interface Web XClarity Administrator.

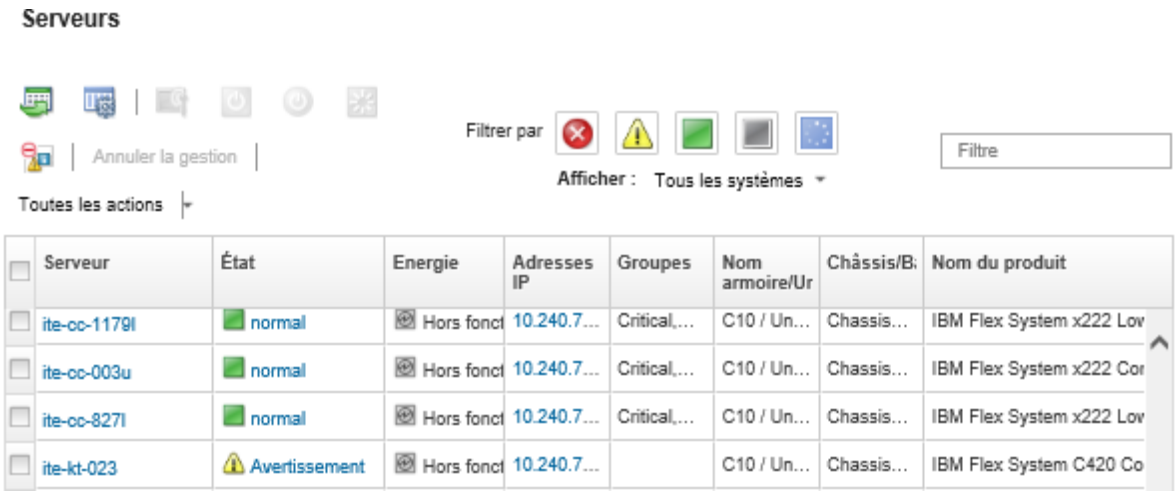
Résolution de données d'identification expirées ou non valides pour un serveur

Lorsqu'une des données d'identification stockées expirent ou deviennent inopérantes sur un appareil, le statut de cet appareil apparaît comme « Hors ligne. »

Procédure

Pour résoudre des données d'identification expirées ou non valides pour un serveur.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Matériel → Serveurs**. La page Serveurs s'affiche avec une vue tabulaire de tous les serveurs gérés (serveurs rack et nœuds de traitement).



Etape 2. Cliquez sur l'en-tête de table **Alimentation** pour grouper tous les serveurs hors ligne en haut de la table.

   En outre, vous pouvez sélectionner un type de système dans la liste déroulante Tous les systèmes et saisir un texte (par exemple, un nom de système ou une adresse IP) dans la zone **Filtre** pour filtrer davantage l'affichage des serveurs.

Etape 3. Sélectionnez le serveur à résoudre.

Etape 4. Cliquez sur **Toutes les actions → Sécurité → Éditer les données d'identification stockées**.

Etape 5. Changez le mot de passe des données d'identification stockées ou sélectionnez d'autres données d'identification stockées à utiliser pour cet appareil géré.

   Remarque : Si vous avez géré plusieurs appareils à l'aide des mêmes données d'identification stockées et si vous modifiez le mot de passe des données d'identification stockées, ce changement de mot de passe affecte tous les dispositifs qui utilisent actuellement les données d'identification stockées.

Récupération d'un serveur défaillant après le déploiement d'un modèle de serveur

Si un serveur est défaillant après le déploiement d'un modèle de serveur, vous pouvez récupérer le serveur en désaffectant le profil du serveur défaillant, puis en réaffectant ce profil à un serveur de secours.

Procédure

Pour récupérer le serveur défaillant qui utilise l'authentification gérée Lenovo XClarity Administrator, procédez comme suit.

Etape 1. Identifiez le serveur défaillant.

Etape 2. Désaffectez le profil de serveur du serveur défaillant (voir Désactivation d'un profil de serveur).

   Attention : Le serveur défaillant doit être mis hors tension pour désactiver les adresses virtuelles affectées *avant* de réaffecter le profil. Lorsque vous désaffectez le profil de serveur, sélectionnez **Mettre le serveur hors tension** dans la boîte de dialogue Désaffecter le profil de serveur pour mettre hors tension le serveur défaillant (voir Mise sous tension et hors tension d'un serveur).

Etape 3. Affectez le profil de serveur à un serveur de secours (voir Activation d'un profil de serveur).

Etape 4. Activez le profil en mettant le serveur de secours sous tension s'il est actuellement hors tension ou en redémarrant le serveur de secours s'il est actuellement sous tension (voir Mise sous tension et hors tension d'un serveur).

Etape 5. Migrez les paramètres VLAN des commutateurs connectés vers le serveur de secours.

Etape 6. Vérifiez que le serveur défaillant est hors tension.

Etape 7. Remplacez ou réparez le serveur défaillant. Si vous réparez le serveur, procédez comme suit pour vérifier que les paramètres par défaut sont réinitialisés pour le serveur récemment réparé :

a. Réinitialisez les valeurs par défaut du module BMC à l'aide de l'interface Web de gestion du serveur. Pour plus d'informations sur la réinitialisation du module BMC, voir Récupération de la gestion d'un serveur M5 ou M6 ThinkSystem, Converged, NeXtScale ou System x après une défaillance du serveur de gestion en réinitialisant le contrôleur de gestion.

b. Effacez les informations UEFI (Unified Extensible Firmware Interface), notamment toutes les adresses virtuelles de carte d'E-S à l'aide des menus UEFI. Pour plus d'informations, voir la documentation de l'interface UEFI.

Récupération de paramètres d'amorçage après le déploiement d'un modèle de serveur

Si un ou plusieurs serveurs ne démarrent pas après le déploiement d'un nouveau modèle de serveur sur ces serveurs, il se peut que les paramètres d'amorçage aient été remplacés par les paramètres d'amorçage par défaut spécifiés dans le modèle de serveur. Pour les systèmes d'exploitation installés en mode UEFI, la restauration des paramètres par défaut peut nécessiter des étapes de configuration supplémentaires pour restaurer la configuration d'amorçage.

Procédure

Exécutez la procédure de récupération manuelle suivante pour chaque serveur affecté pour restaurer les paramètres d'amorçage d'origine.

- Pour un serveur sur lequel Red Hat Enterprise Linux est installé :
  1. Si vous accédez à distance au serveur, établissez une session de contrôle à distance sur le serveur (voir Utilisation du contrôle à distance pour gérer des serveurs Converged, Flex System, NeXtScale et System x).
  2. Redémarrez le serveur en cliquant sur **Outils → Alimentation → Activé**. Lorsque l'écran d'accueil de l'interface UEFI pour le serveur s'affiche dans la session de contrôle à distance, appuyez sur F1 pour afficher l'utilitaire Setup Utility.
  3. Sélectionnez **Boot Manager**.
  4. Sélectionnez **Add Boot Option**.
  5. Sélectionnez **UEFI Full Path Option**.
  6. Dans la liste qui s'affiche, sélectionnez l'entrée qui comporte `SAS`.
  7. Sélectionnez **EFI**.
  8. Sélectionnez **redhat**.
  9. Sélectionnez **grub.efi**.
  10. Sélectionnez la zone **Input the Description**.
  11. Tapez `Red Hat Enterprise Linux`.
  12. Sélectionnez **Commit Changes**.
  13. Placez l'option `Red Hat Enterprise Linux` en premier dans l'ordre d'amorçage, puis retirez toutes les autres options de la liste Boot Order.
  14. Appuyez sur la touche d'échappement, puis sélectionnez **Save changes then exit this menu**.
  15. Appuyez sur la touche d'échappement, puis sélectionnez **Exit the Configuration Utility and Reboot**. Le nœud de traitement redémarre.

- Pour un serveur sur lequel Microsoft Windows Server 2008 est installé :
  1. Mettez le serveur sous tension, puis, lorsque vous y êtes invité, appuyez sur F1 pour entrer dans la configuration.
  2. Sélectionnez **Boot Manager**.
  3. Sélectionnez **Boot from File**.
  4. Sélectionnez la partition système GPT (GUID Partition Table) sur laquelle vous avez installé Microsoft Windows Server 2008.
  5. Sélectionnez **EFI**.
  6. Sélectionnez **Microsoft**.
  7. Sélectionnez **Boot**.
  8. Sélectionnez **bootmgfw.EFI**.

Remarque : Pour plus d'informations, voir Astuce RETAIN 5079636.

Récupération de la gestion du serveur au format tour après une défaillance du serveur de gestion

Si un serveur rack ou au format tour est géré par Lenovo XClarity Administrator, et qu'une défaillance se produit sur XClarity Administrator, vous pouvez restaurer les fonctions de gestion en attendant que XClarity Administrator soit restauré ou remplacé.

À propos de cette tâche

Pour récupérer la gestion d'un serveur Flex System, voir Reprise de la gestion avec un module CMM après une défaillance du serveur de gestion.

Récupération de la gestion d'un serveur rack ou au format tour après une défaillance du serveur de gestion par gestion forcée

Vous pouvez récupérer la gestion d'un serveur en gérant à nouveau le serveur à l'aide de l'option de gestion forcée.

Procédure

Si l'instance de remplacement de Lenovo XClarity Administrator utilise la même adresse IP que l'instance de XClarity Administrator défectueuse, vous pouvez gérer à nouveau l'appareil à l'aide du compte et du mot de passe `RECOVERY_ID`, ainsi que de l'option**Forcer la gestion** (voir Gestion des serveurs).

Récupération d'un serveur M4 System x ou NeXtScale dont la gestion n'a pas été correctement annulée en utilisant le contrôleur de gestion

Vous pouvez récupérer la gestion d'un serveur M4 System x ou NeXtScale en utilisant le contrôleur de gestion de la carte mère.

Procédure

Procédez comme suit pour récupérer la gestion d'un serveur qui utilise l'authentification gérée Lenovo XClarity Administrator.

Etape 1. Connectez-vous à l'interface Web du contrôleur de gestion à l'aide du compte utilisateur et du mot de passe que vous avez créés avant que le serveur ne soit géré par XClarity Administrator.

Etape 2. Effacez les paramètres d'alerte SNMP.

a. Cliquez sur **Gestion IMM → Réseau**.

b. Cliquez sur l'onglet **SNMP**.

c. Cliquez sur l'onglet **Communities**.

d. Localisez l'entrée de communauté de l'instance de XClarity Administrator précédente, par exemple.
   - **LXCA IP address:** 10.240.198.84
   - **LXCA host:** LXCA_maqCBlt86d
   - **Community 2:**
   - **Community name:** LXCA_maqCBlt86d
   - **Type d'accès :** Alerte
   - **Autoriser des hôtes spécifiques pour la réception d'alertes sur cette communauté :** 10.240.198.84

e. Retirez la valeur des zones pour l'entrée de communauté.

f. Cliquez sur **Appliquer**.

Etape 3. Effacez les comptes utilisateur.

a. Cliquez sur **Gestion IMM → Utilisateurs**.

b. Cliquez sur l'onglet **Comptes utilisateur**.

c. Supprimez tous les comptes utilisateur qui sont des comptes XClarity Administrator, y compris les comptes utilisateur ayant les préfixes suivants :
   - DISABLE_*
   - LXCA_*
   - OBSOLETE_*
   - SNMPCFGUSER

Après avoir terminé

Une fois XClarity Administrator restauré ou remplacé, vous pouvez à nouveau gérer le serveur System x ou NeXtScale (voir Gestion des serveurs). Toutes les informations relatives au serveur (telles que les paramètres réseau, les stratégies de serveur et les stratégies de conformité du microprogramme) sont conservées.

Récupération de la gestion d'un serveur M5 ou M6 ThinkSystem, Converged, NeXtScale ou System x après une défaillance du serveur de gestion en réinitialisant le contrôleur de gestion

Vous pouvez récupérer la gestion d'un serveur M5 ou M6 ThinkSystem, Converged, NeXtScale ou System x en réinitialisant les valeurs par défaut du contrôleur de gestion de la carte mère du serveur.

Procédure

Pour récupérer la gestion d'un serveur qui utilise l'authentification gérée Lenovo XClarity Administrator, procédez comme suit.

Etape 1. Si la fonction Encapsulation est activée sur l'appareil, connectez-vous au contrôleur de gestion cible à partir d'un système configuré pour utiliser l'adresse IP du dispositif virtuel XClarity Administrator défaillant.

Etape 2. Réinitialisez les valeurs par défaut du contrôleur de gestion.

a. Connectez-vous à l'interface Web du contrôleur de gestion du serveur à l'aide du compte utilisateur et du mot de passe de récupération que vous avez créés avant que le serveur ne soit géré par XClarity Administrator.

b. Cliquez sur l'onglet **Gestion IMM**.

c. Cliquez sur **Réinitialisation du module IMM aux valeurs par défaut**.

d. Cliquez sur **OK** pour confirmer l'action de réinitialisation.

Important : Une fois sa configuration terminée, le module BMC est redémarré. S'il s'agit d'un serveur local, votre connexion TCP/IP est interrompue et vous devez reconfigurer l'interface réseau pour restaurer la connectivité.

Etape 3. Connectez-vous à nouveau à l'interface Web du contrôleur de gestion du serveur.

- Le module BMC est configuré initialement pour tenter d'obtenir une adresse IP à partir d'un serveur DHCP. S'il n'y parvient pas, il utilise l'adresse IPv4 statique `192.168.70.125`.
- La valeur IMMBMC est définie initialement avec le nom d'utilisateur `USERID` et le mot de passe `PASSWORD` (avec un zéro). Ce compte utilisateur par défaut dispose d'un accès Superviseur. Pour une sécurité accrue, modifiez ce nom d'utilisateur et ce mot de passe lors de votre configuration initiale.

Etape 4. Reconfigurez l'interface réseau pour restaurer la connectivité. Pour plus d'informations, voir le document Documentation en ligne d'Integrated Management Module II.

Après avoir terminé

Une fois XClarity Administrator restauré ou remplacé, vous pouvez à nouveau gérer le serveur (voir Gestion des serveurs). Toutes les informations relatives au serveur (telles que les paramètres réseau, les stratégies de serveur et les stratégies de conformité du microprogramme) sont conservées.

Si le serveur a été configuré à l'aide de Modèles de configuration, vous pouvez désactiver puis réactiver le profil de serveur qui a été affecté au serveur pour appliquer la configuration (voir Utilisation de profils de serveur).

Récupération de la gestion d'un serveur M5 ou M6 ThinkSystem, Converged, NeXtScale ou System x après une défaillance du serveur de gestion en utilisant la commande cimcli

Vous pouvez récupérer la gestion d'un serveur M5 ou M6 ThinkSystem, Converged, NeXtScale ou System x à l'aide de l'utilitaire `cimcli` pour effacer les souscriptions CIM.

Avant de commencer

OpenPegasus avec l'utilitaire cimcli doit être installé sur un système qui dispose d'un accès réseau au serveur cible. Pour plus d'informations sur le téléchargement, la configuration et la compilation d'OpenPegasus, voir le Site Web RPM d'édition OpenPegasus pour Linux.

Remarque : Pour Red Hat Enterprise Linux (RHEL) Server 7 et versions ultérieures, les fichiers RPM sources et binaires d'OpenPegasus sont inclus dans la distribution de Red Hat. Le package `top-pegasus-test.x86_64` inclut l'utilitaire cimcli.

À propos de cette tâche

Une fois la récupération du serveur effectuée, vous pouvez gérer à nouveau le serveur. Toutes les informations relatives au serveur (telles que les paramètres réseau, les stratégies de serveur et les stratégies de conformité du microprogramme) sont conservées.

Procédure

Effectuez les opérations suivantes à partir d'un serveur qui utilise l'authentification gérée Lenovo XClarity Administrator et sur lequel OpenPegasus est installé pour récupérer la gestion d'un serveur.

Etape 1. Si Encapsulation est activé sur l'appareil :

a. Connectez-vous au serveur cible à partir d'un système qui est configuré pour utiliser l'adresse IP du dispositif virtuel XClarity Administrator défectueux.

b. Désactivez Encapsulation en ouvrant une session SSH sur l'appareil et en exécutant la commande suivante :
```
encaps lite off
```

Etape 2. Exécutez les commandes suivantes pour déterminer les instances CIM pour CIM_ListenerDestinationCIMXML, CIM_Indicationfilter et CIM_IndicationSubscription.
```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_ListenerDestinationCIMXML
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_Indicationfilter
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_IndicationSubscription
```

où <*IP_address*>, <*user_ID*> et <*password*> sont l'adresse IP, l'ID utilisateur et le mot de passe du contrôleur de gestion. Par exemple :

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
-s ni CIM_ListenerDestinationCIMXML
CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop s ni CIM_Indicationfilter
CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
s ni CIM_IndicationSubscription
CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""
```

Etape 3. Exécutez la commande suivante pour supprimer l'instance CIM pour CIM_ListenerDestinationCIMXML, CIM_Indicationfilter et CIM_IndicationSubscription, individuellement.
```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s di '<cim_instance>'
```

où <*IP_address*>, <*user_ID*> et <*password*> sont l'adresse IP, l'ID utilisateur et le mot de passe du contrôleur de gestion, et <*cim_instance*> représente les informations retournées pour chaque instance CIM à l'étape précédente, placées entre des guillemets simples. Par exemple :

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
```

```
'CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""'
```

Après avoir terminé

Une fois Lenovo XClarity Administrator restauré ou remplacé, vous pouvez à nouveau gérer le serveur System x ou NeXtScale (voir Gestion des serveurs). Toutes les informations relatives au serveur (telles que les paramètres réseau, les stratégies de serveur et les stratégies de conformité du microprogramme) sont conservées.

Récupération de la gestion d'un serveur ThinkServer après une défaillance du serveur de gestion en utilisant l'interface du contrôleur de gestion

Vous pouvez récupérer la gestion d'un serveur ThinkServer à partir de l'interface du contrôleur de gestion.

Procédure

Pour récupérer la gestion d'un serveur, procédez comme suit.

Etape 1. Connectez-vous en tant qu'administrateur à l'interface Web du contrôleur de gestion du serveur (voir Lancement de l'interface du contrôleur de gestion pour un serveur).

Etape 2. Retirez les comptes IPMI créés par Lenovo XClarity Administrator en sélectionnant Utilisateurs dans le menu principal, puis en supprimant tous les comptes utilisateur ayant le préfixe « LXCA_ ».

Vous pouvez également modifier le nom de l'utilisateur du compte, puis retirer le préfixe « LXCA_ ».

Etape 3. Retirez les destinations d'alerte SNMP en sélectionnant **Gestion PEF** dans le menu principal, cliquez sur l'onglet **Destination LAN**, puis supprimez l'entrée qui pointe sur l'adresse IP de l'instance de XClarity Administrator.

Etape 4. Vérifiez que vos paramètres NTP sont valides en sélectionnant **Paramètres NTP** dans le menu principal, puis en configurant manuellement la date et l'heure ou en fournissant une adresse de serveur NTP valide.

Annulation de la gestion d'un serveur rack ou au format tour

Vous pouvez retirer un serveur rack ou au format tour de la gestion par Lenovo XClarity Administrator. Ce processus est appelé *annulation de la gestion.*

Avant de commencer

Vous pouvez activer XClarity Administrator pour annuler automatiquement la gestion des appareils qui sont hors ligne pendant une durée spécifique. Cette option est désactivée par défaut. Pour activer l'annulation de la gestion automatique des appareils hors ligne, cliquez sur **Matériel → Reconnaître et gérer de nouveaux appareils** dans le menu XClarity Administrator, puis cliquez sur **Éditer** en regard de **Annuler la gestion des appareils hors ligne correspond à : Désactivé**. Ensuite, sélectionnez **Activer l'option Annuler la gestion des appareils hors ligne** et définissez l'intervalle de temps. Par défaut, la gestion des appareils est annulée lorsque ceux-ci sont hors ligne pendant 24 heures.

Avant d'annuler la gestion d'un serveur rack ou au format tour, vérifiez qu'aucun travail actif n'est en cours d'exécution sur le serveur.

Si vous voulez retirer le modèle de serveur et toutes les adresses virtuelles sur le serveur rack ou au format tour, désactivez le profil de serveur avant d'annuler la gestion du serveur (voir Désactivation d'un profil de serveur).

Lorsque l'Appel vers Lenovo est activé dans XClarity Administrator, l'Appel vers Lenovo est désactivé sur tous les châssis et serveurs gérés afin d'éviter de générer des enregistrements de problème en double. Si vous prévoyez de cesser d'utiliser XClarity Administrator pour gérer vos appareils, vous pouvez réactiver l'Appel vers Lenovo sur tous les appareils gérés à partir de XClarity Administrator au lieu de réactiver ultérieurement l'Appel vers Lenovo pour chaque appareil géré individuel (voir Réactivation de l'appel vers Lenovo sur tous les appareils gérés dans la documentation en ligne de XClarity Administrator).

À propos de cette tâche

Lorsque vous annulez la gestion d'un serveur rack ou au format tour, Lenovo XClarity Administrator exécute les actions suivantes :

- Efface la configuration utilisée pour la gestion centralisée des utilisateurs.
- Retire le certificat de sécurité du contrôleur de gestion de la carte mère à partir du fichier de clés certifiées XClarity Administrator.
- Si Encapsulation est activé sur le dispositif, il configure les règles de pare-feu des dispositifs sur les paramètres avant la gestion du dispositif.
- Supprime les souscriptions CIM à la configuration XClarity Administrator afin que XClarity Administrator ne reçoive plus d'événements du serveur rack ou au format tour.
- Désactive Appel vers Lenovo sur le serveur rack ou au format tour si l'Appel vers Lenovo est actuellement activé sur XClarity Administrator.
- Ignore les événements qui ont été envoyés à partir du serveur rack ou au format tour. Vous pouvez conserver ces événements en transmettant les événements dans un référentiel externe, tel qu'un syslog (voir Acheminement des événements).

Lorsque vous annulez la gestion d'un serveur rack ou au format tour, XClarity Administrator conserve certaines informations relatives au serveur. Ces informations sont réappliquées lorsque vous gérez à nouveau le même serveur rack ou au format tour.

Important : Si vous avez annulé la gestion d'un serveur ThinkServer, puis que vous gérez ce serveur à l'aide d'une autre instance de XClarity Administrator, les informations relatives au serveur sont perdues.

Astuce : Tous les appareils de démonstration qui sont éventuellement ajoutés lors de la configuration initiale sont des nœuds dans un châssis. Pour annuler la gestion des appareils de démonstration, annulez la gestion du châssis à l'aide de l'option **Forcer l'annulation de la gestion, même si l'appareil est inaccessible**.

Procédure

Pour annuler la gestion d'un serveur rack ou au format tour, procédez comme suit.

Etape 1. Dans la barre de menus XClarity Administrator, cliquez sur **Matériel → Serveurs** pour afficher la page Serveurs.

Etape 2. Sélectionnez un ou plusieurs serveurs rack ou au format tour dont la gestion doit être annulée.

Etape 3. Cliquez sur **Annuler la gestion**. Le dialogue Annuler la gestion s'affiche.

Etape 4. **Facultatif :** sélectionnez **Forcer l'annulation de la gestion, même si l'appareil est inaccessible**.

Important : Lors de l'annulation de la gestion du matériel de démonstration, veillez à sélectionner cette option.

Etape 5. Cliquez sur **Annuler la gestion**.La boîte de dialogue Annuler la gestion affiche la progression de chaque étape dans le processus d'annulation de gestion.

Etape 6. Une fois le processus d'annulation de gestion terminé, cliquez sur **OK**.

Récupération d'un serveur rack ou au format tour dont la gestion n'a pas été correctement annulée

Si la gestion d'un serveur Converged, NeXtScale, System x ou ThinkServer n'a pas été correctement annulée, vous devez récupérer le serveur pour pouvoir à nouveau le gérer.

Récupération d'un serveur rack ou au format tour dont la gestion n'a pas été correctement annulée par la gestion forcée

Vous pouvez récupérer la gestion d'un serveur en gérant à nouveau le serveur à l'aide de l'option de gestion forcée.

Procédure

Si l'instance de remplacement de Lenovo XClarity Administrator utilise la même adresse IP que l'instance de XClarity Administrator défectueuse, vous pouvez gérer à nouveau l'appareil à l'aide du compte et du mot de passe `RECOVERY_ID`, ainsi que de l'option**Forcer la gestion** (voir Gestion des serveurs).

Récupération d'un serveur M4 System x ou NeXtScale dont la gestion n'a pas été correctement annulée en utilisant le contrôleur de gestion

Vous pouvez récupérer la gestion d'un serveur M4 System x ou NeXtScale à l'aide du contrôleur de gestion.

Procédure

Pour récupérer la gestion d'un serveur, procédez comme suit.

Etape 1. Connectez-vous à l'interface Web du contrôleur de gestion à l'aide du compte utilisateur et du mot de passe que vous avez créés avant que le serveur ne soit géré par XClarity Administrator.

Etape 2. Effacez les paramètres d'alerte SNMP.

a. Cliquez sur **Gestion IMM → Réseau**.

b. Cliquez sur l'onglet **SNMP**.

c. Cliquez sur l'onglet **Communities**.

d. Localisez l'entrée de communauté de l'instance de XClarity Administrator précédente, par exemple.
- **LXCA IP address:** 10.240.198.84
- **LXCA host:** LXCA_maqCBlt86d
- **Community 2:**
- **Community name:** LXCA_maqCBlt86d
- **Type d'accès :** Alerte
- **Autoriser des hôtes spécifiques pour la réception d'alertes sur cette communauté :** 10.240.198.84

e. Retirez la valeur des zones pour l'entrée de communauté.

f. Cliquez sur **Appliquer**.

Etape 3. Effacez les comptes utilisateur.

a. Cliquez sur **Gestion IMM → Utilisateurs**.

b. Cliquez sur l'onglet **Comptes utilisateur**.

c. Supprimez tous les comptes utilisateur qui sont des comptes XClarity Administrator, y compris les comptes utilisateur ayant les préfixes suivants :
- DISABLE_*
- LXCA_*
- OBSOLETE_*
- SNMPCFGUSER

Etape 4. Gérez le serveur à l'aide de Lenovo XClarity Administrator.

a. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Reconnaître et gérer de nouveaux appareils**. La page Reconnaître et gérer s'affiche.

b. Sélectionnez **Saisie manuelle**.

c. Cliquez sur **Système unique**, entrez l'adresse IP du serveur à gérer, puis cliquez sur **OK**.

d. Spécifiez l'ID utilisateur et le mot de passe pour l'authentification sur le serveur.

e. Cliquez sur **Gérer**.

Une boîte de dialogue s'affiche et présente la progression de ce processus de gestion. Surveillez la progression pour vérifier si le processus aboutit.

f. Une fois le processus terminé, cliquez sur **OK**.

Récupération d'un serveur M5 ou M6 ThinkSystem, Converged, NeXtScale ou System x dont la gestion n'a pas été correctement annulée en réinitialisant les valeurs par défaut du contrôleur de gestion

Vous pouvez récupérer la gestion d'un serveur M5 ou M6 ThinkSystem, Converged, NeXtScale ou System x en réinitialisant les valeurs par défaut du contrôleur de gestion de la carte mère (BMC) du serveur.

Procédure

Pour récupérer la gestion d'un serveur, procédez comme suit.

Etape 1. Si la fonction Encapsulation est activée sur l'appareil, connectez-vous au contrôleur de gestion cible à partir d'un système configuré pour utiliser l'adresse IP du dispositif virtuel XClarity Administrator défaillant.

Etape 2. Réinitialisez les valeurs par défaut du contrôleur de gestion.

a. Connectez-vous à l'interface Web du contrôleur de gestion du serveur à l'aide du compte utilisateur et du mot de passe de récupération que vous avez créés avant que le serveur ne soit géré par XClarity Administrator.

b. Cliquez sur l'onglet **Gestion IMM**.

c. Cliquez sur **Réinitialisation du module IMM aux valeurs par défaut**.

d. Cliquez sur **OK** pour confirmer l'action de réinitialisation.

Important : Une fois sa configuration terminée, le module BMC est redémarré. S'il s'agit d'un serveur local, votre connexion TCP/IP est interrompue et vous devez reconfigurer l'interface réseau pour restaurer la connectivité.

Etape 3. Connectez-vous à nouveau à l'interface Web du contrôleur de gestion du serveur.

- Le module BMC est configuré initialement pour tenter d'obtenir une adresse IP à partir d'un serveur DHCP. S'il n'y parvient pas, il utilise l'adresse IPv4 statique `192.168.70.125`.
- La valeur IMMBMC est définie initialement avec le nom d'utilisateur `USERID` et le mot de passe `PASSWORD` (avec un zéro). Ce compte utilisateur par défaut dispose d'un accès Superviseur. Pour une sécurité accrue, modifiez ce nom d'utilisateur et ce mot de passe lors de votre configuration initiale.

Etape 4. Reconfigurez l'interface réseau pour restaurer la connectivité. Pour plus d'informations, voir le document Documentation en ligne d'Integrated Management Module II.

Etape 5. Gérez le serveur à l'aide de Lenovo XClarity Administrator.

a. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Reconnaître et gérer de nouveaux appareils**. La page Reconnaître et gérer s'affiche.

b. Sélectionnez **Saisie manuelle**.

c. Cliquez sur **Système unique**, entrez l'adresse IP du serveur à gérer, puis cliquez sur **OK**.

d. Spécifiez l'ID utilisateur et le mot de passe pour l'authentification sur le serveur.

e. Cliquez sur **Gérer**.

Une boîte de dialogue s'affiche et présente la progression de ce processus de gestion. Surveillez la progression pour vérifier si le processus aboutit.

f. Une fois le processus terminé, cliquez sur **OK**.

Etape 6. Si le serveur a été configuré à l'aide de Modèles de configuration, réactivez le profil de serveur qui a été affecté au serveur.

a. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Profils de serveur**. La page Modèles de configuration : Profils de serveur s'affiche.

b. Sélectionnez le profil de serveur, puis cliquez sur l'icône **Désactiver un profil de serveur** ( ).

c. Cliquez sur **Mettre ITE hors tension** pour mettre le serveur hors tension. Lorsque le serveur est remis sous tension, les affectations d'adresses virtuelles reviennent aux valeurs par défaut gravées.

d. Cliquez sur **Désactiver**. L'état du profil devient « Inactif » dans la colonne État du profil. Remarque : Les serveurs conservent leurs informations d'identification (par exemple, le nom d'hôte, l'adresse IP, l'adresse MAC virtuelle) lorsqu'un profil est désactivé.

e. Sélectionnez à nouveau le profil de serveur, puis cliquez sur l'icône **Activer le profil de serveur** ( ).

f. Cliquez sur **Activer** pour activer les profils de serveur sur le serveur. L'état du profil devient « Actif » dans la colonne État du profil.

Etape 7. Si une stratégie de conformité était affectée au serveur, réaffectez-la.

a. Dans la barre de menus XClarity Administrator, cliquez sur **Distribution → Appliquer/Activer**. La page Mises à jour de microprogramme : Appliquer/Activer s'affiche avec la liste des appareils gérés.

b. Sélectionnez la stratégie appropriée pour le serveur dans le menu déroulant dans la colonne **Stratégie affectée**.

Récupération d'un serveur M5 ou M6 ThinkSystem, Converged, NeXtScale ou System x dont la gestion n'a pas été correctement annulée en utilisant la commande cimcli

Vous pouvez récupérer la gestion d'un serveur ThinkSystem, Converged, NeXtScale ou System x à l'aide de la commande `cimcli` pour effacer les souscriptions CIM.

Avant de commencer

OpenPegasus avec l'utilitaire cimcli doit être installé sur un système qui dispose d'un accès réseau au serveur cible. Pour plus d'informations sur le téléchargement, la configuration et la compilation d'OpenPegasus, voir le Site Web RPM d'édition OpenPegasus pour Linux.

Remarque : Pour Red Hat Enterprise Linux (RHEL) Server 7 et versions ultérieures, les fichiers RPM sources et binaires d'OpenPegasus sont inclus dans la distribution de Red Hat. Le package `top-pegasus-test.x86_64` inclut l'utilitaire cimcli.

À propos de cette tâche

Une fois la récupération du serveur effectuée, vous pouvez gérer à nouveau le serveur. Toutes les informations relatives au serveur (telles que les paramètres réseau, les stratégies de serveur et les stratégies de conformité du microprogramme) sont conservées.

Procédure

Effectuez les opérations suivantes à partir d'un serveur qui utilise l'authentification gérée Lenovo XClarity Administrator et sur lequel OpenPegasus est installé pour récupérer la gestion d'un serveur.

Etape 1. Si Encapsulation est activé sur l'appareil :

a. Connectez-vous au serveur cible à partir d'un système qui est configuré pour utiliser l'adresse IP du dispositif virtuel XClarity Administrator défectueux.

b. Désactivez Encapsulation en ouvrant une session SSH sur l'appareil et en exécutant la commande suivante :
```
encaps lite off
```

Etape 2. Exécutez les commandes suivantes pour déterminer les instances CIM pour CIM_ListenerDestinationCIMXML, CIM_Indicationfilter et CIM_IndicationSubscription.
```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_ListenerDestinationCIMXML
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_Indicationfilter
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s ni CIM_IndicationSubscription
```

où <*IP_address*>, <*user_ID*> et <*password*> sont l'adresse IP, l'ID utilisateur et le mot de passe du contrôleur de gestion. Par exemple :

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
-s ni CIM_ListenerDestinationCIMXML
CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop s ni CIM_Indicationfilter
CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop
s ni CIM_IndicationSubscription
CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
```

```
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""
```

Etape 3. Exécutez la commande suivante pour supprimer l'instance CIM pour CIM_ ListenerDestinationCIMXML, CIM_Indicationfilter et CIM_IndicationSubscription, individuellement.

```
cimcli -l <IP_address> -u <user_ID> -p <password> -n /root/interop
       -s di '<cim_instance>'
```

où <*IP_address*>, <*user_ID*> et <*password*> sont l'adresse IP, l'ID utilisateur et le mot de passe du contrôleur de gestion, et <*cim_instance*> représente les informations retournées pour chaque instance CIM à l'étape précédente, placées entre des guillemets simples. Par exemple :

```
$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_ListenerDestinationCIMXML.creationclassname="CIM_ListenerDestinationCIMXML",
name="Lenovo:LXCA_10.243.5.191:Handler",systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_Indicationfilter.creationclassname="CIM_IndicationFilter",
name="Lenovo:LXCA_10.243.5.191:Filter",
systemcreationclassname="CIM_ComputerSystem",
systemname="FC3058CADF8B11D48C9B9B1B1B1B1B57"'

$ cimcli -l 10.243.6.68 -u ADMIN -p PASSWORD -n /root/interop di
'CIM_IndicationSubscription.filter="root/interop:cim_indicationfilter.creationclassname=
\"CIM_IndicationFilter\",name=\"Lenovo:LXCA_10.243.5.191:Filter\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\"",
handler="root/interop:cim_listenerdestinationcimxml.creationclassname=
\"CIM_ListenerDestinationCIMXML\",name=\"Lenovo:LXCA_10.243.5.191:Handler\",
systemcreationclassname=\"CIM_ComputerSystem\",
systemname=\"FC3058CADF8B11D48C9B9B1B1B1B1B57\""'
```

Etape 4. Gérez le serveur à l'aide de Lenovo XClarity Administrator.

a. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Reconnaître et gérer de nouveaux appareils**. La page Reconnaître et gérer s'affiche.

b. Sélectionnez **Saisie manuelle**.

c. Cliquez sur **Système unique**, entrez l'adresse IP du serveur à gérer, puis cliquez sur **OK**.

d. Spécifiez l'ID utilisateur et le mot de passe pour l'authentification sur le serveur.

e. Cliquez sur **Gérer**.

   Une boîte de dialogue s'affiche et présente la progression de ce processus de gestion. Surveillez la progression pour vérifier si le processus aboutit.

f. Une fois le processus terminé, cliquez sur **OK**.

Récupération de la gestion d'un serveur ThinkServer dont la gestion n'a pas été correctement annulée en utilisant l'interface du contrôleur de gestion

Vous pouvez récupérer la gestion d'un serveur ThinkServer en utilisant l'interface Web du contrôleur de gestion.

Procédure

Pour récupérer la gestion d'un serveur, procédez comme suit.

Etape 1. Connectez-vous en tant qu'administrateur à l'interface Web du contrôleur de gestion du serveur (voir Lancement de l'interface du contrôleur de gestion pour un serveur).

Etape 2. Retirez les comptes IPMI créés par Lenovo XClarity Administrator en sélectionnant Utilisateurs dans le menu principal, puis en supprimant tous les comptes utilisateur ayant le préfixe « LXCA_ ».

Vous pouvez également modifier le nom de l'utilisateur du compte, puis retirer le préfixe « LXCA_ ».

Etape 3. Retirez les destinations d'alerte SNMP en sélectionnant **Gestion PEF** dans le menu principal, cliquez sur l'onglet **Destination LAN**, puis supprimez l'entrée qui pointe sur l'adresse IP de l'instance de XClarity Administrator.

Etape 4. Vérifiez que vos paramètres NTP sont valides en sélectionnant **Paramètres NTP** dans le menu principal, puis en configurant manuellement la date et l'heure ou en fournissant une adresse de serveur NTP valide.

Chapitre 9. Gestion des dispositifs de stockage

Lenovo XClarity Administrator peut gérer plusieurs types de dispositifs de stockage, notamment les systèmes de stockage Lenovo Storage, Flex System et les bandothèques.

En savoir plus :  XClarity Administrator : Reconnaissance

Avant de commencer

Attention : Passez en revue la section Remarques sur la gestion du stockage avant de gérer un dispositif de stockage.

Remarque : Les dispositifs de stockage Flex System sont automatiquement reconnus et gérés lorsque vous gérez le châssis dans lequel ils se trouvent. Vous ne pouvez pas reconnaître et gérer les dispositifs de stockage Flex System indépendants du châssis.

Certains ports doivent être disponibles pour communiquer avec des appareils. Vérifiez que tous les ports requis sont disponibles avant de tenter de gérer des dispositifs de stockage. Pour plus d'informations sur les ports, voir Disponibilité de port dans la documentation en ligne de XClarity Administrator.

Vérifiez que le microprogramme minimal requis est installé sur chaque dispositif de stockage que vous souhaitez gérer avec XClarity Administrator. Vous pouvez rechercher les niveaux de microprogramme minimum requis par la Support de XClarity Administrator – Page Web de compatibilité en cliquant sur l'onglet **Compatibilité**, puis en cliquant sur le lien des types d'appareil appropriés.

Important : Vérifiez que les exigences suivantes sont satisfaites avant de détecter et de gérer des dispositifs de stockage rack (autre que la série ThinkSystem DE). Pour plus d'informations, voir Impossible de reconnaître un appareil et Impossible de gérer un appareil dans la documentation en ligne de XClarity Administrator.

- La configuration réseau doit autoriser le trafic SLP entre XClarity Administrator et le dispositif de stockage rack.
- Protocole SLP monodiffusion est requis.
- La multidiffusion SLP est nécessaire si vous souhaitez que XClarity Administrator reconnaisse les dispositifs Lenovo Storage automatiquement. En outre, SLP doit être activé sur le dispositif de stockage rack.

À propos de cette tâche

XClarity Administrator peut détecter automatiquement des dispositifs de stockage dans votre environnement en sondant les dispositifs gérables présents dans le même sous-réseau IP que XClarity Administrator. Pour reconnaître les dispositifs de stockage qui se trouvent dans d'autres sous-réseaux, définissez une adresse IP ou une plage d'adresses IP ou importez les informations à partir d'un tableur.

Une fois que les dispositifs de stockage sont gérés par XClarity Administrator, XClarity Administrator interroge régulièrement chaque dispositif de stockage géré afin de collecter des informations, telles que l'inventaire, les données techniques essentielles et l'état. Vous pouvez afficher et surveiller chaque dispositif de stockage géré et effectuer des tâches de gestion (telles que la configuration des paramètres système, la mise à jour du microprogramme, ainsi que la mise sous tension et hors tension).

Un dispositif peut être géré par une seule instance XClarity Administrator à la fois. La gestion par plusieurs instances de XClarity Administrator n'est pas prise en charge. Si un dispositif est géré par une instance de

XClarity Administrator, et que vous souhaitez le gérer avec une autre instance de XClarity Administrator, vous devez d'abord annuler la gestion du dispositif dans l'instance de XClarity Administrator en cours, puis la gérer avec la nouvelle instance de XClarity Administrator. Si une erreur se produit lors du processus d'annulation de gestion, vous pouvez sélectionner l'option **Forcer la gestion** lors de la gestion sur la nouvelle instance de XClarity Administrator.

Remarque : En analysant le réseau pour rechercher des dispositifs gérables, XClarity Administrator ne sait pas si un dispositif est déjà géré par un autre gestionnaire avant d'avoir tenté de gérer le dispositif.

Procédure

Effectuez l'une des procédures suivantes pour gérer les dispositifs de stockage à l'aide de XClarity Administrator.

- Détectez et gérez un grand nombre d'appareils de stockage et d'autres types d'appareils à l'aide d'un fichier d'importation en masse (voir Gestion des systèmes dans la documentation en ligne XClarity Administrator).
- Reconnaissez et gérez les dispositifs de stockage présents sur le même sous-réseau IP que XClarity Administrator.
  1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Reconnaître et gérer de nouveaux appareils**. La page Reconnaître et gérer de nouveaux appareils s'affiche.

Vous pouvez trier les colonnes du tableau afin de faciliter la recherche des dispositifs de stockage que vous souhaitez gérer. En outre, vous pouvez entrer du texte (comme un nom ou l'adresse IP) dans la zone **Filtre** pour filtrer davantage les systèmes de stockage affichés. Vous pouvez modifier les colonnes qui s'affichent et l'ordre de tri par défaut en cliquant sur l'icône **Personnaliser les colonnes** ().

2. Cliquez sur l'icône **Actualiser** () pour reconnaître tous les périphériques gérables dans le domaine XClarity Administrator. La reconnaissance peut prendre plusieurs minutes.
3. Sélectionnez un ou plusieurs dispositifs de stockage à gérer.
4. Cliquez sur **Gérer la sélection**. La boîte de dialogue Gérer s'affiche.
5. Spécifiez l'ID utilisateur et le mot de passe pour l'authentification au dispositif de stockage.

   Astuce : Il est recommandé d'utiliser un compte administrateur ou superviseur pour gérer l'appareil. Si un compte avec un niveau de droits plus bas est utilisé, la gestion peut échouer, ou la gestion peut aboutir, mais d'autres futures opérations XClarity Administrator sur l'appareil peuvent échouer (notamment si l'appareil est géré sans authentification gérée).
6. Cliquez sur **Modifier** pour modifier les groupes de rôles qui doivent être affectés aux appareils.

   Remarques :

   - Vous pouvez effectuer votre sélection dans une liste de groupes de rôles affectée à l'utilisateur en cours.
   - Si vous ne modifiez pas les groupes de rôles, les groupes de rôles par défaut sont utilisés. Pour plus d'informations sur les groupes de rôles par défaut, voir Modification des droits par défaut.
7. Cliquez sur **Gérer**.

   Une boîte de dialogue s'affiche et présente la progression de ce processus de gestion. Pour vérifier si le processus aboutit, surveillez la progression.
8. Une fois le processus terminé, cliquez sur **OK**.

   Le dispositif est désormais géré par XClarity Administrator, qui interroge automatiquement et régulièrement le dispositif géré afin de collecter des informations à jour, telles que l'inventaire.

   Si la gestion n'a pas abouti en raison d'une des conditions d'erreur suivantes, répétez cette procédure en utilisant l'option **Forcer la gestion**.

   - Si l'instance de XClarity Administrator a échoué et ne peut pas être récupérée.

     Remarque : Si l'instance de remplacement de XClarity Administrator utilise la même adresse IP que l'instance de XClarity Administrator ayant rencontré une défaillance, vous pouvez gérer à nouveau le dispositif à l'aide du compte et du mot de passe RECOVERY_ID (le cas échéant) et de l'option **Forcer la gestion**.
   - Si l'instance XClarity Administrator de gestion a été mise hors tension avant que la gestion des appareils n'ait été annulée.
   - Si l'annulation de la gestion des appareils n'a pas été correctement effectuée.

   Attention : Les appareils peuvent être géré par une seule instance XClarity Administrator à la fois. La gestion par plusieurs instances de XClarity Administrator n'est pas prise en charge. Si un appareil est géré par une instance de XClarity Administrator, et que vous souhaitez le gérer avec une autre instance de XClarity Administrator, vous devez d'abord annuler la gestion de l'appareil dans l'instance de XClarity Administrator d'origine, puis la gérer avec la nouvelle instance de XClarity Administrator.

- Reconnaissez et gérez les dispositifs de stockage qui ne figurent pas sur le même sous-réseau IP que XClarity Administrator en spécifiant manuellement des adresses IP.

1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Reconnaître et gérer de nouveaux appareils**. La page Reconnaître et gérer s'affiche.
2. Sélectionnez **Saisie manuelle**.
3. Indiquez les adresses réseau des dispositifs de stockage que vous souhaitez gérer :
   - Cliquez sur **Système unique**, puis entrez un nom de domaine d'adresse IP unique, ou un nom de domaine complet (FQDN).

     Remarque : Pour indiquer un nom FQDN, vérifiez qu'un nom de domaine valide est spécifié sur la page Accès réseau (voir Configuration de l'accès réseau).
   - Cliquez sur **Plusieurs systèmes** et entrez une plage d'adresses IP. Pour ajouter une autre plage, cliquez sur l'icône **Ajouter** (). Pour supprimer une plage, cliquez sur l'icône **Supprimer** ().
4. Cliquez sur **OK**.
5. Spécifiez l'ID utilisateur et le mot de passe pour l'authentification au dispositif de stockage.

   Astuce : Il est recommandé d'utiliser un compte administrateur ou superviseur pour gérer l'appareil. Si un compte avec un niveau de droits plus bas est utilisé, la gestion peut échouer, ou la gestion peut aboutir, mais d'autres futures opérations XClarity Administrator sur l'appareil peuvent échouer (notamment si l'appareil est géré sans authentification gérée).
6. Cliquez sur **Modifier** pour modifier les groupes de rôles qui doivent être affectés aux appareils.

   Remarques :
   - Vous pouvez effectuer votre sélection dans une liste de groupes de rôles affectée à l'utilisateur en cours.
   - Si vous ne modifiez pas les groupes de rôles, les groupes de rôles par défaut sont utilisés. Pour plus d'informations sur les groupes de rôles par défaut, voir Modification des droits par défaut.
7. Cliquez sur **Gérer**.

   Une boîte de dialogue s'affiche et présente la progression de ce processus de gestion. Pour vérifier si le processus aboutit, surveillez la progression.
8. Une fois le processus terminé, cliquez sur **OK**.

   Le dispositif est désormais géré par XClarity Administrator, qui interroge automatiquement et régulièrement le dispositif géré afin de collecter des informations à jour, telles que l'inventaire.

   Si la gestion n'a pas abouti en raison d'une des conditions d'erreur suivantes, répétez cette procédure en utilisant l'option **Forcer la gestion**.
   - Si l'instance de XClarity Administrator a échoué et ne peut pas être récupérée.

     Remarque : Si l'instance de remplacement de XClarity Administrator utilise la même adresse IP que l'instance de XClarity Administrator ayant rencontré une défaillance, vous pouvez gérer à nouveau le dispositif à l'aide du compte et du mot de passe RECOVERY_ID (le cas échéant) et de l'option **Forcer la gestion**.
   - Si l'instance XClarity Administrator de gestion a été mise hors tension avant que la gestion des appareils n'ait été annulée.
   - Si l'annulation de la gestion des appareils n'a pas été correctement effectuée.

   Attention : Les appareils peuvent être géré par une seule instance XClarity Administrator à la fois. La gestion par plusieurs instances de XClarity Administrator n'est pas prise en charge. Si un appareil est géré par une instance de XClarity Administrator, et que vous souhaitez le gérer avec une autre instance de XClarity Administrator, vous devez d'abord annuler la gestion de l'appareil dans l'instance de XClarity Administrator d'origine, puis la gérer avec la nouvelle instance de XClarity Administrator.

Après avoir terminé

- Reconnaître et gérer d'autres dispositifs.
- Mettez à jour le microprogramme sur les dispositifs qui ne sont pas en conformité avec les stratégies actuelles (voir Mise à jour du microprogramme sur les appareils gérés).
- Ajouter les nouveaux dispositifs dans l'armoire appropriée pour refléter l'environnement physique (voir Gestion des armoires).
- Surveillez l'état et les informations détaillées du matériel (voir Affichage de l'état des dispositifs de stockage).
- Surveillez les événements et alertes (voir Utilisation des événements et Utilisation des alertes).

Remarques sur la gestion du stockage

Avant de gérer un dispositif de stockage, prenez connaissance des remarques importantes présentées ci-après.

Pour plus d'informations sur les exigences liées aux ports, voir Disponibilité de port dans la documentation en ligne de Lenovo XClarity Administrator.

Important : Vérifiez que les exigences suivantes sont satisfaites avant de détecter et de gérer des dispositifs de stockage rack (autre que la série ThinkSystem DE). Pour plus d'informations, voir Impossible de reconnaître un appareil et Impossible de gérer un appareil dans la documentation en ligne de XClarity Administrator.

- La configuration réseau doit autoriser le trafic SLP entre XClarity Administrator et le dispositif de stockage rack.
- Protocole SLP monodiffusion est requis.
- La multidiffusion SLP est nécessaire si vous souhaitez que XClarity Administrator reconnaisse les dispositifs Lenovo Storage automatiquement. En outre, SLP doit être activé sur le dispositif de stockage rack.

Pour les dispositifs Lenovo Storage, la température ambiante au niveau du système est mesurée par le détecteur de température le plus proche de la carte médiane du système et reflète la température ambiante après le passage de la ventilation au travers des unités. Notez que la température ambiante signalée par XClarity Administrator et celle communiquée par le contrôleur de gestion peuvent être différentes si elles sont capturées à des moments différents.

Pour les dispositifs de stockage Lenovo série DE, les deux contrôleurs de gestion doivent être accessibles sur le réseau lors de la gestion initiale.

Pour certains dispositifs de stockage, les alertes SNMP sont uniquement en anglais.

Affichage de l'état des dispositifs de stockage

Vous pouvez afficher des informations d'état récapitulatives et détaillées pour les dispositifs de stockage gérés à partir de Lenovo XClarity Administrator.

En savoir plus :

- XClarity Administrator : Inventaire
- XClarity Administrator : Surveillance

À propos de cette tâche

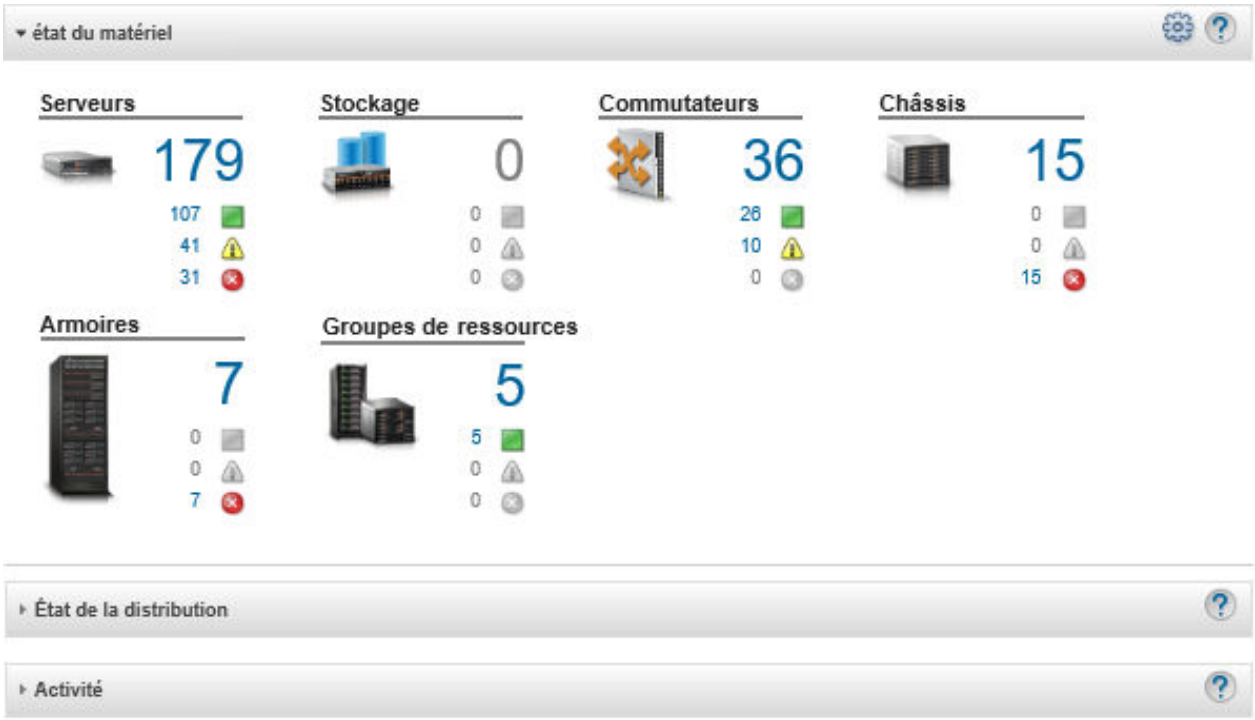
Les icônes d'état suivantes sont utilisées pour indiquer l'état de santé global de l'appareil. Si les certificats ne correspondent pas, la mention « (Non sécurisé) » est ajoutée à l'état de chaque appareil concerné, par exemple Avertissement (Non sécurisé). En cas de problème de connectivité ou si une connexion à l'appareil n'est pas sécurisée, la mention « (Connectivité) » est ajoutée à l'état de chaque appareil concerné, par exemple Avertissement (Connectivité).

- ( ) Critique
- ( ) Avertissement
- ( ) En attente
- ( ) Informations
- ( ) Normal
- ( ) Hors ligne
- ( ) Inconnu

Procédure

Pour afficher l'état d'un dispositif de stockage géré, exécutez l'une ou plusieurs des actions suivantes.

- Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Tableau de bord**. La page Tableau de bord affiche la présentation et l'état de tous les dispositifs de stockage gérés et d'autres ressources.



- Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Matériel → Stockage**. La page Stockage affiche une vue tabulaire de tous les dispositifs de stockage installés dans un châssis géré.

  Vous pouvez trier les colonnes du tableau afin de faciliter la recherche des dispositifs de stockage que vous souhaitez gérer. En outre, saisissez du texte (par exemple, un nom de système ou une adresse IP) dans la zone **Filtre** et cliquez sur les icônes d'état pour afficher uniquement la liste des dispositifs de stockage qui répondent aux critères sélectionnés.

Depuis cette page, vous pouvez effectuer les actions suivantes :

- Afficher des informations détaillées sur le dispositif de stockage et ses composants (voir Affichage des détails d'un dispositif de stockage).
- Afficher un dispositif de stockage dans la vue graphique Armoire ou Châssis en cliquant sur **Toutes les actions → Vues → Afficher dans la vue Armoire** ou sur **Toutes les actions → Vues → Afficher dans la vue Châssis**.
- Lancer l'interface Web du contrôleur de gestion pour le dispositif de stockage en cliquant sur le lien **Adresse IP** (voir Lancement de l'interface du contrôleur de gestion pour un dispositif de stockage).
- Mettre sous tension et hors tension le contrôleur de stockage dans le dispositif de stockage (voir Mise sous tension et hors tension d'un dispositif de stockage).
- Modifier des informations système en sélectionnant un dispositif de stockage, puis en cliquant sur **Toutes les actions → Inventaire → Éditer les propriétés**.
- Actualiser l'inventaire en sélectionnant un dispositif de stockage et en cliquant sur **Toutes les actions → Inventaire → Actualiser l'inventaire**.
- Exporter des informations détaillées relatives à un ou plusieurs dispositifs de stockage vers un seul fichier CSV en sélectionnant les dispositifs de stockage et en cliquant sur **Toutes les actions → Inventaire → Exporter l'inventaire**.

  Remarque : Vous pouvez exporter les données d'inventaire pour un maximum de 60 dispositifs en même temps.

  Conseil : Lors de l'importation d'un fichier CSV dans Microsoft Excel, Excel traite les valeurs textuelles contenant uniquement des numéros sous la forme de valeurs numériques (par exemple, pour des UUID). Formatez chaque cellule sous forme de texte pour résoudre cette erreur.
- Annuler la gestion du dispositif de stockage (voir Désactivation de la gestion d'un dispositif de stockage).
- (Dispositifs de stockage Flex System uniquement) Réinstaller virtuellement le contrôleur de stockage dans le dispositif de stockage (voir Réinstallation virtuelle de contrôleurs de stockage dans un dispositif de stockage Flex System).
- Exclure les événements qui ne vous intéressent pas de toutes les pages sur lesquelles des événements sont affichés en cliquant sur l'icône **Exclure des événements** ( ). (Voir Exclusion d'événements).
- Corriger les problèmes pouvant survenir entre le certificat de sécurité de Lenovo XClarity Administrator et le certificat de sécurité du CMM dans le châssis dans lequel le dispositif de stockage est installé en sélectionnant un dispositif de stockage et en cliquant sur **Toutes les actions → Sécurité → Résoudre les certificats non sécurisés** (voir Résolution d'un certificat du serveur non sécurisé).
- Ajoutez ou retirez un dispositif de stockage d'un groupe de ressources statique en cliquant sur **Toutes les actions → Groupes → Ajouter au groupe** ou **Toutes les actions → Groupes → Retirer du groupe**.

Affichage des détails d'un dispositif de stockage

Vous pouvez afficher des informations détaillées sur des dispositifs de stockage gérés à partir de Lenovo XClarity Administrator, y compris l'adresse IP, le nom de produit, le numéro de série et les caractéristiques de chaque cartouche.

À propos de cette tâche

En savoir plus :

- XClarity Administrator : Inventaire
- XClarity Administrator : Surveillance

Pour les dispositifs Lenovo Storage, la température ambiante au niveau du système est mesurée par le détecteur de température le plus proche de la carte médiane du système et reflète la température ambiante après le passage de la ventilation au travers des unités. Notez que la température ambiante signalée par XClarity Administrator et celle communiquée par le contrôleur de gestion peuvent être différentes si elles sont capturées à des moments différents.

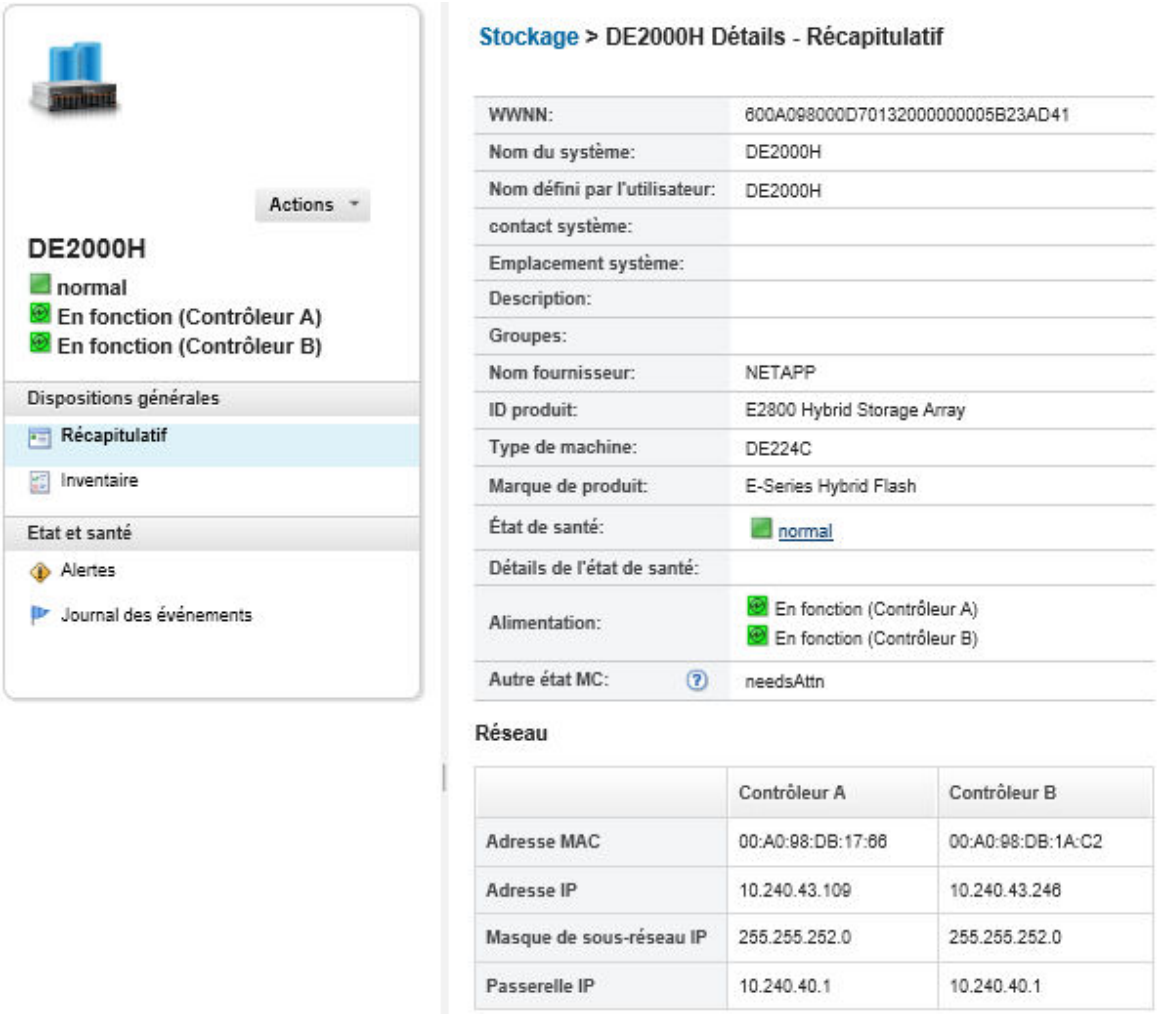
Procédure

Pour afficher les détails d'un dispositif de stockage géré spécifique, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Stockage**. La page Stockage affiche une vue tabulaire de tous les dispositifs de stockage installés dans un châssis géré.

Vous pouvez trier les colonnes du tableau afin de faciliter la recherche de dispositifs de stockage spécifiques. En outre, vous pouvez saisir un texte (par exemple, un nom de système ou une adresse IP) dans la zone **Filtre** pour filtrer davantage l'affichage des dispositifs de stockage.

Etape 2. Cliquez sur le nom du dispositif de stockage dans la colonne **Stockage**. La page Récapitulatif s'affiche et présente les propriétés, ainsi que la liste des composants installés dans ce dispositif de stockage.



Etape 3. Procédez à au moins l'une des actions suivantes pour afficher des informations sur le stockage. En fonction du type de dispositif de stockage, il se peut que les données affichées ne soient pas identiques.

- Cliquez sur **Récapitulatif** pour afficher un récapitulatif du serveur et des composants qu'il contient, y compris les informations système et les dispositifs installés (voir Affichage de l'état des dispositifs de stockage).
- Cliquez sur **Détails d'inventaire** pour afficher des détails sur les composants du dispositif de stockage, y compris :
  - Les niveaux de microprogramme du dispositif de stockage.
  - Les détails du réseau de contrôleur de gestion, tels que le nom d'hôte, l'adresse IPv4, l'adresse IPv6 et les adresses MAC.
  - Les détails des actifs du dispositif de stockage.
  - Les détails relatifs à chaque cartouche présente dans le dispositif de stockage.

  Astuce : Si un nœud d'extension, tel qu'un Nœud d'extension de stockage Flex System ou un PCIe Expansion Node Flex System est installé dans le châssis et connecté à un dispositif de stockage, les détails d'inventaire du nœud d'extension s'affichent également.
- Cliquez sur **Alertes** pour afficher les alertes de la liste d'alertes qui sont liées au dispositif de stockage (voir Utilisation des alertes).
- Cliquez sur **Journal des événements** pour afficher les événements du journal des événements qui sont liés au dispositif de stockage dispositif de stockage (voir Utilisation des événements).

- Cliquez sur **Travaux** pour afficher la liste des travaux associés au dispositif de stockage (voir Surveillance des travaux).
- Cliquez sur **Light Path** pour afficher l'état actuel de chaque voyant sur le dispositif de stockage.
- Cliquez sur **Électrique et thermique** pour afficher les caractéristiques électriques et thermiques du dispositif de stockage.

  Conseil : utilisez le bouton d'actualisation de votre navigateur Web pour collecter les dernières données électriques et thermiques. La collecte de données peut prendre plusieurs minutes.

Après avoir terminé

En plus d'afficher le récapitulatif et des informations détaillées relatives à un dispositif de stockage, vous pouvez effectuer les actions suivantes :

- Afficher un dispositif de stockage dans la vue graphique Armoire ou Châssis en cliquant sur **Actions → Vues → Afficher dans la vue Armoire** ou sur **Actions → Vues → Afficher dans la vue Châssis**.
- Exporter des informations détaillées sur le dispositif de stockage dans un fichier CSV en cliquant sur **Actions → Inventaire → Exporter l'inventaire**.

  Remarques :

  – Pour plus d'informations sur les données d'inventaire dans le fichier CSV, voirGET /storage/<*UUID_list*> REST API dans la documentation en ligne de Lenovo XClarity Administrator.

  – Lors de l'importation d'un fichier CSV dans Microsoft Excel, Excel traite les valeurs textuelles contenant uniquement des numéros sous la forme de valeurs numériques (par exemple, pour des UUID). Formatez chaque cellule sous forme de texte pour résoudre cette erreur.
- Lancer l'interface Web du contrôleur de gestion pour le dispositif de stockage en cliquant sur le lien **Adresse IP** (voir Lancement de l'interface du contrôleur de gestion pour un dispositif de stockage).
- Mettre sous tension et hors tension un contrôleur de stockage dans le dispositif de stockage (voir Mise sous tension et hors tension d'un dispositif de stockage).
- Réinstaller virtuellement le contrôleur de stockage dans le dispositif de stockage (voir Réinstallation virtuelle d'un serveur dans un châssis Flex System).
- Modifier des informations système en sélectionnant un dispositif de stockage, puis en cliquant sur **Éditer les propriétés**.
- Actualiser l'inventaire en sélectionnant un dispositif de stockage, puis en cliquant sur **Actions → Inventaire → Actualiser l'inventaire**.
- Exclure les événements qui ne vous intéressent pas de toutes les pages sur lesquelles des événements sont affichés en cliquant sur **Actions → Réinitialisation de service → Exclure des événements** (voir Exclusion d'événements).
- Corriger les problèmes pouvant survenir entre le certificat de sécurité de XClarity Administrator et le certificat de sécurité du CMM dans le châssis dans lequel le dispositif de stockage est installé en sélectionnant un dispositif de stockage, puis en cliquant sur **Actions → Service → Résoudre les certificats non sécurisés** (voir Résolution d'un certificat du serveur non sécurisé).

Sauvegarde et restauration des données de configuration de stockage

Lenovo XClarity Administrator n'inclut pas de fonctions de sauvegarde intégrées pour les données de configuration de stockage. À la place, utilisez les fonctions de sauvegarde qui sont disponibles pour votre dispositif de stockage géré.

Pour plus d'informations sur la récupération de l'appareil, consultez la documentation produit fournie avec votre dispositif de stockage.

- Pour les dispositifs Lenovo Storage, voir Documentation du produit Lenovo Storage S2200/S3200.
- Pour les dispositifs de stockage Lenovo ThinkSystem, voir Documentation du produit ThinkSystem Storage.

Mise sous tension et hors tension d'un dispositif de stockage

Vous pouvez mettre sous tension et hors tension un dispositif de stockage à partir de Lenovo XClarity Administrator.

À propos de cette tâche

Pour les dispositifs de stockage Flex System, lorsqu'un contrôleur de stockage est mis hors tension, les données sont d'abord stockées sur l'unité interne et l'unité de stockage entre en état de veille. En état de veille, les volumes qui sont fournis par le dispositif de stockage ne sont plus accessibles.

Pour mettre sous tension un dispositif de stockage ThinkSystem DM Series, vérifiez que le contrôleur de stockage qui est utilisé pour la gestion est en ligne, et que l'adresse IP est en mesure de communiquer directement avec le processeur de service du contrôleur de stockage de hors tension via le réseau externe.

Procédure

Procédez comme suit pour mettre sous et hors tension un dispositif de stockage géré.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Stockage**. La page Stockage affiche une vue tabulaire de tous les dispositifs de stockage installés dans un châssis géré.

Vous pouvez trier les colonnes du tableau afin de faciliter la recherche de dispositifs de stockage spécifiques. En outre, vous pouvez saisir un texte (par exemple, un nom de système ou une adresse IP) dans la zone **Filtre** pour filtrer davantage l'affichage des dispositifs de stockage dispositifs de stockage.

Etape 2. Sélectionnez le dispositif de stockage à mettre sous tension ou hors tension.

Etape 3. Cliquez sur **Toutes les actions**, puis sur l'une des actions d'alimentation suivantes :
- **Mettre le contrôleur A sous tension**
- **Mettre le contrôleur B sous tension**
- **Mettre le contrôleur A hors tension**
- **Mettre le contrôleur B hors tension**
- **Redémarrer le contrôleur A**
- **Redémarrer le contrôleur B**

Réinstallation virtuelle de contrôleurs de stockage dans un dispositif de stockage Flex System

Vous pouvez effectuer une réinstallation virtuelle et simuler ainsi le retrait et l'insertion d'un contrôleur de stockage (cartouche) dans la baie du dispositif de stockage.

À propos de cette tâche

Au cours de la réinstallation virtuelle, toutes les connexions réseau au dispositif de stockage sont perdues et l'état d'alimentation de ce dernier change. Avant d'effectuer une réinstallation virtuelle, vérifiez que vous avez enregistré toutes les données utilisateur.

Procédure

Procédez comme suit virtuelle pour réinstaller virtuellement un contrôleur de stockage.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Matériel → Stockage**. La page Stockage qui s'affiche présente une vue tabulaire de tous les dispositifs de stockage.

Vous pouvez trier les colonnes du tableau afin de faciliter la recherche de dispositifs de stockage spécifiques. En outre, vous pouvez saisir un texte (par exemple, un nom de système ou une adresse IP) dans la zone **Filtre** pour filtrer davantage l'affichage des dispositifs de stockage.

Etape 2. Sélectionnez le dispositif de stockage Flex System.

Etape 3. Cliquez sur **Toutes les actions → Service**, puis sur **Réinstallation virtuelle du contrôleur A** ou **Réinstallation virtuelle du contrôleur B**.

Etape 4. Cliquez sur **Réinstallation virtuelle**.

Lancement de l'interface du contrôleur de gestion pour un dispositif de stockage

Vous pouvez lancer l'interface Web du contrôleur de gestion pour le châssis dans lequel le dispositif de stockage est installé à partir de Lenovo XClarity Administrator.

Procédure

Procédez comme suit pour lancer une interface Web du contrôleur de gestion.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Stockage**. La page Stockage qui s'affiche présente une vue tabulaire de tous les dispositifs de stockage gérés.

Vous pouvez trier les colonnes du tableau afin de faciliter la recherche de dispositifs de stockage spécifiques. En outre, vous pouvez saisir un texte (par exemple, un nom de dispositif ou une adresse IP) dans la zone **Filtre** pour filtrer davantage l'affichage des dispositifs de stockage.

Etape 2. Sélectionnez le dispositif de stockage.

Etape 3. Cliquez sur **Actions → Lancer → Interface Web de gestion**. L'interface Web du contrôleur de gestion est démarrée.

Etape 4. Connectez-vous à l'interface du contrôleur de gestion.

Remarque : Pour les dispositifs de stockage Flex System, utilisez les données d'identification de l'utilisateur de XClarity Administrator.

Modification des propriétés système pour un dispositif de stockage

Vous pouvez modifier les propriétés système d'un dispositif de stockage spécifique.

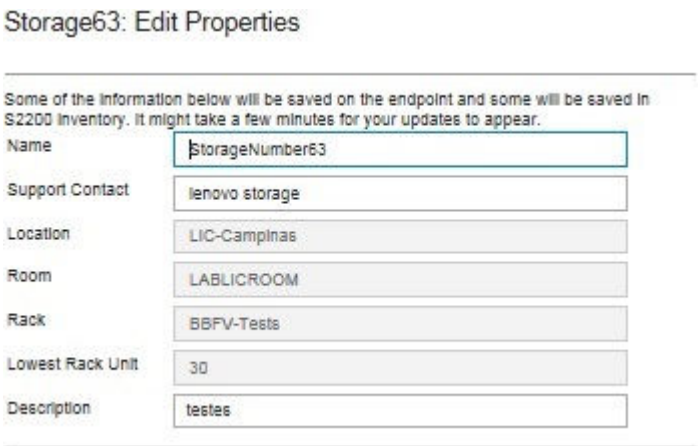
Procédure

Procédez comme suit pour modifier les propriétés système :

Etape 1. Dans la barre de menus Lenovo XClarity Administrator, cliquez sur **Matériel → Stockage** pour afficher la page Stockage.

Etape 2. Sélectionnez le dispositif de stockage à mettre à jour.

Etape 3. Cliquez sur **Toutes les actions → Inventaire → Éditer les propriétés** pour afficher la boîte de dialogue Éditer.



Etape 4. Modifiez les informations suivantes, si nécessaire.
- Nom
- Contact pour support technique
- Description

Remarque : XClarity Administrator met à jour l'emplacement, la pièce, l'armoire et les propriétés de l'unité d'armoire la plus basse lorsque vous ajoutez ou supprimez des dispositifs d'une armoire dans l'interface Web (voir Gestion des armoires).

Etape 5. Cliquez sur **Enregistrer**.

Remarque : Si vous modifiez ces propriétés, vous devrez peut-être attendre quelques instants avant que les modifications n'apparaissent dans l'interface Web XClarity Administrator.

Récupération de la gestion d'un dispositif de stockage rack après une défaillance du serveur de gestion

Si la gestion d'un dispositif de stockage rack n'a pas été correctement annulée, vous devez récupérer ce dispositif de stockage pour pouvoir le gérer à nouveau. Vous pouvez récupérer la gestion en effaçant des parties spécifiques de la configuration du dispositif de stockage précédemment définie par Lenovo XClarity Administrator.

Procédure

Exécutez l'une des étapes suivantes pour récupérer un dispositif de stockage rack.

- Si l'instance de remplacement de XClarity Administrator utilise la même adresse IP que l'instance de XClarity Administrator défectueuse, vous pouvez gérer à nouveau le dispositif à l'aide de l'option **Forcer la gestion** (voir Gestion des dispositifs de stockage).
- Retirez tous les comptes utilisateur comportant le préfixe « LXCA_ » et, le cas échéant, retirez les comptes utilisateur comportant le préfixe « SYSMGR_ » et dont le type est « SNMPv3 » dans le dispositif de stockage.

Après avoir terminé

Après la restauration ou le remplacement de XClarity Administrator, vous pouvez gérer à nouveau le dispositif de stockage (voir Gestion des dispositifs de stockage). Toutes les informations sur le dispositif de stockage (par exemple, les propriétés système) sont conservées.

Récupération de la gestion d'un dispositif de stockage Lenovo ThinkSystem DE Series après une défaillance du serveur de gestion

Si la gestion d'un dispositif de stockage Lenovo ThinkSystem DE Series n'a pas été correctement annulée, vous devez récupérer ce dispositif de stockage pour pouvoir le gérer à nouveau. Vous pouvez récupérer la gestion en effaçant des parties spécifiques de la configuration du dispositif de stockage précédemment définie par Lenovo XClarity Administrator.

Procédure

Exécutez l'une des étapes suivantes pour récupérer un dispositif de stockage Lenovo ThinkSystem DE Series.

- Si l'instance de remplacement de XClarity Administrator utilise la même adresse IP que l'instance de XClarity Administrator défectueuse, vous pouvez gérer à nouveau le dispositif à l'aide de l'option **Forcer la gestion** (voir Gestion des dispositifs de stockage).
- Retirez l'enregistrement de paire de clés « LXCA_REMOTE_MANAGMENT_VERIFICATION » de l'API de paire de clés du dispositif de stockage.

Après avoir terminé

Après la restauration ou le remplacement de XClarity Administrator, vous pouvez gérer à nouveau le dispositif de stockage (voir Gestion des dispositifs de stockage). Toutes les informations sur le dispositif de stockage (par exemple, les propriétés système) sont conservées.

Désactivation de la gestion d’un dispositif de stockage

Vous pouvez retirer un dispositif de stockage de la gestion par Lenovo XClarity Administrator. Ce processus est appelé *annulation de la gestion.*

Avant de commencer

Avant d’annuler la gestion d’un dispositif de stockage, vérifiez qu’il n’y a pas de travaux actifs en cours d’exécution sur le commutateur.

À propos de cette tâche

Lorsque vous avez annulé la gestion d'un dispositif de stockage, XClarity Administrator conserve certaines informations sur le dispositif de stockage. Ces informations sont réappliquées lorsque vous gérez à nouveau le même dispositif de stockage.

Astuce : Tous les appareils de démonstration qui sont éventuellement ajoutés lors de la configuration initiale sont des nœuds dans un châssis. Pour annuler la gestion des appareils de démonstration, annulez la gestion du châssis à l’aide de l'option **Forcer l'annulation de la gestion, même si l'appareil est inaccessible**.

Procédure

Pour annuler la gestion d’un dispositif de stockage, procédez comme suit.

Etape 1. Dans la barre de menus XClarity Administrator, cliquez sur **Matériel → Stockage** pour afficher la page Stockage.

Etape 2. Sélectionnez un ou plusieurs dispositifs de stockage dans les listes de commutateurs gérés.

Etape 3. Cliquez sur **Annuler la gestion**. Le dialogue Annuler la gestion s'affiche.

Etape 4. **Facultatif :** sélectionnez **Forcer l'annulation de la gestion, même si l'appareil est inaccessible**.

Important : Lors de l'annulation de la gestion du matériel de démonstration, veillez à sélectionner cette option.

Etape 5. Cliquez sur **Annuler la gestion**.La boîte de dialogue Annuler la gestion affiche la progression de chaque étape dans le processus d'annulation de gestion.

Etape 6. Une fois le processus d'annulation de gestion terminé, cliquez sur **OK**.

Récupération d'un dispositif de stockage rack dont la gestion n'a pas été correctement annulée

Si Lenovo XClarity Administrator gère un dispositif de stockage rack et qu'une défaillance se produit sur XClarity Administrator, vous pouvez récupérer les fonctions de gestion en attendant que le serveur de gestion soit restauré ou remplacé. Vous pouvez récupérer la gestion du système en effaçant des parties spécifiques de la configuration du dispositif de stockage précédemment définie par XClarity Administrator.

Procédure

Exécutez l'une des étapes suivantes pour récupérer un dispositif de stockage rack.

- Si l'instance de remplacement de XClarity Administrator utilise la même adresse IP que l'instance de XClarity Administrator défectueuse, vous pouvez gérer à nouveau le dispositif à l'aide de l'option **Forcer la gestion** (voir Gestion des dispositifs de stockage).

- Retirez tous les comptes utilisateur comportant le préfixe « LXCA_ » et, le cas échéant, retirez les comptes utilisateur comportant le préfixe « SYSMGR_ » et dont le type est « SNMPv3 » dans le dispositif de stockage.

Après avoir terminé

Après la restauration ou le remplacement de XClarity Administrator, vous pouvez gérer à nouveau le dispositif de stockage (voir Gestion des dispositifs de stockage). Toutes les informations sur le dispositif de stockage (par exemple, les propriétés système) sont conservées.

Chapitre 10. Gestion des commutateurs

Lenovo XClarity Administrator peut gérer des commutateurs réseau.

En savoir plus :

- XClarity Administrator : Reconnaissance
- XClarity Administrator : gestion des commutateurs

Avant de commencer

Attention : Tenez compte des remarques sur la gestion des commutateurs avant de gérer un commutateur. Pour plus d'informations, voir Remarques sur la gestion des commutateurs.

Remarque : Les commutateurs Flex sont automatiquement reconnus et gérés lorsque vous gérez le châssis dans lequel ils se trouvent. Vous ne pouvez pas reconnaître et gérer les commutateurs Flex indépendants d'un châssis.

Certains ports doivent être disponibles pour permettre la communication avec les commutateurs. Vérifiez que tous les ports requis sont disponibles avant de tenter de gérer un commutateur. Pour plus d'informations sur les ports, voir Disponibilité de port dans la documentation en ligne de XClarity Administrator.

Vérifiez que le microprogramme minimal requis est installé sur chaque commutateur que vous souhaitez gérer à l'aide de XClarity Administrator. Vous pouvez rechercher les niveaux de microprogramme minimum requis par la Support de XClarity Administrator – Page Web de compatibilité en cliquant sur l'onglet **Compatibilité**, puis en cliquant sur le lien des types d'appareil appropriés.

Vérifiez que vous créez des données d'identification stockées dans XClarity Administrator avant de gérer les commutateurs d'armoire. XClarity Administrator utilise les données d'identification stockées uniquement pour l'authentification auprès des commutateurs d'armoire. Les données d'identification stockées doivent correspondre à un compte utilisateur actif sur l'appareil. Vous pouvez créer des données d'identification stockées à partir des boîtes de dialogue de gestion ou de la page Données d'identification stockées. Pour plus d'informations, voir Gestion de données d'identification stockées.

La gestion à l'aide d'interfaces en boucle est prise en charge pour tous les appareils RackSwitch. Vérifiez que XClarity Administrator dispose d'une connectivité à l'interface en boucle, en ajoutant une route statique ou en annonçant l'adresse via un protocole de routage. Notez que le cheminement des câbles ne peut pas être effectué entre le port de gestion et *des* ports de données (y compris en boucle).

Pour les commutateurs Lenovo ThinkSystem série DB :

- FOS 8.2.3 ou une version ultérieure est nécessaire
- Assurez-vous de bien configurer l'utilisateur SNMPv3 au niveau de l'indice 1 sur le commutateur *avant* de gérer le commutateur en exécutant la commande ci-après sur le commutateur : `snmpconfig --add snmpv3 -index 1 -user snmpadmin1 -groupname rw`
- Assurez-vous que REST est activé sur le commutateur. Pour activer REST, exécutez la commande suivante : `mgmtapp --enable rest`
- Assurez-vous que le nombre de sessions REST autorisées est de 10. Pour définir le nombre de sessions REST, exécutez la commande suivante : `mgmtapp --config -maxrestsession 10`

- Les commutateurs Lenovo ThinkSystem série DB ne peuvent pas être reconnus à l'aide de protocoles de reconnaissance de service. Pour gérer ces commutateurs, utilisez l'option **Saisie manuelle**, effacez **Protocoles de reconnaissance de service utilisateur pour identifier le type d'appareil**, puis sélectionnez « Commutateur Lenovo ThinkSystem série DB » dans la liste **Type d'appareil**. Pour plus de détails, reportez-vous à la procédure ci-dessous sur la reconnaissance et la gestion des commutateurs qui ne font pas partie du même sous-réseau IP que XClarity Administrator.

Pour les commutateurs NVIDIA :

- Cumulus 4.3 ou une version ultérieure est nécessaire
- Les commutateurs NVIDIA ne peuvent pas être reconnus à l'aide de protocoles de reconnaissance de service. Pour gérer ces commutateurs, utilisez l'option **Saisie manuelle**, effacez Protocoles de reconnaissance de service utilisateur pour identifier le type d'appareil, puis sélectionnez « Commutateur NVIDIA » dans la liste **Type d'appareil**. Pour plus de détails, reportez-vous à la procédure ci-dessous sur la reconnaissance et la gestion des commutateurs qui ne font pas partie du même sous-réseau IP que XClarity Administrator.

À propos de cette tâche

XClarity Administrator peut détecter automatiquement des commutateurs RackSwitch dans votre environnement en sondant les appareils gérables présents dans le même sous-réseau IP que XClarity Administrator. Pour reconnaître les commutateurs qui se trouvent dans d'autres sous-réseaux, définissez une adresse IP ou une plage d'adresses IP ou importez les informations à partir d'un tableur.

Remarque : Les données d'identification manuelles ne sont pas prises en charge pour les commutateurs d'armoire dans XClarity Administrator.

Une fois que les commutateurs sont gérés par XClarity Administrator, XClarity Administrator interroge régulièrement chaque commutateur géré afin de collecter des informations, telles que l'inventaire, les données techniques essentielles et l'état. Vous pouvez afficher et surveiller chaque commutateur géré et effectuer des tâches de gestion, telles que le lancement de la console de gestion et la mise sous tension et hors tension.

Si le XClarity Administrator perd la communication avec le commutateur (par exemple, en raison d'une panne de courant ou de réseau, ou si le commutateur est hors ligne), alors qu'il collecte l'inventaire durant le processus de gestion, la gestion se terminera avec succès, toutefois certaines informations liées à l'inventaire peuvent être incomplètes. Patientez que le commutateur soit à nouveau en ligne et que XClarity Administrator interroge le commutateur pour obtenir les données d'inventaire, ou bien collectez manuellement l'inventaire sur le commutateur en sélectionnant ce dernier et en cliquant sur **Toutes les actions → Inventaire → Actualiser l'inventaire**.

Remarque : Les commutateurs peuvent être empilés. Un *commutateur empilé* est un groupe de commutateurs qui fonctionnent comme un seul commutateur réseau. La pile inclut un *commutateur principal* et un ou plusieurs *commutateurs membres*. Concernant les commutateurs Flex, vous pouvez afficher et surveiller chaque commutateur de ce type dans la pile et collecter des données de diagnostic ; en revanche, vous ne pouvez effectuer aucune tâche de gestion (comme les mises à jour de microprogramme et la configuration de serveur) sur un commutateur empilé. Ces tâches de gestion XClarity Administrator sont désactivées pour tous les commutateurs empilés, y compris le commutateur principal. Vous pouvez mettre à jour le microprogramme sur le commutateur empilé directement à partir de l'interface de ligne de commande de commutateur principal. Concernant les commutateurs RackSwitch, vous ne pouvez afficher et surveiller que les informations relatives au commutateur principal. Les commutateurs de membres ne sont pas reconnus par XClarity Administrator.

Les tâches de gestion sont également désactivées pour les Commutateurs Flex qui sont en mode protégé.

Un dispositif peut être géré par une seule instance XClarity Administrator à la fois. La gestion par plusieurs instances de XClarity Administrator n'est pas prise en charge. Si un dispositif est géré par une instance de XClarity Administrator, et que vous souhaitez le gérer avec une autre instance de XClarity Administrator, vous devez d'abord annuler la gestion du dispositif dans l'instance de XClarity Administrator en cours, puis la gérer avec la nouvelle instance de XClarity Administrator. Si une erreur se produit lors du processus d'annulation de gestion, vous pouvez sélectionner l'option **Forcer la gestion** lors de la gestion sur la nouvelle instance de XClarity Administrator.

Remarque : En analysant le réseau pour rechercher des dispositifs gérables, XClarity Administrator ne sait pas si un dispositif est déjà géré par un autre gestionnaire avant d'avoir tenté de gérer le dispositif.

Lorsqu'un commutateur est géré directement à l'aide de SSH ou indirectement via un module CMM, il est identifié comme étant géré par XClarity Administrator, la configuration nécessaire pour l'interaction est effectuée et l'inventaire est collecté.

Procédure

Exécutez l'une des procédures suivantes pour gérer vos commutateurs RackSwitch à l'aide de XClarity Administrator.

- Détectez et gérez un grand nombre de commutateurs et d'autres appareils à l'aide d'un fichier d'importation en masse (voir Gestion des systèmes dans la documentation en ligne Lenovo XClarity Administrator).
- Reconnaissez et gérez les commutateurs RackSwitch présents sur le même sous-réseau IP que XClarity Administrator.
  1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Reconnaître et gérer de nouveaux appareils**. La page Reconnaître et gérer de nouveaux appareils s'affiche.

Vous pouvez trier les colonnes du tableau afin de faciliter la recherche des commutateurs que vous souhaitez gérer. En outre, vous pouvez saisir un texte (par exemple, un nom ou une adresse IP) dans la zone **Filtre** pour filtrer davantage l'affichage des commutateurs. Vous pouvez modifier les colonnes qui s'affichent et l'ordre de tri par défaut en cliquant sur l'icône **Personnaliser les colonnes** ( ).

2. Cliquez sur l'icône **Actualiser** ( ) pour reconnaître tous les périphériques gérables dans le domaine XClarity Administrator. La reconnaissance peut prendre plusieurs minutes.
3. Sélectionnez un ou plusieurs commutateurs à gérer.
4. Cliquez sur **Gérer la sélection**.
5. Indiquez les données d'identification stockées pour l'authentification auprès des commutateurs.

   Astuce :

   - Cliquez sur **Gérer les données d'identification stockées** pour créer et gérer les données d'identification stockées dans XClarity Administrator (voir Gestion de données d'identification stockées).
   - Il est recommandé d'utiliser un compte administrateur ou superviseur pour gérer l'appareil. Si un compte avec un niveau de droits plus bas est utilisé, la gestion peut échouer, ou la gestion peut aboutir, mais d'autres opérations futures XClarity Administrator sur l'appareil peuvent échouer (notamment si l'appareil est géré sans authentification gérée).

6. (Commutateurs exécutant ENOS uniquement) S'il est défini, spécifiez le mot de passe « enable » qui est utilisé pour entrer en mode Exec Privileged sur le commutateur.

   Lorsque vous gérez un commutateur RackSwitch commutateur exécutant ENOS, l'accès au mode Exec Privileged sur le commutateur est requis. Cela est utilisé par XClarity Administrator en exécutant la commande « enable » sur le commutateur. Aucun mot de passe n'est défini par défaut pour cette commande sur le commutateur. Cependant, si l'administrateur de commutateur a configuré un mot de passe pour cette commande dans le but de renforcer la sécurité, celui-ci doit être spécifié pour permettre à XClarity Administrator de gérer correctement le commutateur.

7. Facultatif : (Commutateurs exécutant ENOS uniquement) Choisissez d'activer HTTPS sur le commutateur en cliquant sur **Avancé**, puis en sélectionnant **Activer HTTPS**. Cette option est activée par défaut.

   Remarques :

   - Pour les commutateurs exécutant CNOS, HTTPS doit être activé sur le commutateur avant la gestion (voir Remarques sur la gestion des commutateurs).
   - Si vous choisissez de ne pas activer HTTPS, le paramètre actuel sur le commutateur est utilisé.
   - Lorsque le commutateur est non géré, XClarity Administrator restaure HTTPS aux paramètres d'origine.

8. Facultatif : Indiquez si la configuration NTP doit être remplacée sur le commutateur par les paramètres de configuration NTP et les paramètres de fuseau horaire qui sont définis pour Lenovo XClarity Administrator en cliquant sur **Avancé**, puis en sélectionnant **Configurer les clients NTP afin d'utiliser les paramètres NTP depuis le serveur de gestion**. Cette option est activée par défaut.

   Remarques :

   - Si vous choisissez de ne *pas* remplacer la configuration NTP et le fuseau horaire, l'horodatage des entrées du journal et des événements ne sont plus synchronisés entre le commutateur géré et le serveur de gestion.
   - Lorsque le commutateur est non géré, XClarity Administrator restaure une configuration NTP et le fuseau horaire aux paramètres d'origine.

9. Cliquez sur **Modifier** pour modifier les groupes de rôles qui doivent être affectés aux appareils.

   Remarques :

   - Vous pouvez effectuer votre sélection dans une liste de groupes de rôles affectée à l'utilisateur en cours.
   - Si vous ne modifiez pas les groupes de rôles, les groupes de rôles par défaut sont utilisés. Pour plus d'informations sur les groupes de rôles par défaut, voir Modification des droits par défaut.

10. Cliquez sur **Gérer**.

    Une boîte de dialogue s'affiche et présente la progression de ce processus de gestion. Pour vérifier si le processus aboutit, surveillez la progression du travail.

11. Une fois le processus terminé, cliquez sur **OK**.

    Le dispositif est désormais géré par XClarity Administrator, qui interroge automatiquement et régulièrement le dispositif géré afin de collecter des informations à jour, telles que l'inventaire.

    Si la gestion n'a pas abouti en raison d'une des conditions d'erreur suivantes, répétez cette procédure en utilisant l'option **Forcer la gestion**.

    - Si l'instance de XClarity Administrator a échoué et ne peut pas être récupérée.

      Remarque : Si l'instance de remplacement de XClarity Administrator utilise la même adresse IP que l'instance de XClarity Administrator ayant rencontré une défaillance, vous pouvez gérer à

nouveau le dispositif à l'aide du compte et du mot de passe RECOVERY_ID (le cas échéant) et de l'option **Forcer la gestion**.

- Si l'instance XClarity Administrator de gestion a été mise hors tension avant que la gestion des appareils n'ait été annulée.
- Si l'annulation de la gestion des appareils n'a pas été correctement effectuée.

Attention : Les appareils peuvent être géré par une seule instance XClarity Administrator à la fois. La gestion par plusieurs instances de XClarity Administrator n'est pas prise en charge. Si un appareil est géré par une instance de XClarity Administrator, et que vous souhaitez le gérer avec une autre instance de XClarity Administrator, vous devez d'abord annuler la gestion de l'appareil dans l'instance de XClarity Administrator d'origine, puis la gérer avec la nouvelle instance de XClarity Administrator.

- Reconnaissez et gérez les commutateurs RackSwitch qui ne figurent pas sur le même sous-réseau IP que XClarity Administrator en spécifiant manuellement des adresses IP :
  1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Matériel → Reconnaître et gérer de nouveaux appareils**. La page Reconnaître et gérer s'affiche.
  2. Sélectionnez **Saisie manuelle**.
  3. Indiquez les adresses réseau des commutateurs que vous souhaitez gérer :
     - Cliquez sur **Système unique**, puis entrez un nom de domaine d'adresse IP unique, ou un nom de domaine complet (FQDN).

       Remarque : Pour indiquer un nom FQDN, vérifiez qu'un nom de domaine valide est spécifié sur la page Accès réseau (voir Configuration de l'accès réseau).
     - Cliquez sur **Plusieurs systèmes** et entrez une plage d'adresses IP. Pour ajouter une autre plage, cliquez sur l'icône **Ajouter** (). Pour supprimer une plage, cliquez sur l'icône **Supprimer** ().
  4. S'il n'est pas possible de reconnaître le type de dispositif à l'aide des protocoles de reconnaissance des services, effacez les protocoles de reconnaissance des services utilisateur pour identifier le type de dispositif, puis sélectionnez le type de dispositif devant être géré depuis le menu déroulant.

     Les protocoles de reconnaissance des services, comme SLP et SSDP, permettent à XClarity Administrator de reconnaître automatiquement le type de dispositif qui va être géré, puis de faire appel au mécanisme adapté pour le gérer. Certains types de dispositifs ne sont pas compatibles avec les protocoles de reconnaissance des services. Dans certains environnements, les protocoles de reconnaissance des services sont désactivés volontairement. Dans tous les cas, vous devez choisir le type de dispositif adapté pour mener à bien le processus de gestion. Les types de dispositifs suivants doivent être identifiés explicitement.
     - Commutateur Lenovo ThinkSystem série DB
     - Commutateur NVIDIA Mellanox
  5. Cliquez sur **OK**.
  6. Indiquez les données d'identification stockées pour l'authentification auprès des commutateurs.

     Astuce :

     - Cliquez sur **Gérer les données d'identification stockées** pour créer et gérer les données d'identification stockées dans XClarity Administrator (voir Gestion de données d'identification stockées).
     - Il est recommandé d'utiliser un compte administrateur ou superviseur pour gérer l'appareil. Si un compte avec un niveau de droits plus bas est utilisé, la gestion peut échouer, ou la gestion peut aboutir, mais d'autres opérations futures XClarity Administrator sur l'appareil peuvent échouer (notamment si l'appareil est géré sans authentification gérée).

7. (Commutateurs exécutant ENOS uniquement) S'il est défini, spécifiez le mot de passe « enable » qui est utilisé pour entrer en mode Exec Privileged sur le commutateur.

   Lorsque vous gérez un commutateur RackSwitch commutateur exécutant ENOS, l'accès au mode Exec Privileged sur le commutateur est requis. Cela est utilisé par XClarity Administrator en exécutant la commande « enable » sur le commutateur. Aucun mot de passe n'est défini par défaut pour cette commande sur le commutateur. Cependant, si l'administrateur de commutateur a configuré un mot de passe pour cette commande dans le but de renforcer la sécurité, celui-ci doit être spécifié pour permettre à XClarity Administrator de gérer correctement le commutateur.

8. Facultatif : (Commutateurs exécutant ENOS uniquement) Choisissez d'activer HTTPS sur le commutateur en cliquant sur **Avancé**, puis en sélectionnant **Activer HTTPS**. Cette option est activée par défaut.

   Remarques :

   - Pour les commutateurs exécutant CNOS, HTTPS doit être activé sur le commutateur avant la gestion (voir Remarques sur la gestion des commutateurs).
   - Si vous choisissez de ne pas activer HTTPS, le paramètre actuel sur le commutateur est utilisé.
   - Lorsque le commutateur est non géré, XClarity Administrator restaure HTTPS aux paramètres d'origine.

9. Facultatif : Indiquez si la configuration NTP doit être remplacée sur le commutateur par les paramètres de configuration NTP et les paramètres de fuseau horaire qui sont définis pour Lenovo XClarity Administrator en cliquant sur **Avancé**, puis en sélectionnant **Configurer les clients NTP afin d'utiliser les paramètres NTP depuis le serveur de gestion**. Cette option est activée par défaut.

   Remarques :

   - Si vous choisissez de ne *pas* remplacer la configuration NTP et le fuseau horaire, l'horodatage des entrées du journal et des événements ne sont plus synchronisés entre le commutateur géré et le serveur de gestion.
   - Lorsque le commutateur est non géré, XClarity Administrator restaure une configuration NTP et le fuseau horaire aux paramètres d'origine.

10. Cliquez sur **Modifier** pour modifier les groupes de rôles qui doivent être affectés aux appareils.

    Remarques :

    - Vous pouvez effectuer votre sélection dans une liste de groupes de rôles affectée à l'utilisateur en cours.
    - Si vous ne modifiez pas les groupes de rôles, les groupes de rôles par défaut sont utilisés. Pour plus d'informations sur les groupes de rôles par défaut, voir Modification des droits par défaut.

11. Cliquez sur **Gérer**.

    Une boîte de dialogue s'affiche et présente la progression de ce processus de gestion. Pour vérifier si le processus aboutit, surveillez la progression du travail.

12. Une fois le processus terminé, cliquez sur **OK**.

    Le dispositif est désormais géré par XClarity Administrator, qui interroge automatiquement et régulièrement le dispositif géré afin de collecter des informations à jour, telles que l'inventaire.

    Si la gestion n'a pas abouti en raison d'une des conditions d'erreur suivantes, répétez cette procédure en utilisant l'option **Forcer la gestion**.

    - Si l'instance de XClarity Administrator a échoué et ne peut pas être récupérée.

      Remarque : Si l'instance de remplacement de XClarity Administrator utilise la même adresse IP que l'instance de XClarity Administrator ayant rencontré une défaillance, vous pouvez gérer à

nouveau le dispositif à l'aide du compte et du mot de passe RECOVERY_ID (le cas échéant) et de l'option **Forcer la gestion**.

– Si l'instance XClarity Administrator de gestion a été mise hors tension avant que la gestion des appareils n'ait été annulée.

– Si l'annulation de la gestion des appareils n'a pas été correctement effectuée.

Attention : Les appareils peuvent être géré par une seule instance XClarity Administrator à la fois. La gestion par plusieurs instances de XClarity Administrator n'est pas prise en charge. Si un appareil est géré par une instance de XClarity Administrator, et que vous souhaitez le gérer avec une autre instance de XClarity Administrator, vous devez d'abord annuler la gestion de l'appareil dans l'instance de XClarity Administrator d'origine, puis la gérer avec la nouvelle instance de XClarity Administrator.

Après avoir terminé

- Reconnaître et gérer d'autres dispositifs.
- Ajoutez les dispositifs récemment gérés dans l'armoire appropriée pour refléter l'environnement physique (voir Gestion des armoires).
- Surveillez l'état et les informations détaillées du matériel (voir Affichage de l'état de commutateurs).
- Surveillez des événements (voir Utilisation des événements).

Remarques sur la gestion des commutateurs

Avant de gérer un commutateur, prenez connaissance des remarques importantes présentées ci-après.

Pour plus d'informations sur les exigences liées aux ports, voir Disponibilité de port dans la documentation en ligne de Lenovo XClarity Administrator.

Les appareils RackSwitch peuvent être gérés via un port de gestion ou l'un des ports de données. les appareils Rackswitch exécutant CNOS peuvent être gérés uniquement sur des interfaces appartenant au VRF de « gestion » ou « default ».

Remarque : La gestion des appareils RackSwitch à l'aide d'une adresse de liaison locale IPv6 via un port de données ou de gestion n'est pas prise en charge.

Événements XClarity et configuration d'alerte SNMP

Lorsqu'un appareil RackSwitch exécutant ENOS (toute version) est géré ; la source d'alerte SNMP est définie sur l'interface qui comporte l'adresse IP utilisée pour la gestion.

Lorsqu'un appareil RackSwitch exécutant CNOS v10.8.1 ou ultérieur est géré, la source d'alerte SNMP VRF est vérifiée et modifiée pour correspondre au port qui est utilisé pour la gestion.

Pour les appareils RackSwitch exécutant une version CNOS antérieure à la version 10.8.1, XClarity Administrator requiert que la source d'alerte SNMP soit le VRF connecté au port qui est utilisé pour la gestion. La valeur par défaut « all » permet d'utiliser les ports de gestion ou de données. Si la configuration de commutateur n'utilise pas la valeur par défaut, elle doit être modifiée afin de correspondre au port qui est utilisé pour la gestion.

- Si le port de gestion est utilisée pour la gestion, définissez l'alerte SNMP VRF sur « all » ou « management. »
- Si l'un des ports de données est utilisé pour la gestion, définissez l'alerte SNMP VRF sur « all » ou « default. »

Commutateurs RackSwitch exécutant CNOS

HTTPS doit être activé pour la gestion et SLP doit être activé pour la reconnaissance.

Remarque : HTTPS est activé par défaut sur CNOS. Si vous avez modifié la configuration par défaut de restApi (à l'aide de la commande `feature restApi http`), vous pouvez revenir à HTTPS à l'aide de la commande `feature restApi`. Pour vérifier l'état en cours, utilisez la commande `display restApi server`. La sortie indique l'état actuel. Si le numéro de port est suivi de « (HTTP) », cela signifie que HTTPS est *désactivé*. Sinon, le port doit être 443.

Lorsque la gestion d'un appareil RackSwitch est annulée, XClarity Administrator peut ne pas restaurer l'option « prefer » sur la valeur antérieure de l'appareil avant qu'il ne soit géré selon la version de microprogramme CNOS.

Commutateurs RackSwitch exécutant ENOS

- Si les commutateurs RackSwitch ne figurent pas sur le même réseau que XClarity Administrator, le réseau concerné doit être configuré pour autoriser le trafic UPD entrant via les ports 161 et 162 de sorte que XClarity Administrator puisse recevoir des événements et gérer ces appareils.
- SSH doit être activé pour la gestion et SLP doit être activé pour la reconnaissance. HTTPS est facultatif. Toutefois, il doit être activé pour lancer l'interface Web du commutateur
- Selon la version de microprogramme du commutateur RackSwitch, vous serez peut-être amené à activer manuellement la transmission SLP multidiffusion et SSH sur chaque commutateur RackSwitch à l'aide des commandes suivantes pour permettre la reconnaissance et la gestion du commutateur par XClarity Administrator. Pour plus d'informations, voir les Commutateurs d'armoire dans la documentation en ligne System x.
  - `ip slp enable`
  - `ssh enable`
- Lorsqu'un commutateur RackSwitch est géré, XClarity Administrator modifie les paramètres de configuration suivants. La modification de ces paramètres sur un commutateur géré peut interrompre la connectivité et empêcher les actions de gestion suivantes de s'exécuter correctement. Lorsque la gestion d'un commutateur RackSwitch est annulée, les paramètres de configuration sont restaurés aux valeurs d'origine (avant la gestion).
  - snmp-server access 32
  - snmp-server group 16
  - snmp-server notify 16
  - snmp-server target-parameters 16
  - snmp-server target-address 16
  - snmp-server trap-source <*IP interface*>
  - snmp-server user 16
  - snmp-server vesrion <*v3only or v1v2v3*>
  - ntp enable
  - ntp primary-server <*hostname or IP address*> MGT
  - ntp secondary-server <*hostname or IP address*> MGT
  - ntp interval 1500
  - ntp offset 500
  - access https enable

  Vous pouvez utiliser XClarity Administrator pour modifier les paramètres de configuration suivants en modifiant les informations de contact de support, le nom ou les propriétés d'emplacement du commutateur. L'emplacement est modifié lors de l'ajout du commutateur à une armoire.
  - hostname "<*device_name*>"
  - snmp-server location "Location:<*location*>,Room:<*room*>,Rack:<*rack*>,LRU:<*lru*>"
  - snmp-server contact "<*contact_name*>"

Affichage de l'état de commutateurs

Vous pouvez afficher l'état de tous les commutateurs gérés par Lenovo XClarity Administrator.

En savoir plus :

- XClarity Administrator : Inventaire
- XClarity Administrator : Surveillance

À propos de cette tâche

Les icônes d'état suivantes sont utilisées pour indiquer l'état de santé global de l'appareil. Si les certificats ne correspondent pas, la mention « (Non sécurisé) » est ajoutée à l'état de chaque appareil concerné, par exemple Avertissement (Non sécurisé). En cas de problème de connectivité ou si une connexion à l'appareil n'est pas sécurisée, la mention « (Connectivité) » est ajoutée à l'état de chaque appareil concerné, par exemple Avertissement (Connectivité).

- ( ) Critique
  - La valeur signalée par un ou plusieurs des détecteurs de température se situe dans la plage de défaillance.
  - Les modules ventilateur ou les ventilateurs ne fonctionnent pas correctement, comme décrit ci-dessous :
    - RackSwitch G8124-E : Un ou plusieurs ventilateurs fonctionnent à une vitesse inférieure ou égale à 100 tr/min.
    - RackSwitch G8052 : Moins de trois modules ventilateur présentent un état satisfaisant. Si les ventilateurs de ce module fonctionnent à une vitesse supérieure à 500 tr/min, l'état de ce module ventilateur est considéré comme satisfaisant.
    - RackSwitch G8264, G8264CS, G8332, G8272 : Moins de quatre modules ventilateur présentent un état satisfaisant. Si les ventilateurs de ce module fonctionnent à une vitesse supérieure à 500 tr/min, l'état de ce module ventilateur est considéré comme satisfaisant.
    - RackSwitch G8296 : Moins de trois ventilateurs présentent un état satisfaisant. Si les ventilateurs de ce module fonctionnent à une vitesse supérieure à 480 tr/min, l'état de ce module ventilateur est considéré comme satisfaisant.
    - RackSwitch G7028, G7052 : Moins de trois modules ventilateur présentent un état satisfaisant. Si les ventilateurs de ce module fonctionnent à une vitesse supérieure à 500 tr/min, l'état de ce module ventilateur est considéré comme satisfaisant.
  - Un bloc d'alimentation est désactivé.
- ( ) Avertissement
  - La valeur signalée par un ou plusieurs des détecteurs de température se situe dans la plage d'avertissement.
  - Une image mémoire d'alerte existe dans le module d'alimentation flash.
- ( ) En attente
- ( ) Informations
- ( ) Normal
  - Les valeurs signalées par tous les détecteurs de température se situent dans la plage normale.
  - Tous les modules ventilateur ou ventilateurs fonctionnent correctement.
  - Les deux blocs d'alimentation sont activés.
  - Aucune image mémoire d'alerte n'est présente dans le module d'alimentation flash.
- ( ) Hors ligne
- ( ) Inconnu

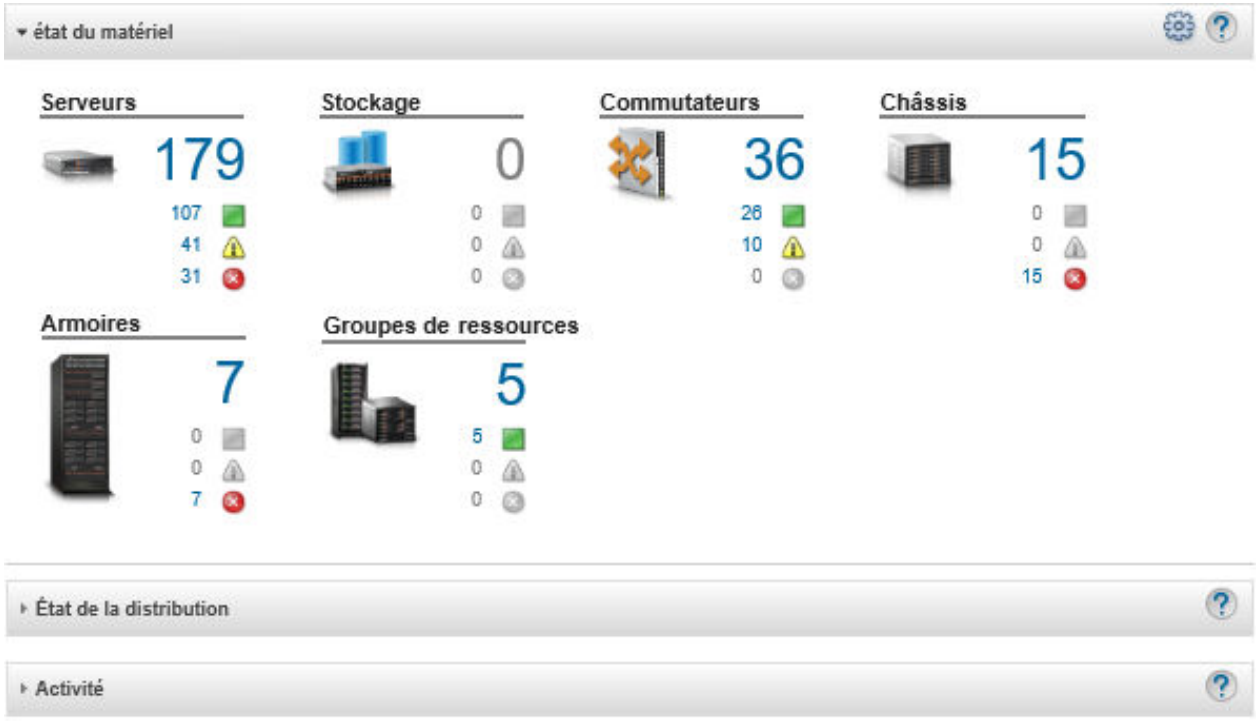
Un appareil peut se trouver dans l'un des états d'alimentation suivants :

- En fonction
- Hors fonction
- Arrêter
- veille
- Mettre en veille prolongée
- Unknown

Procédure

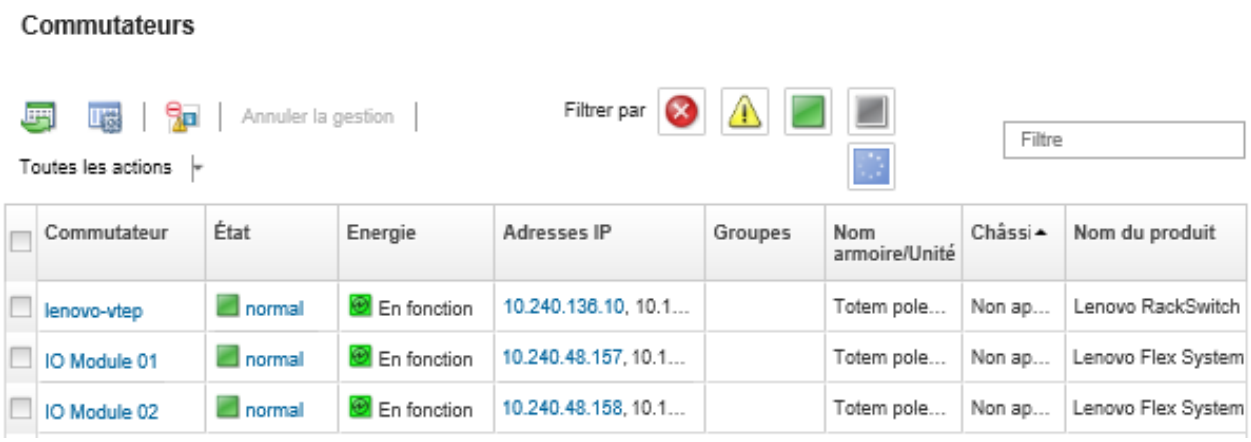
Pour afficher l'état d'commutateur géré, exécutez l'une ou plusieurs des actions suivantes.

- Dans la barre de menus de XClarity Administrator, cliquez sur **Tableau de bord**. La page Tableau de bord affiche la présentation et l'état de tous les commutateurs gérés et d'autres ressources.



- Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Commutateurs**. La page Commutateurs qui s'affiche présente une vue tabulaire de tous les commutateurs gérés.

  Vous pouvez trier les colonnes du tableau afin de faciliter la recherche des commutateurs que vous souhaitez gérer. En outre, saisissez du texte (par exemple, un nom ou une adresse IP) dans la zone **Filtre** et cliquez sur les icônes d'état pour afficher uniquement les commutateurs qui répondent aux critères sélectionnés.



Depuis cette page, vous pouvez effectuer les actions suivantes :

- Afficher des informations détaillées relatives au commutateur (voir Affichage des détails d'un commutateur).
- Afficher un commutateur Flex dans la vue graphique Armoire ou Châssis en cliquant sur **Toutes les actions → Vues → Afficher dans la vue Armoire** ou sur **Toutes les actions → Vues → Afficher dans la vue Châssis**.
- Afficher un commutateur RackSwitch dans la vue graphique Armoire en cliquant sur **Toutes les actions → Vues → Afficher dans la vue Armoire**.
- Lancer l'interface Web du contrôleur de gestion pour le commutateur en cliquant sur le lien **Adresse IP** (voir Lancement de l'interface du contrôleur de gestion pour un commutateur).
- Lancer la console SSH du commutateur (voir Lancement d'une session SSH à distance pour un commutateur).
- Mettre le commutateur sous tension et hors tension (voir Mise sous tension et hors tension d'un commutateur).
- (Commutateurs RackSwitch uniquement) Modifier des informations système en sélectionnant un commutateur et en cliquant sur **Toutes les actions → Inventaire → Éditer les propriétés**.
- Actualiser l'inventaire en sélectionnant un serveur et en cliquant sur **Toutes les actions → Inventaire → Actualiser l'inventaire**.
- Exporter des informations détaillées relatives à un ou plusieurs commutateurs vers un seul fichier CSV en sélectionnant les commutateurs, puis en cliquant sur **Toutes les actions → Inventaire → Exporter l'inventaire** (voir Exclusion d'événements).

  Remarque : Vous pouvez exporter les données d'inventaire pour un maximum de 60 dispositifs en même temps.

  Conseil : Lors de l'importation d'un fichier CSV dans Microsoft Excel, Excel traite les valeurs textuelles contenant uniquement des numéros sous la forme de valeurs numériques (par exemple, pour des UUID). Formatez chaque cellule sous forme de texte pour résoudre cette erreur.
- Exclure les événements qui ne vous intéressent pas de toutes les pages sur lesquelles des événements sont affichés en cliquant sur l'icône **Exclure des événements** ( ) (voir Exclusion d'événements).
- (Commutateurs Flex uniquement) Corriger les problèmes pouvant survenir entre le certificat de sécurité de XClarity Administrator et le certificat de sécurité du CMM dans le châssis dans lequel le commutateur est installé en sélectionnant un commutateur et en cliquant sur **Toutes les actions → Sécurité → Résoudre les certificats non sécurisés** (voir Résolution d'un certificat du serveur non sécurisé).

– Ajouter ou retirer un commutateur d'un groupe de ressources statique en cliquant sur **Toutes les actions → Groupes → Ajouter au groupe** ou sur **Toutes les actions → Groupes → Retirer du groupe**.

Affichage des détails d'un commutateur

Vous pouvez afficher des informations détaillées sur un commutateur géré à partir de Lenovo XClarity Administrator, y compris les niveaux de microprogramme et les adresses IP.

En savoir plus :

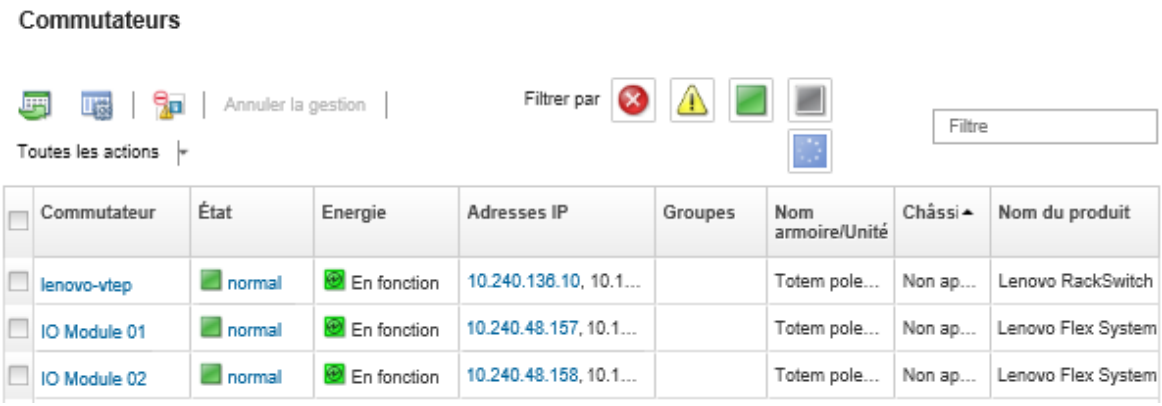
- XClarity Administrator : Inventaire
- XClarity Administrator : Surveillance

Procédure

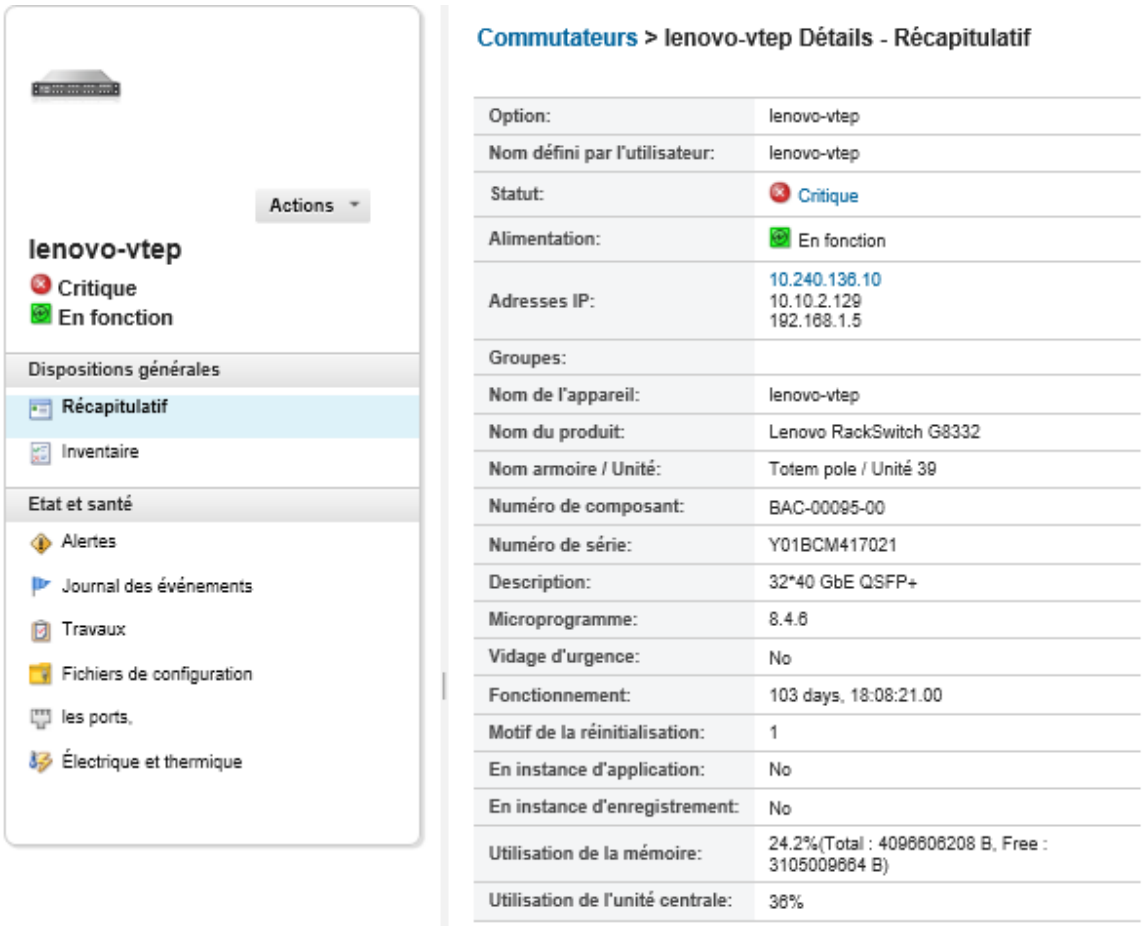
Pour afficher les détails d'un commutateur spécifique géré par XClarity Administrator, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Commutateurs**. La page Commutateurs qui s'affiche présente une vue tabulaire de tous les commutateurs installés dans un châssis géré.

Vous pouvez trier les colonnes du tableau afin de faciliter la recherche des commutateurs que vous souhaitez gérer. En outre, vous pouvez saisir un texte (par exemple, un nom ou une adresse IP) dans la zone **Filtre** pour filtrer davantage l'affichage des commutateurs.



Etape 2. Cliquez sur le commutateur dans la colonne **Commutateurs**. La page Récapitulatif s'affiche et présente les propriétés, ainsi que la liste des composants installés dans ce commutateur.



Etape 3. Exécutez l'une ou plusieurs des étapes suivantes pour afficher des détails d'inventaire :

Remarque : Il se peut que certaines informations détaillées ne soient pas disponibles pour tous les commutateurs.

- Cliquez sur **Récapitulatif** pour afficher un récapitulatif du commutateur, y compris les informations système et le microprogramme (voir Affichage de l'état des dispositifs de stockage).
- Cliquez sur **Détails d'inventaire** pour afficher des détails sur les composants de commutateur, y compris :
  - Les niveaux de microprogramme du commutateur
  - Les détails du réseau de contrôleur de gestion, tels que le nom d'hôte, l'adresse IPv4, l'adresse IPv6 et les adresses MAC
  - Les détails des actifs du commutateur
- Cliquez sur **Connectivité d'E-S** pour afficher les détails de connectivité relatifs au commutateur sélectionné et les cartes réseau associées qu'il contient.
- Cliquez sur **Alertes** pour afficher les alertes de la liste d'alertes qui sont liées au commutateur (voir Utilisation des alertes).
- Cliquez sur **Journal des événements** pour afficher les événements du journal des événements qui sont liés au commutateur (voir Utilisation des événements).
- Cliquez sur **Fichiers de configuration** pour sauvegarder et restaurer la configuration de commutateur (voir Sauvegarde et restauration des données de configuration de commutateur).

- Cliquez sur **Historique de déploiement** pour afficher des informations sur les modèles de configuration de commutateur qui ont été déployés dans le commutateur (voir Afficher l'historique de déploiement de la configuration de commutateur).
- Cliquez sur **Travaux** pour afficher les fichiers de données de configuration du commutateur (voir Surveillance des travaux).
- Cliquez sur **Ports** pour afficher l'état et la configuration de tous les ports dans un commutateur géré, et pour activer ou désactiver les ports du commutateur.

  Remarque : Pour les commutateurs Flex, cliquez sur l'icône **Actualiser** () afin de collecter les données de port actuelles. La collecte de données peut prendre plusieurs minutes.
- Cliquez sur **Light Path** pour afficher l'état actuel de chaque voyant sur le commutateur.
- Cliquez sur **Électrique et thermique** pour afficher des informations sur la température, les blocs d'alimentation et les ventilateurs.

  Astuce : Pour collecter les dernières données électriques et thermiques, utilisez le bouton Actualiser de votre navigateur Web. La collecte de données peut prendre plusieurs minutes.

Après avoir terminé

En plus d'afficher le récapitulatif et des informations détaillées relatives à un commutateur, vous pouvez effectuer les actions suivantes :

- Afficher un commutateur Flex dans la vue graphique Armoire ou Châssis en cliquant sur **Actions → Vues → Afficher dans la vue Armoire** ou sur **Actions → Vues → Afficher dans la vue Châssis**.
- Afficher un commutateur RackSwitch dans la vue graphique Armoire en cliquant sur **Actions → Vues → Afficher dans la vue Armoire**.
- Lancer l'interface Web du contrôleur de gestion pour le commutateur en cliquant sur le lien **Adresse IP** (voir Lancement de l'interface du contrôleur de gestion pour un commutateur).
- Lancer la console SSH du commutateur (voir Lancement d'une session SSH à distance pour un commutateur).
- Mettre le commutateur sous tension et hors tension (voir Mise sous tension et hors tension d'un commutateur).
- (Commutateurs RackSwitch uniquement) Modifier des informations système en sélectionnant un commutateur, puis en cliquant sur **Éditer les propriétés**.
- Exporter des informations détaillées sur le commutateur dans un fichier CSV en cliquant sur **Actions → Inventaire → Exporter l'inventaire**.

  Remarques :

  – Pour plus d'informations sur les données d'inventaire dans le fichier CSV, voirGET /switches/<*UUID_list*> REST API dans la documentation en ligne de XClarity Administrator.

  – Lors de l'importation d'un fichier CSV dans Microsoft Excel, Excel traite les valeurs textuelles contenant uniquement des numéros sous la forme de valeurs numériques (par exemple, pour des UUID). Formatez chaque cellule sous forme de texte pour résoudre cette erreur.
- Exclure les événements qui ne vous intéressent pas de toutes les pages sur lesquelles des événements sont affichés en cliquant sur **Actions → Réinitialisation de service → Exclure des événements** (voir Exclusion d'événements).
- Corriger les problèmes pouvant survenir entre le certificat de sécurité de XClarity Administrator et le certificat de sécurité du RackSwitch ou du CMM dans le châssis dans lequel le commutateur Flex System est installé en sélectionnant un commutateur et en cliquant sur **Actions → Sécurité → Résoudre les certificats non sécurisés** (voir Résolution d'un certificat du serveur non sécurisé).

Mise sous tension et hors tension d'un commutateur

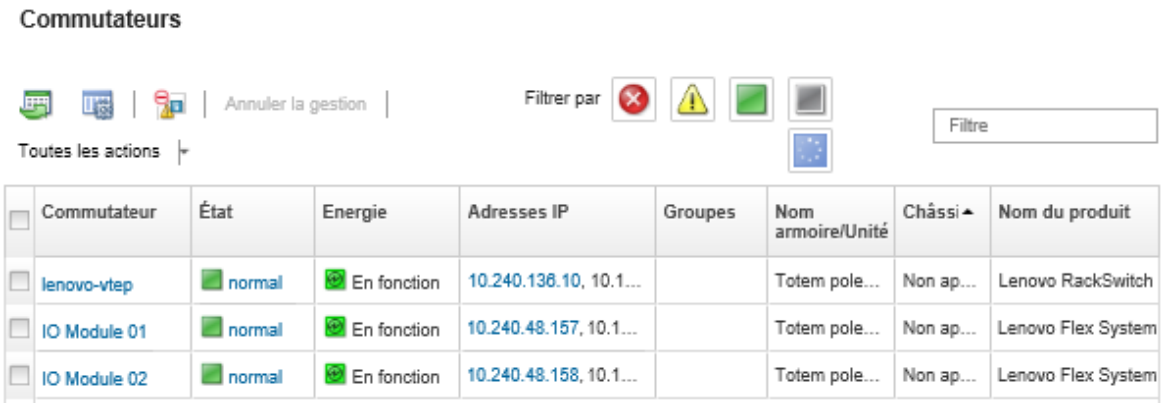
Vous pouvez mettre sous tension, mettre hors tension et redémarrer un commutateur Flex System ou RackSwitch à partir de Lenovo XClarity Administrator.

Procédure

Procédez comme suit pour mettre sous tension ou hors tension un commutateur géré.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Commutateurs**. La page Commutateurs qui s'affiche présente une vue tabulaire de tous les commutateurs installés dans un châssis géré.

Vous pouvez trier les colonnes du tableau afin de faciliter la recherche des commutateurs que vous souhaitez gérer. En outre, vous pouvez saisir un texte (par exemple, un nom ou une adresse IP) dans la zone **Filtre** pour filtrer davantage l'affichage des commutateurs.



Etape 2. Sélectionnez le commutateur à mettre sous tension ou hors tension ou à redémarrer.

Etape 3. Cliquez sur **Toutes les actions**, puis sur l'une des actions d'alimentation suivantes :
- **Mettre sous tension** (commutateurs Flex System uniquement)
- **Mettre hors tension** (commutateurs Flex System uniquement)
- **Redémarrer**. Le commutateur est redémarré une fois que toutes les opérations en cours d'exécution sont terminées. Les opérations qui sont démarrées pendant le redémarrage du commutateur sont rejetées.

Activation et désactivation des ports de commutateur

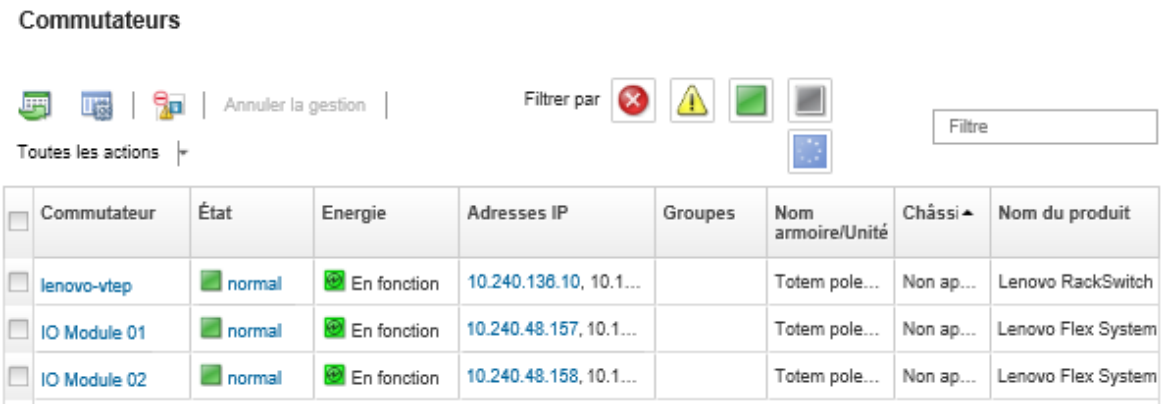
Vous pouvez activer ou désactiver des ports spécifiques sur un commutateur RackSwitch ou Flex System.

Procédure

Pour activer ou désactiver des ports de commutateur, procédez comme suit.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Matériel → Commutateurs**. La page Commutateurs qui s'affiche présente une vue tabulaire de tous les commutateurs installés dans un châssis géré.

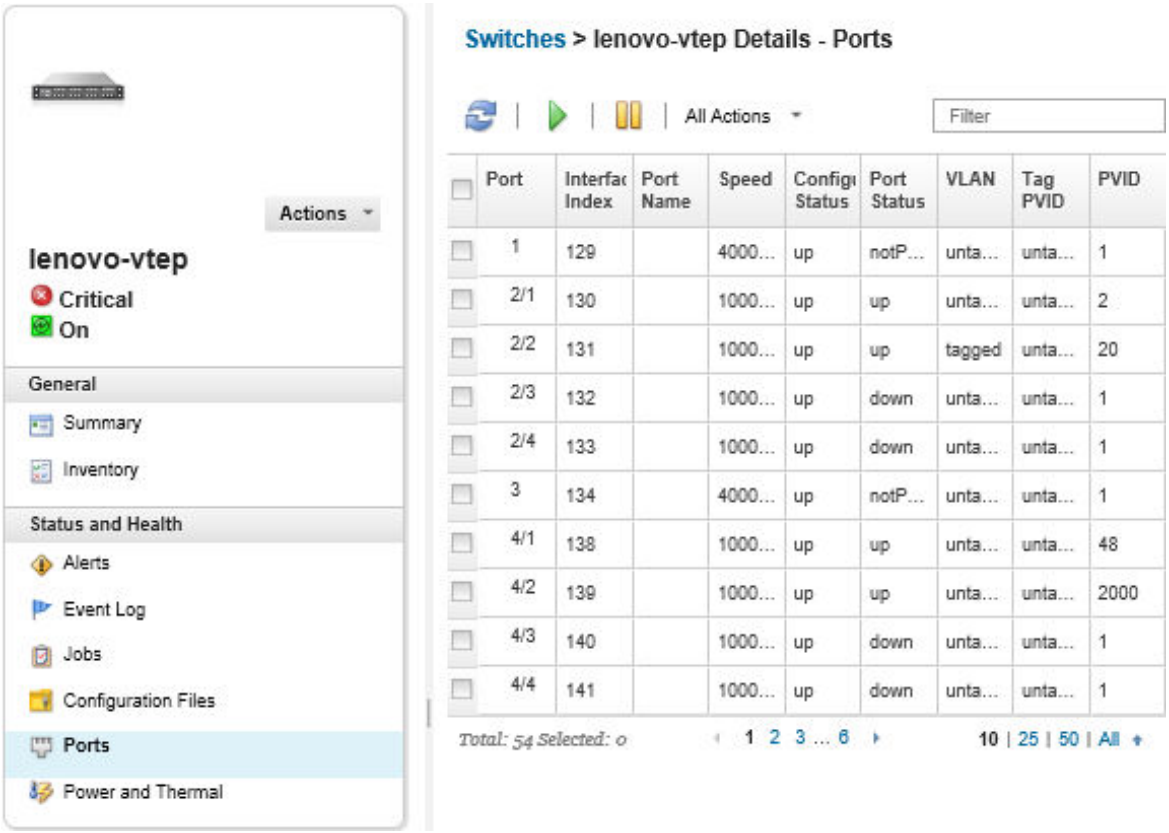
Vous pouvez trier les colonnes du tableau afin de faciliter la recherche des commutateurs que vous souhaitez gérer. En outre, vous pouvez saisir un texte (par exemple, un nom ou une adresse IP) dans la zone **Filtre** pour filtrer davantage l'affichage des commutateurs.



Etape 2. Cliquez sur le commutateur dans la colonne **Commutateurs**. La page Récapitulatif s'affiche et présente les propriétés, ainsi que la liste des composants installés dans ce commutateur.

Etape 3. Cliquez sur **Ports** dans le volet de navigation gauche pour afficher l'état et la configuration de tous les ports dans le commutateur :

Remarque : Pour les commutateurs Flex, cliquez sur l'icône **Actualiser** ( ) afin de collecter les données de port actuelles. La collecte de données peut prendre plusieurs minutes



Etape 4. Sélectionnez le port, puis cliquez sur l'icône **Activer** ( ) ou sur l'icône **Désactiver** ( ).

Sauvegarde et restauration des données de configuration de commutateur

Vous pouvez utiliser Lenovo XClarity Administrator pour sauvegarder et restaurer les données de configuration de vos commutateurs RackSwitch et Flex System. Vous pouvez également exporter des fichiers de configuration de commutateur sur votre système local et importer des fichiers de configuration dans XClarity Administrator.

Sauvegarde des données de configuration de commutateur

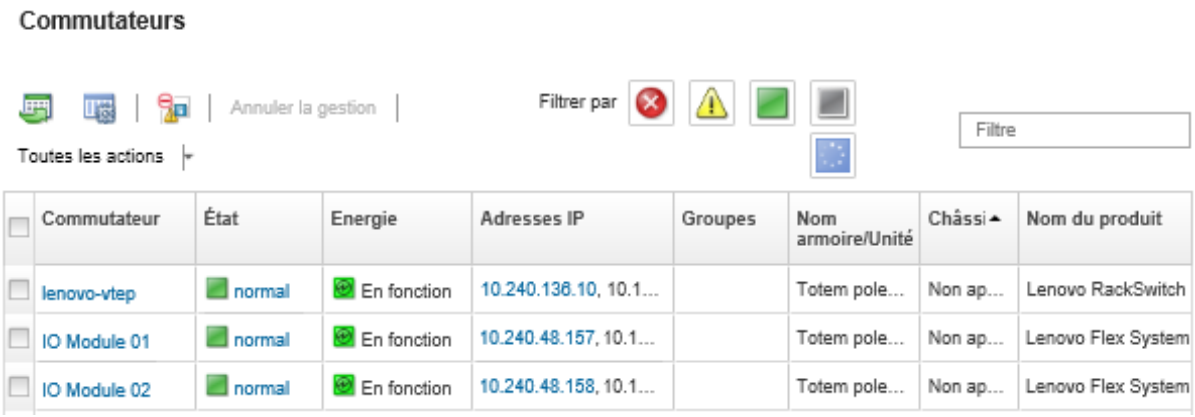
Vous pouvez sauvegarder les données de configuration pour un commutateur RackSwitch ou Flex System. Lorsque vous sauvegardez un commutateur, les données de configuration sont importées dans Lenovo XClarity Administrator depuis le commutateur cible sous forme de fichier de données de configuration de commutateur.

Procédure

Pour sauvegarder les données de configuration d'un commutateur géré, procédez comme suit.

- Pour un seul commutateur :
  1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Commutateurs**. La page Commutateurs qui s'affiche présente une vue tabulaire de tous les commutateurs installés dans un châssis géré.

     Vous pouvez trier les colonnes du tableau afin de faciliter la recherche des commutateurs que vous souhaitez gérer. En outre, vous pouvez saisir un texte (par exemple, un nom ou une adresse IP) dans la zone **Filtre** pour filtrer davantage l'affichage des commutateurs.



  2. Cliquez sur le commutateur dans la colonne **Commutateurs**. La page Récapitulatif s'affiche et présente les propriétés, ainsi que la liste des composants installés dans ce commutateur.
  3. Cliquez sur **Configuration** pour afficher les fichiers de configuration du commutateur.
  4. Cliquez sur l'icône **Sauvegarder les données de configuration** ( ) pour sauvegarder la configuration du commutateur.
  5. (Facultatif) Spécifiez un nom pour le fichier de configuration de commutateur.

     Pour les dispositifs CNOS, le nom de fichier peut contenir des caractères alphanumériques et les caractères spéciaux suivants : soulignement (_), tiret (-) et point (.). Pour les commutateurs ENOS, le nom de fichier peut contenir des caractères alphanumériques et tous les caractères spéciaux.

     Si un nom de fichier n'est pas spécifié, le nom par défaut suivant est utilisé : « *<nom_commutateur>_<adresse_IP>_<horodatage>*.cfg. »

6. (Facultatif) Ajoutez un commentaire décrivant la sauvegarde.
7. Cliquez sur **Sauvegarder** pour sauvegarder les données de configuration de commutateur immédiatement ou sur **Planning** afin de planifier cette sauvegarde à une période ultérieure.

   Si vous avez choisi planifier une sauvegarde, vous pouvez sélectionner **Remplacer** pour sauvegarder les données de configuration du commutateur dans le même fichier à l'exécution de chaque tâche, en remplaçant son contenu. Si vous choisissez de ne pas remplacer le fichier, les noms des fichiers de sauvegarde suivants sont ajoutés par un numéro unique (par exemple, MyBackup_33.cfg).

   Remarque : Lors de la planification d'une sauvegarde, vous ne peut pas choisir les noms de fichier dynamique ou des commentaires pour chaque tâche planifiée.

- Pour plusieurs commutateurs :
  1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Commutateurs**. La page Commutateurs qui s'affiche présente une vue tabulaire de tous les commutateurs installés dans un châssis géré.
  2. Sélectionnez un ou plusieurs commutateurs.
  3. Cliquez sur **Toutes les actions → Configuration → Fichier de configuration de sauvegarde**.
  4. (Facultatif) Spécifiez un nom pour le fichier de configuration de commutateur.

     Pour les dispositifs CNOS, le nom de fichier peut contenir des caractères alphanumériques et les caractères spéciaux suivants : soulignement (_), tiret (-) et point (.). Pour les commutateurs ENOS, le nom de fichier peut contenir des caractères alphanumériques et tous les caractères spéciaux.

     Si un nom de fichier n'est pas spécifié, le nom par défaut suivant est utilisé : « <*nom_commutateur*>_<*adresse_IP*>_<*horodatage*>.cfg. »
  5. (Facultatif) Ajoutez un commentaire décrivant la sauvegarde.
  6. Cliquez sur **Sauvegarder** pour sauvegarder les données de configuration de commutateur immédiatement ou sur **Planning** afin de planifier cette sauvegarde à une période ultérieure.

     Si vous avez choisi planifier une sauvegarde, vous pouvez sélectionner **Remplacer** pour sauvegarder les données de configuration du commutateur dans le même fichier à l'exécution de chaque tâche, en remplaçant son contenu. Si vous choisissez de ne pas remplacer le fichier, les noms des fichiers de sauvegarde suivants sont ajoutés par un numéro unique (par exemple, MyBackup_33.cfg).

     Remarque : Lors de la planification d'une sauvegarde, vous ne peut pas choisir les noms de fichier dynamique ou des commentaires pour chaque tâche planifiée.

Après avoir terminé

Lorsque le processus de sauvegarde est terminé, le fichier configuration de commutateur est ajouté à l'onglet **Fichiers de configuration** de la page des détails du commutateur.

Depuis cette page, vous pouvez aussi exécuter les actions suivantes sur le fichier de configuration de commutateur sélectionné :

- Restaurer la configuration de commutateur en sélectionnant le fichier de configuration de commutateur et en cliquant sur l'icône **Restaurer les données de configuration** ( ).
- Supprimer les fichiers de configuration de commutateur dans XClarity Administrator en cliquant sur l'icône **Supprimer** ( ).
- Exporter des fichiers de configuration de commutateur dans votre système local en sélectionnant les fichiers et en cliquant sur l'icône **Exporter le fichier de configuration** ( ).

- Importer les fichiers de configuration de commutateur dans XClarity Administrator en cliquant sur l'icône **Importer le fichier de configuration** ( ).

Restauration des données de configuration de commutateur

Vous pouvez utiliser des données qui ont été sauvegardées ou importées dans Lenovo XClarity Administrator pour un commutateur RackSwitch ou Flex System. Le fichier de configuration de commutateur est téléchargé depuis XClarity Administrator dans le commutateur cible et la configuration entre immédiatement en vigueur.

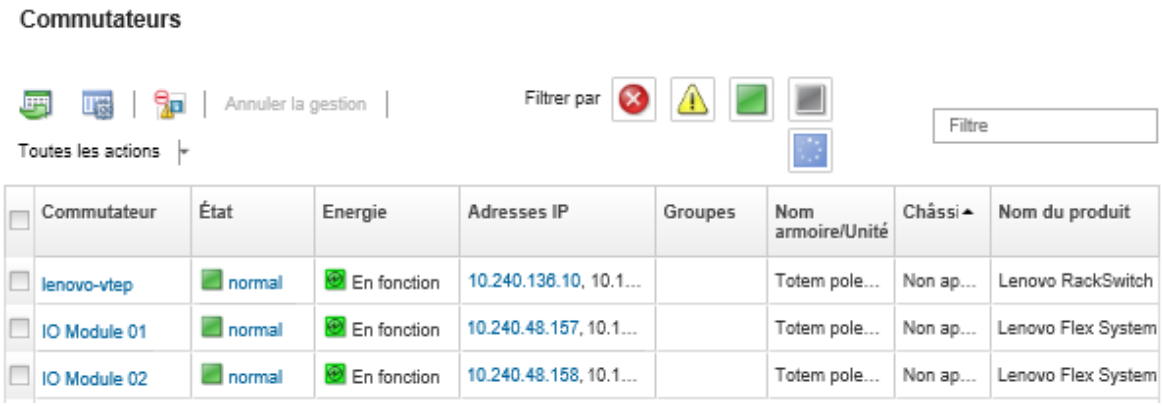
Les fichiers de configuration sont associés avec un commutateur spécifique. Vous pouvez restaurer un fichier de configuration uniquement sur le commutateur auquel il est associé. Vous ne pouvez pas utiliser un fichier de configuration qui a été sauvegardé pour un commutateur ou restaurer la configuration sur un fichier de sauvegarde.

Procédure

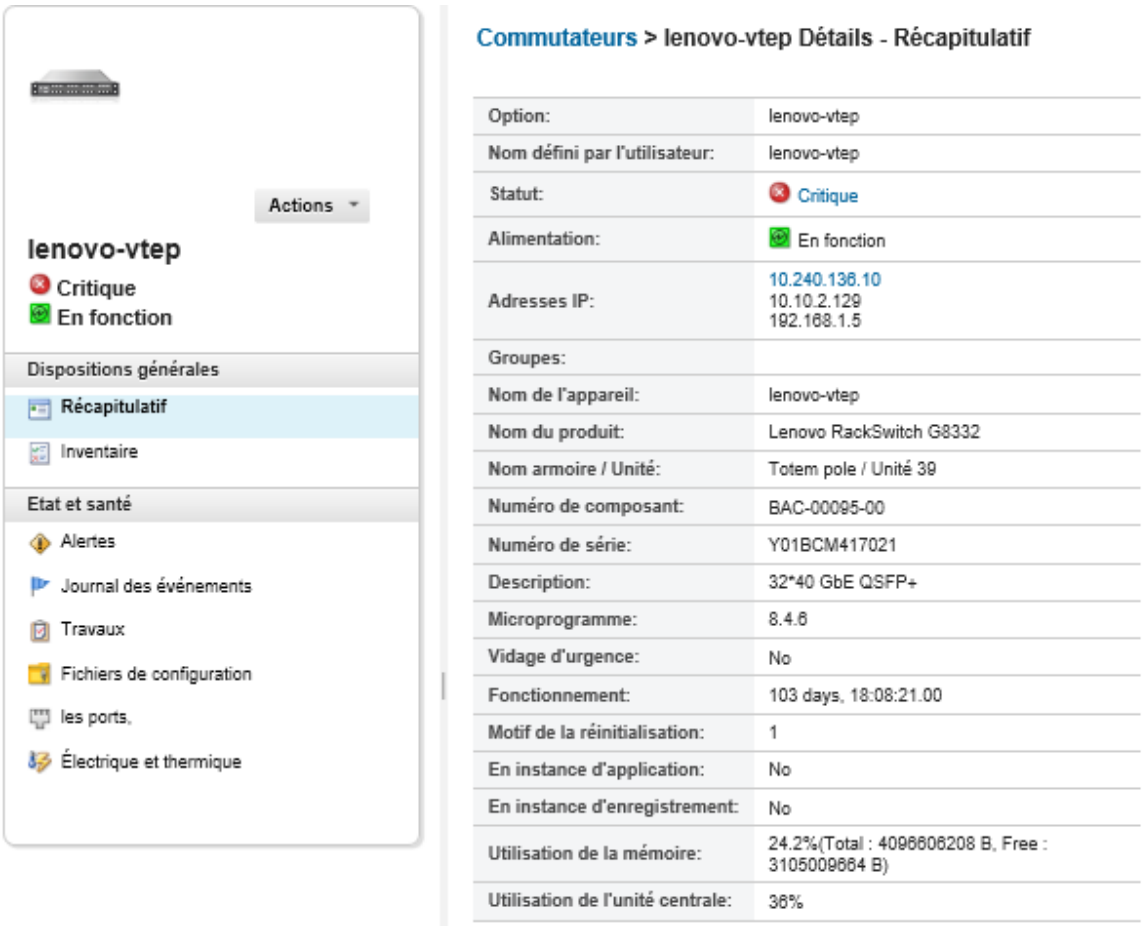
Pour restaurer des données de configuration sur un commutateur géré, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Commutateurs**. La page Commutateurs qui s'affiche présente une vue tabulaire de tous les commutateurs installés dans un châssis géré.

Vous pouvez trier les colonnes du tableau afin de faciliter la recherche des commutateurs que vous souhaitez gérer. En outre, vous pouvez saisir un texte (par exemple, un nom ou une adresse IP) dans la zone **Filtre** pour filtrer davantage l'affichage des commutateurs.



Etape 2. Cliquez sur le commutateur dans la colonne **Commutateurs**. La page Récapitulatif s'affiche et présente les propriétés, ainsi que la liste des composants installés dans ce commutateur.



Etape 3. Cliquez sur **Fichiers de configuration** pour afficher les fichiers de configuration du commutateur.

Etape 4. Sélectionnez le fichier de configuration que vous voulez restaurer sur le commutateur, puis cliquez sur l'icône **Restaurer les données de configuration** ( ). La boîte de dialogue Restaurer s'affiche.

Etape 5. (Commutateurs CNOS uniquement) Choisissez de redémarrer le commutateur après que la restauration soit terminée.

Si vous choisissez de ne pas redémarrer automatiquement le commutateur, vous devez redémarrer manuellement le commutateur CNOS pour activer les données de configuration restaurées. Si vous attendez trop longtemps et qu'une opération de sauvegarde produit (par exemple, si un port est activé ou désactivé), l'opération de restauration est interrompue et les données de configuration en cours d'exécution sont utilisées.

Etape 6. Cliquez sur **Restaurer** pour restaurer les données de configuration sur le commutateur immédiatement, ou cliquez sur **Planning** afin de planifier cette restauration à une période ultérieure.

Remarque : Soyez prudent lors de la planification de travaux de restauration récurrents. Si votre commutateur se réinitialise à une configuration antérieure, consultez la page Travaux planifiés des travaux de restauration planifiée.

Exportation et importation de fichiers de configuration de commutateur

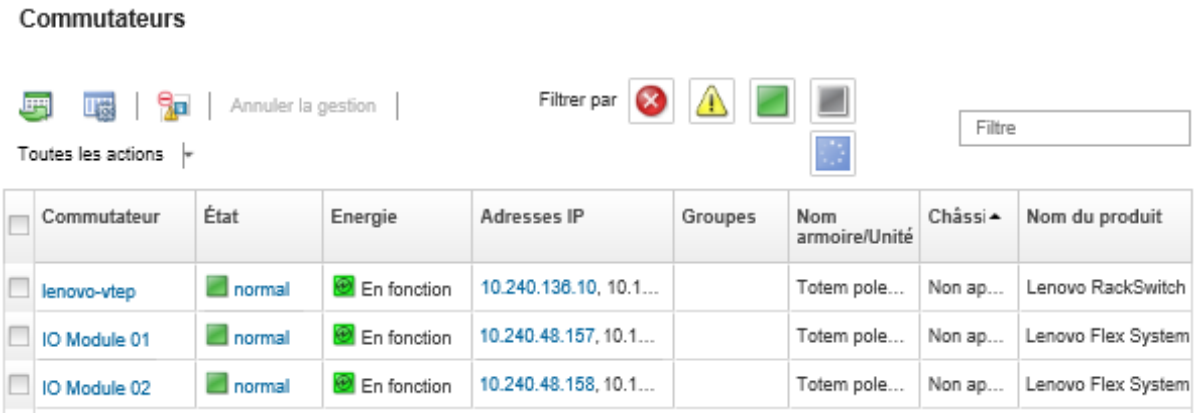
Vous pouvez exporter des fichiers de configuration de commutateur sur votre système local et importer des fichiers de configuration dans Lenovo XClarity Administrator.

Procédure

Pour sauvegarder les données de configuration d'un commutateur géré, procédez comme suit.

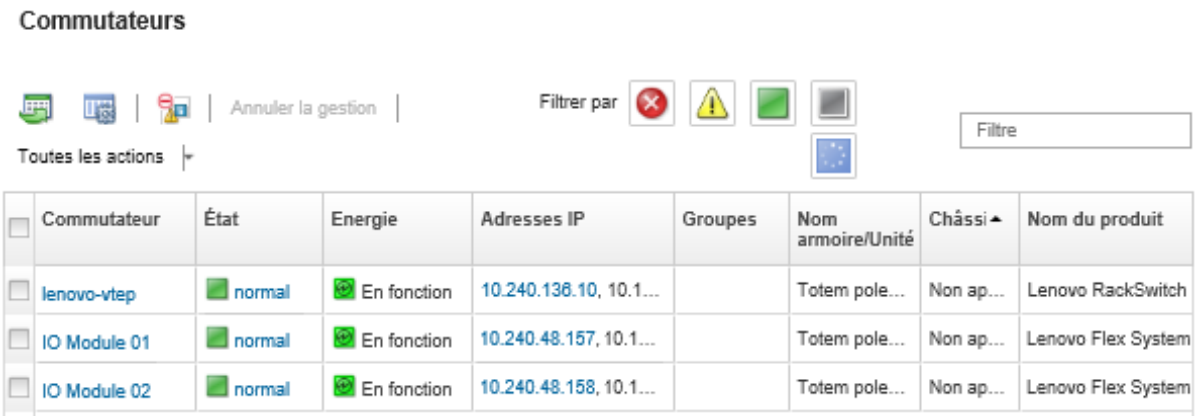
- Exporter des fichiers de configuration de commutateur
  1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Commutateurs**. La page Commutateurs qui s'affiche présente une vue tabulaire de tous les commutateurs installés dans un châssis géré.

     Vous pouvez trier les colonnes du tableau afin de faciliter la recherche des commutateurs que vous souhaitez gérer. En outre, vous pouvez saisir un texte (par exemple, un nom ou une adresse IP) dans la zone **Filtre** pour filtrer davantage l'affichage des commutateurs.



  2. Cliquez sur le commutateur dans la colonne **Commutateurs**. La page Récapitulatif s'affiche et présente les propriétés, ainsi que la liste des composants installés dans ce commutateur.
  3. Cliquez sur **Configuration** pour afficher les fichiers de configuration du commutateur.
  4. Sélectionnez les fichier de configuration de commutateur à exporter.
  5. Cliquez sur l'icône **Exporter le fichier configuration** ( ) pour sauvegarder la configuration du commutateur.
- Importer des fichiers de configuration de commutateur
  1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Commutateurs**. La page Commutateurs qui s'affiche présente une vue tabulaire de tous les commutateurs installés dans un châssis géré.

     Vous pouvez trier les colonnes du tableau afin de faciliter la recherche des commutateurs que vous souhaitez gérer. En outre, vous pouvez saisir un texte (par exemple, un nom ou une adresse IP) dans la zone **Filtre** pour filtrer davantage l'affichage des commutateurs.



2. Cliquez sur le commutateur dans la colonne **Commutateurs**. La page Récapitulatif s'affiche et présente les propriétés, ainsi que la liste des composants installés dans ce commutateur.
3. Cliquez sur **Configuration** pour afficher les fichiers de configuration du commutateur.
4. Cliquez sur l'icône **Importer le fichier configuration** ( ) pour sauvegarder la configuration du commutateur.
5. Entrez le nom du fichier de configuration de commutateur ou cliquez sur **Parcourir** pour rechercher le fichier d'amorçage que vous souhaitez importer.
6. **Facultatif :** Entrez une description pour le fichier de configuration de commutateur.
7. Cliquez sur **Importer**.

   Si vous fermez l'onglet ou la fenêtre de navigateur Web dans lesquels le fichier est téléchargé avant la fin du téléchargement, l'importation échoue.

Lancement de l'interface du contrôleur de gestion pour un commutateur

Vous pouvez lancer l'interface Web du contrôleur de gestion pour un commutateur RackSwitch ou Flex System System exécutant ENOS à partir de Lenovo XClarity Administrator.

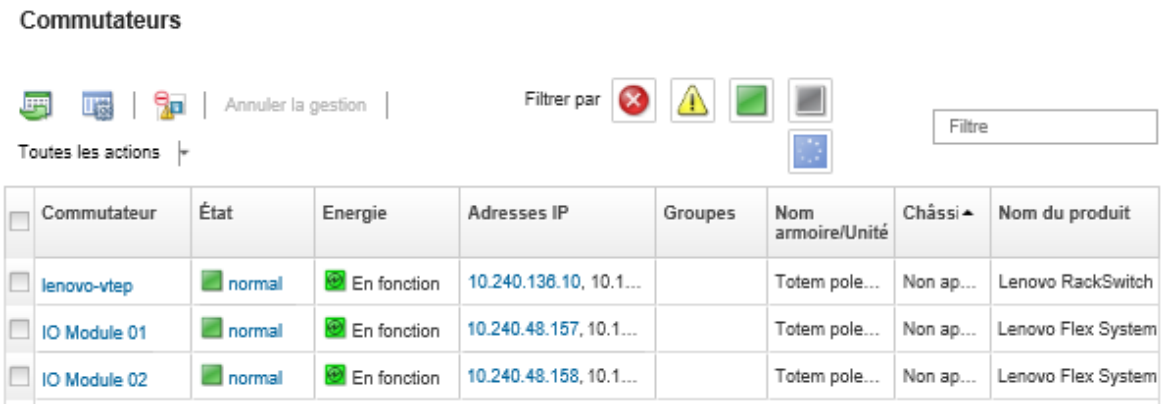
Procédure

Procédez comme suit pour lancer l'interface du contrôleur de gestion pour un commutateur.

Remarque : Le lancement d'une interface Web du contrôleur de gestion à partir de XClarity Administrator à l'aide du navigateur Web Safari n'est pas pris en charge.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Commutateurs**. La page Commutateurs qui s'affiche présente une vue tabulaire de tous les commutateurs installés dans un châssis géré.

Vous pouvez trier les colonnes du tableau afin de faciliter la recherche des commutateurs que vous souhaitez gérer. En outre, vous pouvez saisir un texte (par exemple, un nom ou une adresse IP) dans la zone **Filtre** pour filtrer davantage l'affichage des commutateurs.



Etape 2. Sélectionnez le commutateur et cliquez sur **Toutes les actions → Lancer → Interface Web de gestion**. L'interface Web du contrôleur de gestion pour le commutateur s'affiche.

Astuce : Vous pouvez également lancer l'interface du contrôleur de gestion en cliquant sur le lien Adresse IP dans la colonne **Adresse IP** et sur les pages d'informations récapitulatives et d'informations détaillées du commutateur.

Etape 3. Connectez-vous à l'interface du contrôleur de gestion.

Astuce : Pour les commutateurs Flex, utilisez vos données d'identification utilisateur XClarity Administrator. Pour les commutateurs XClarity Administrator, utilisez les données d'identification du commutateur.

Lancement d'une session SSH à distance pour un commutateur

Vous pouvez lancer une session SSH à distance pour un commutateur RackSwitch ou Flex System géré à partir de Lenovo XClarity Administrator. À partir de la session SSH à distance, vous pouvez utiliser l'interface de ligne de commande pour effectuer des tâches de gestion qui ne sont pas fournies par XClarity Administrator.

Avant de commencer

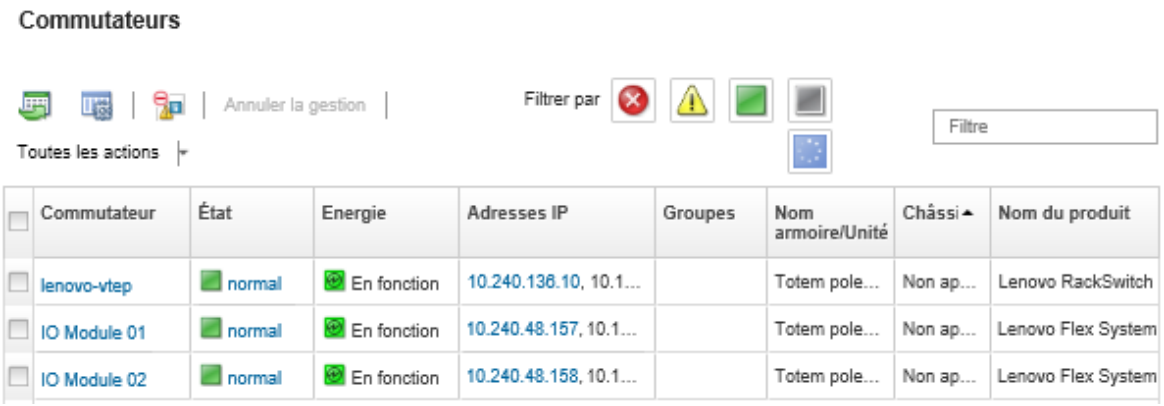
Vérifiez que le commutateur est configuré pour activer SSH. Pour les commutateurs RackSwitch, SSH est activé lorsque le commutateur est géré par XClarity Administrator. Pour les commutateurs Flex, SSH est généralement activé par défaut. Si SSH n'est pas activé, il doit être activé avant que le commutateur soit géré par XClarity Administrator.

Procédure

Procédez comme suit pour lancer une session SSH à distance pour un commutateur géré.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Commutateurs**. La page Commutateurs qui s'affiche présente une vue tabulaire de tous les commutateurs installés dans un châssis géré.

Vous pouvez trier les colonnes du tableau afin de faciliter la recherche des commutateurs que vous souhaitez gérer. En outre, vous pouvez saisir un texte (par exemple, un nom ou une adresse IP) dans la zone **Filtre** pour filtrer davantage l'affichage des commutateurs.



Etape 2. Sélectionnez le commutateur pour lequel vous souhaitez lancer une session SSH.

Etape 3. Cliquez sur **Toutes les actions → Lancer → Console SSH**.

Etape 4. Si nécessaire, connectez-vous au commutateur à l'aide de votre ID utilisateur et de votre mot de passe.

Modification des propriétés système d'un commutateur

Vous pouvez modifier les propriétés système d'un commutateur Flex System ou RackSwitch spécifique.

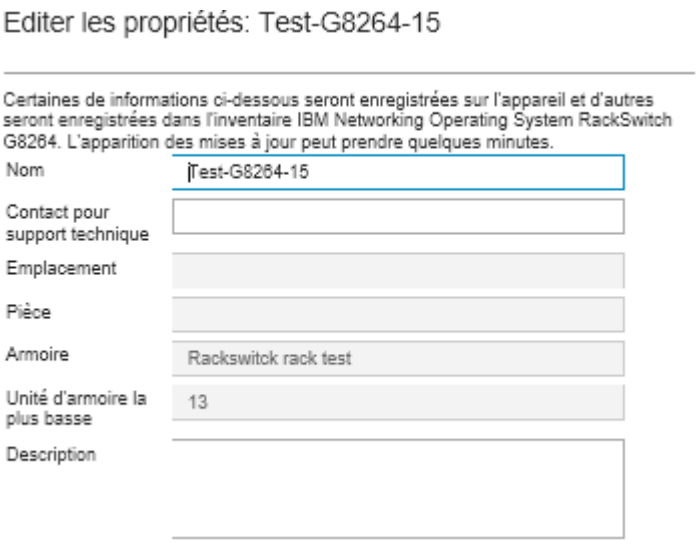
Procédure

Procédez comme suit pour modifier les propriétés système :

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Matériel → Commutateurs** pour afficher la page Commutateurs.

Etape 2. Sélectionnez le commutateur à mettre à jour.

Etape 3. Cliquez sur **Toutes les actions → Inventaire → Éditer les propriétés** pour afficher la boîte de dialogue Éditer.



Etape 4. Modifiez les informations suivantes, si nécessaire.
- Nom du commutateur
- Contact pour support technique
- Description

Remarque : Les propriétés d'emplacement, de pièce, d'armoire et d'unité d'armoire la plus basse sont mises à jour par XClarity Administrator lorsque vous ajoutez ou retirez des appareils dans une armoire dans l'interface Web (voir Gestion des armoires).

Etape 5. Cliquez sur **Enregistrer**.

Remarque : Si vous modifiez ces propriétés, vous devrez peut-être attendre quelques instants avant que les modifications n'apparaissent dans l'interface Web XClarity Administrator.

Résolution de données d'identification expirées ou non valides pour un commutateur

Lorsqu'une des données d'identification stockées expirent ou deviennent inopérantes sur un appareil, le statut de cet appareil apparaît comme « Hors ligne. »

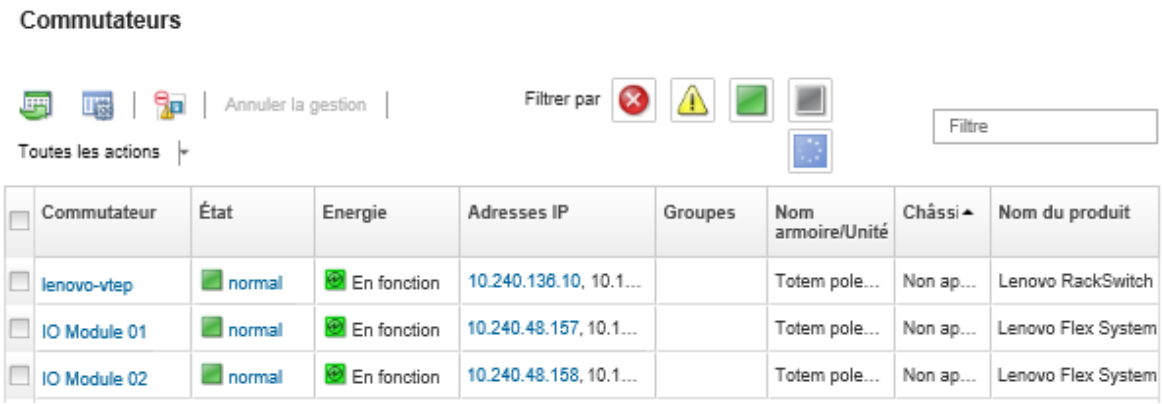
Procédure

Pour résoudre des données d'identification expirées ou non valides pour un commutateur, procédez comme suit.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Matériel → Commutateurs**. La page Commutateurs qui s'affiche présente une vue tabulaire de tous les commutateurs gérés.

Etape 2. Cliquez sur l'en-tête de colonne **Alimentation** pour grouper tous les commutateurs hors ligne en haut de la table.

Vous pouvez trier les colonnes du tableau pour trouver plus facilement le commutateur que vous souhaitez gérer. En outre, vous pouvez entrer du texte (comme un nom de système ou l'adresse IP) dans le champ **Filtre** pour filtrer davantage les commutateurs affichés.



Etape 3. Sélectionnez le commutateur à résoudre.

Etape 4. Cliquez sur **Toutes les actions → Sécurité → Éditer les données d'identification stockées**.

Etape 5. Changez le mot de passe des données d'identification stockées ou sélectionnez d'autres données d'identification stockées à utiliser pour cet appareil géré.

Remarque : Si vous avez géré plusieurs appareils à l'aide des mêmes données d'identification stockées et si vous modifiez le mot de passe des données d'identification stockées, ce changement de mot de passe affecte tous les dispositifs qui utilisent actuellement les données d'identification stockées.

Récupération de la gestion avec un commutateur après une défaillance du serveur de gestion

Vous pouvez récupérer la gestion d'un commutateur dont l'annulation de la gestion n'a pas été effectuée proprement (par exemple, en raison de problèmes de connectivité lors de l'annulation de la gestion ou d'une défaillance du Lenovo XClarity Administrator de gestion).

Procédure

- Gérez à nouveau le commutateur à l'aide de l'option **Forcer la gestion** (voir Gestion des commutateurs).
- Pour supprimer définitivement une configuration spécifique de XClarity Administrator sur un commutateur dont l'annulation de la gestion n'a pas été effectuée proprement et qui ne sera pas géré à nouveau, procédez comme suit.
  - Gérez le commutateur à nouveau à l'aide de l'option **Forcer la gestion** (voir Gestion des commutateurs), puis annulez la gestion du commutateur afin de nettoyer la configuration (voir Annulation de la gestion d'un commutateur).
  - (ENOS) Connectez-vous au commutateur via le port de console de commutateur ou une session SSH ou Telnet et exécutez les commandes de configuration suivantes dans l'ordre indiqué pour effacer la configuration du commutateur.

```
no snmp-server access 32
no snmp-server group 16
no snmp-server notify 16
no snmp-server target-parameters 16
no snmp-server target-address 16
no snmp-server user 16
```

Annulation de la gestion d'un commutateur

Vous pouvez retirer un commutateur de la gestion à l'aide de Lenovo XClarity Administrator. Ce processus est appelé *annulation de la gestion.*

Avant de commencer

Vous pouvez activer XClarity Administrator pour annuler automatiquement la gestion des appareils qui sont hors ligne pendant une durée spécifique. Cette option est désactivée par défaut. Pour activer l'annulation de la gestion automatique des appareils hors ligne, cliquez sur **Matériel → Reconnaître et gérer de nouveaux appareils** dans le menu XClarity Administrator, puis cliquez sur **Éditer** en regard de **Annuler la gestion des appareils hors ligne correspond à : Désactivé**. Ensuite, sélectionnez **Activer l'option Annuler la gestion des appareils hors ligne** et définissez l'intervalle de temps. Par défaut, la gestion des appareils est annulée lorsque ceux-ci sont hors ligne pendant 24 heures.

Avant d'annuler la gestion d'un commutateur, vérifiez qu'il n'y a pas de travaux actifs en cours d'exécution sur le commutateur.

À propos de cette tâche

Lorsque vous avez annulé la gestion d'un commutateur, XClarity Administrator conserve certaines informations relatives au commutateur. Ces informations sont réappliquées lorsque vous gérez à nouveau le même commutateur.

Astuce : Tous les appareils de démonstration qui sont éventuellement ajoutés lors de la configuration initiale sont des nœuds dans un châssis. Pour annuler la gestion des appareils de démonstration, annulez la gestion du châssis à l'aide de l'option **Forcer l'annulation de la gestion, même si l'appareil est inaccessible**.

Procédure

Pour annuler la gestion d'un commutateur, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Matériel → Commutateurs** pour afficher la page Commutateurs.

Etape 2. Sélectionnez un ou plusieurs commutateurs dans les listes de commutateurs gérés.

Etape 3. Cliquez sur **Annuler la gestion du commutateur**. Le dialogue Annuler la gestion s'affiche.

Etape 4. **Facultatif :** sélectionnez **Forcer l'annulation de la gestion, même si l'appareil est inaccessible**.

Important : Lors de l'annulation de la gestion du matériel de démonstration, veillez à sélectionner cette option.

Etape 5. Cliquez sur **Annuler la gestion**.La boîte de dialogue Annuler la gestion affiche la progression de chaque étape dans le processus d'annulation de gestion.

Etape 6. Une fois le processus d'annulation de gestion terminé, cliquez sur **OK**.

Récupération d'un commutateur dont la gestion n'a pas été correctement annulée

Si un commutateur est géré par Lenovo XClarity Administrator et que XClarity Administrator est défaillant, vous pouvez récupérer les fonctions de gestion en attendant que le serveur de gestion soit restauré ou remplacé.

Procédure

- Gérez à nouveau le commutateur à l'aide de l'option **Forcer la gestion** (voir Gestion des commutateurs).
- Pour supprimer définitivement une configuration spécifique de XClarity Administrator sur un commutateur dont l'annulation de la gestion n'a pas été effectuée proprement et qui ne sera pas géré à nouveau, procédez comme suit.
  - Gérez le commutateur à nouveau à l'aide de l'option **Forcer la gestion** (voir Gestion des commutateurs), puis annulez la gestion du commutateur afin de nettoyer la configuration (voir Annulation de la gestion d'un commutateur).
  - (ENOS) Connectez-vous au commutateur via le port de console de commutateur ou une session SSH ou Telnet et exécutez les commandes de configuration suivantes dans l'ordre indiqué pour effacer la configuration du commutateur.

```
no snmp-server access 32
no snmp-server group 16
no snmp-server notify 16
no snmp-server target-parameters 16
no snmp-server target-address 16
no snmp-server user 16
```

Chapitre 11. Configuration des serveurs à l’aide de modèles de configuration

Les modèles de serveur sont utilisés pour distribuer ou prédistribuer rapidement sur plusieurs serveurs (armoire, serveurs au format tour et nœuds de traitement) à partir d'un seul jeu de paramètres de configuration définis.

En savoir plus :

- XClarity Administrator : du serveur au cluster
- XClarity Administrator : modèles de configuration

Avant de commencer

Au bout de la période d'essai de 90 jours, vous pouvez continuer à utiliser XClarity Administrator pour gérer et surveiller votre matériel sans frais ; vous devez cependant acheter des licences d'activation de l'ensemble des fonctionnalités pour chaque serveur géré qui prend en charge les fonctionnalités avancées XClarity Administrator afin de continuer à utiliser la fonction de configuration de serveur. Lenovo XClarity Pro fournit l'accès au service et au support, ainsi qu'une licence d'activation des fonctionnalités complètes. Pour plus d’informations sur l’achat de Lenovo XClarity Pro, contactez votre représentant Lenovo ou votre partenaire commercial agréé. Pour plus d'informations, voir Installation de la licence d'activation de l'ensemble des fonctionnalités dans la documentation en ligne de XClarity Administrator.

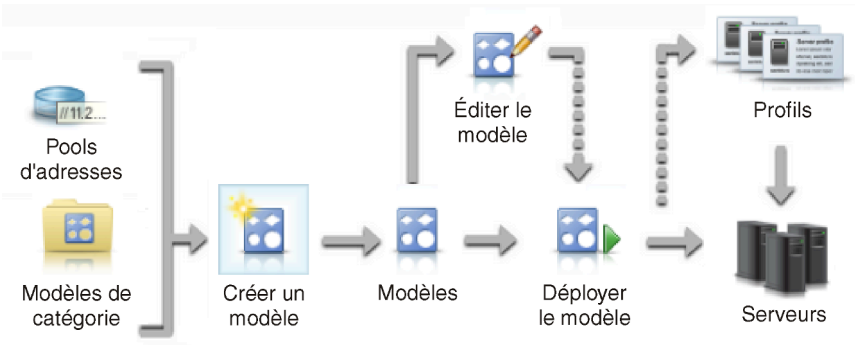
Consultez la section Considérations relatives à la configuration pour connaître les informations importantes relatives à la prise en charge de la configuration pour des serveurs et dispositifs spécifiques.

À propos de cette tâche

Vous pouvez utiliser des modèles de serveur dans XClarity Administrator pour configurer le stockage local, les cartes d’E-S, l'ordre d'amorçage, ainsi que d'autres paramètres de contrôleur de gestion de la carte mère et UEFI (Unified Extensible Firmware Interface) sur les serveurs gérés. Les modèles de serveur intègrent également une prise en charge de la virtualisation des adresses d'E-S. Vous pouvez donc virtualiser les connexions de matrice de serveur ou réaffecter des serveurs sans interruption dans la matrice. Vous pouvez également initier des demandes de modification de segmentation SAN avant la réception de nouveau matériel en virtualisant (préconfigurant) des adresses Fibre Channel.

Procédure

La figure suivante illustre le flux de travaux relatif à la configuration de serveurs gérés. Les flèches pleines indiquent les actions que vous avez effectuées. Les flèches en pointillé indiquent les actions qui sont exécutées automatiquement par XClarity Administrator.



Etape 1. **Créez des pools d'adresses.**Un *pool d'adresses* est un ensemble défini de plages d'adresses. Lenovo XClarity Administrator utilise des pools d'adresses pour affecter des adresses IP et d'E-S à des serveurs individuels lorsque des modèles de serveur sont déployés sur ces serveurs.

Pour plus d'informations sur la création de pools d'adresse, voir Définition de pools d'adresses.

Etape 2. **Créez des modèles de catégorie.**

Un *modèle de catégorie* regroupe les paramètres de microprogramme associés et qui peuvent être réutilisés dans plusieurs modèles de serveur. Vous pouvez créer des modèles pour les catégories de microprogramme suivantes :

- Informations système
- Interfaces de gestion
- Appareils et ports d'E-S
- Cibles d'amorçage FC
- Ports de carte d'E-S

Pour plus d'informations sur les modèles de catégorie, voir Utilisation de modèles de serveur.

Etape 3. **Créez un modèle de serveur.**

Un *modèle de serveur* représente les configurations de serveur pré-système d'exploitation, y compris la configuration de stockage local, la configuration de carte d'E-S, les paramètres d'amorçage, ainsi que d'autres paramètres de contrôleur de gestion de la carte mère et paramètres de microprogramme UEFI. Un modèle de serveur est un modèle global utilisé pour configurer rapidement plusieurs serveurs simultanément.

Vous pouvez définir plusieurs modèles de serveur pour représenter les différentes configurations qui sont utilisées dans votre centre de données.

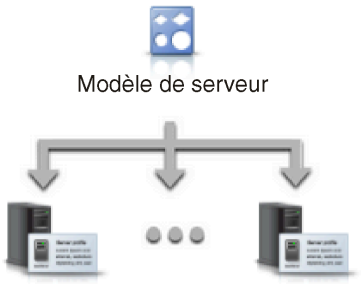
Lorsque vous définissez un modèle de serveur, sélectionnez les modèles de catégorie et les pools d'adresses dont vous avez besoin pour construire la configuration d'un groupe de serveurs spécifique comme vous le souhaitez. Un modèle de catégorie regroupe les paramètres de configuration associés qui peuvent être réutilisés par plusieurs modèles de serveur.

Vous pouvez créer un modèle de serveur à partir de zéro pour les serveurs Converged, Flex System, NeXtScale et System x afin de définir la configuration souhaitée avant l'arrivée du matériel. Vous pouvez aussi créer un modèle de serveur à partir d'un serveur géré existant. Lorsque vous créez un modèle de serveur à partir d'un serveur existant, XClarity Administrator mémorise les modèles de catégorie du serveur sélectionné.

Pour plus d'informations sur la création de modèles de serveur, voir Création d'un modèle de serveur.

Etape 4. **Déployez le modèle de serveur.**

Vous pouvez déployer un modèle de serveur sur un ou plusieurs serveurs individuels ou sur un groupe de serveurs. Par exemple, vous pouvez déployer un modèle de serveur sur un châssis de sorte que tous les nœuds de traitement de ce châssis soient configurés de manière identique. Lors du déploiement, XClarity Administrator crée un profil de serveur pour chaque serveur sur lequel le modèle de serveur a été déployé. Chaque *profil de serveur* représente la configuration spécifique d'un seul serveur. Il hérite des paramètres du modèle de serveur et contient également des informations spécifiques au serveur (comme les adresses IP et les adresses MAC affectées). Étant donné que le profil de serveur hérite des paramètres du modèle de serveur, si vous modifiez ce modèle, les modifications sont automatiquement mises à jour dans le profil de serveur. Ainsi, vous pouvez gérer des configurations communes à un seul emplacement.



Remarque : Les paramètres d'un serveur peuvent ne plus être conformes au profil du serveur s'ils ont été modifiés sans modèles de configuration ou si un problème s'est produit lors du déploiement, par exemple un problème de microprogramme ou de paramètre non valide. Vous pouvez déterminer l'état de conformité de chaque serveur en consultant la page Modèles de configuration : Profils de serveur.

Vous pouvez déployer un modèle de serveur pour :

- **Les serveurs existants**. Un profil de serveur est créé pour chaque serveur. Le profil de serveur est activé une fois le serveur associé réamorcé.
- **Des baies vides dans un châssis existant**. Un profil de serveur est créé pour chaque baie vide. Le profil de serveur qui est associé à la baie vide peut ensuite être activé une fois le nœud de traitement physiquement installé.
- **La marque de réservation d'un châssis que vous n'avez pas encore**. Vous pouvez pré-distribuer sur les nœuds de traitement d'un châssis que vous n'avez pas encore en définissant un *châssis de marque de réservation qui agit en tant que cible pour le modèle de serveur avant l'arrivée du matériel.* Le châssis de marque de réservation regroupe tous les profils de serveur qui sont créés pour chaque baie de nœud de traitement vide. Ainsi, lorsque le matériel arrive, vous pouvez affecter les profils de serveur à tous les nœuds de traitement dans le nouveau châssis en déployant le châssis de marque de réservation dans le nouveau châssis. Chaque profil de serveur est activé une fois le nœud de traitement associé réamorcé.

Remarque : Vous pouvez déployer un modèle de serveur sur plusieurs serveurs. Toutefois, il n'est pas possible de déployer plusieurs modèles sur un serveur unique.

Pour plus d'informations sur le déploiement d'un modèle de serveur, voir Déploiement d'un modèle de serveur sur un serveur et Déploiement d'un châssis de marque de réservation.

Etape 5. **Éditez le modèle de serveur.**

Vous pouvez utiliser des modèles de serveur pour contrôler une configuration commune à partir d'un seul site. Vous ne mettez plus à jour directement les paramètres sur les serveurs. Au lieu de cela, vous mettez à jour les modèles de catégorie et les modèles de serveur, et les modifications sont automatiquement déployées dans tous les profils associés et leurs serveurs.

Pour plus d'informations sur le déploiement d'un modèle de serveur, voir Modification d'un modèle de serveur.

Considérations relatives à la configuration

Avant de commencer à configurer des serveurs via Lenovo XClarity Administrator, tenez compte des considérations importantes suivantes.

- Si un profil de serveur inclut des niveaux de microprogramme plus anciens et que vous mettez à jour le microprogramme à des niveaux ultérieurs, XClarity Administrator compare les paramètres du profil stocké

aux paramètres du serveur, et renvoie « Non conforme ». Passez le curseur au-dessus du statut « Non conforme » pour déterminer la raison de la non conformité.

Vous pouvez modifier manuellement le statut des appareils « Non conforme » en « Conforme » sans redéployer le profil en sélectionnant les appareils, puis en cliquant sur **Toutes les actions → Rendre conforme**.

- Après la mise à niveau du microprogramme (par exemple, des contrôleurs UEFI, BMC ou d'E-S) sur un serveur, certaines configurations peuvent changer (par exemple, lors de l'ajout de nouveaux éléments, de la suppression d'éléments existants ou de la modification des comportements ou de la plage de valeurs d'un élément). Par conséquent, le profil de serveur peut devenir non compatible ou l'application du modèle de serveur peut échouer s'il est créé à l'aide d'un niveau de microprogramme précédent. Dans ce cas, il est recommandé de choisir un nouveau modèle en fonction du microprogramme mis à jour ou d'éditer le modèle qui a échoué, afin d'exclure la configuration d'éléments spécifiques, puis de l'appliquer au serveur.
- L'adaptateur QLogic 8200 double port 10 GbE SFP+ VFA possède des valeurs non valides pour ces paramètres : iSCSIFirstTargetParameters_iSCSIName, iSCSISecondTargetParameters_iSCSIName et IPv6LinkLocalAddress. Vous devez corriger manuellement ces valeurs dans la configuration du système avant d'apprendre le modèle de configuration à partir du serveur ou corriger les valeurs du modèle de configuration appris.
- Pour les nœuds de traitement Flex System x240 et x440 avec adaptateurs RAID intégrés, des modèles de serveur de définition de configuration RAID peuvent être déployés uniquement sur un ou plusieurs serveurs qui n'ont pas de configurations RAID existantes. Si un modèle de serveur est déployé sur un serveur ayant une configuration RAID existante, les grappes et volumes existants ne sont pas remplacés. Pour appliquer la configuration RAID définie dans le modèle de serveur, vous devez d'abord effacer la configuration RAID existante des serveurs (voir Réinitialisation des adaptateurs de stockage aux valeurs par défaut), puis redéployer le profil de serveur en sélectionnant le serveur et en cliquant sur **Plus → Déployer un profil de serveur**.
- Les contrôleurs de stockage intégrés sur des serveurs Flex System x220, Flex System x222 et ThinkSystem prennent en charge RAID basé sur un logiciel. Toutefois, la configuration du logiciel RAID à l'aide de modèles de configuration n'est pas prise en charge.
- Lors de la configuration RAID à l'aide de Modèles de configuration, si le serveur est mis hors tension, le serveur s'amorce sur la configuration BIOS/UEFI automatiquement avant d'activer le profil de serveur.
- Pour les serveurs ThinkServer, les Modèles de configuration ne sont pas pris en charge.
- Certains dispositifs d'E-S ne peuvent pas être configurés à l'aide de modèles de serveur. Pour plus d'informations, voir Support de XClarity Administrator – Page Web de compatibilité.
- Si des fonctionnalités avancées (telles que SPAR, Easy Connect et l'empilement) sont activées sur les commutateurs Flex EN4093R, CN4093, SI4093 ou SI4091, les configurations réseau peuvent ne pas être appliquées correctement sur les ports internes.
- Par défaut, le commutateur Flex SI4093 est fourni avec SPAR activé. Si vous souhaitez déployer des paramètres réseau à l'aide de modèles du port sur les ports internes de ces commutateurs, vous devez retirer manuellement les ports internes de commutateur du service SPAR ou retirer les configurations SPAR du commutateur.
- Il est recommandé de *ne pas* utiliser XClarity Administrator pour configurer les dispositifs Converged et ThinkAgile à l'aide de modèles de configuration.
- Vérifiez que tous les ports disponibles sont activées sur les adaptateurs installés avant de créer les modèles de configuration à partir d'un serveur existant, de sorte que tous les ports et paramètres disponibles soient inclus dans le modèle. Ensuite, si nécessaire, vous pouvez désactiver les ports à l'aide des paramètres appropriés définis dans le modèle. Si les ports sont désactivés lors de la création du modèle, ce dernier ne peut pas être créé correctement, il peut ne pas être déployé.

Définition de pools d'adresses

Un *pool d'adresses* est un ensemble défini de plages d'adresses. Lenovo XClarity Administrator utilise des pools d'adresses pour affecter des adresses IP et d'E-S à des serveurs individuels lorsque des modèles de serveur sont déployés sur ces serveurs.

À propos de cette tâche

XClarity Administrator prend en charge les pools d'adresses IP et d'E-S.

Pools d'adresses IP

Les *pools d'adresses IP* définissent des plages d'adresses IP à utiliser lors de la configuration de l'interface réseau du contrôleur de gestion de la carte mère de vos serveurs. Vous pouvez utiliser ou personnaliser des pools d'adresses prédéfinis ou vous pouvez créer de nouveaux pools, si nécessaire. Lors de la création de modèles de serveur, vous pouvez choisir le pool d'adresses IP à utiliser lors du déploiement. Lorsque le modèle de serveur est déployé, des adresses IP sont allouées depuis le pool sélectionné et affectées à des contrôleurs de gestion individuels.

Remarque : Si vous êtes satisfait de la configuration réseau du contrôleur de gestion, n'utilisez pas cette option.

Attention :

- Vérifiez que vous sélectionnez une sous-plage d'adresses IP qui n'est pas en conflit avec des adresses d'E-S existantes dans votre centre de données.
- Vérifiez que les adresses IP des plages indiquées font partie du même sous-réseau et sont accessibles par XClarity Administrator.
- Vérifiez que les adresses IP des plages indiquées sont uniques pour chaque domaine XClarity Administrator et les outils de gestion IP existants afin d'éviter des conflits d'adresses.

La plage de pool d'adresses globale est dérivée de la longueur de préfixe de routage et de la passerelle ou de la plage initiale indiqués. Vous pouvez créer des pools de différentes tailles selon la longueur de préfixe de routage spécifique, mais les plages de pool globales doivent être uniques au sein du domaine de XClarity Administrator. Les plages sont ensuite créées à partir de la plage de pool globale.

Les plages d'adresses permettent de séparer les hôtes (par exemple, par type de système d'exploitation, types de charge de travail et type de commerce). Les plages d'adresses peuvent également être liées à des règles réseau d'organisations.

Pools d'adresses Ethernet

Les pools d'adresse Ethernet sont des collections d'adresses MAC uniques qui peuvent être affectées aux cartes réseau lors de la configuration des serveurs. Vous pouvez utiliser ou personnaliser des pools d'adresses prédéfinis si nécessaire, ou vous pouvez créer de nouveaux pools. Lors de la création de modèles de serveur, vous pouvez choisir le pool d'adresses Ethernet à utiliser lors du déploiement. Lorsque le modèle de serveur est déployé, des adresses sont allouées depuis le pool sélectionné et affectées aux ports d'adaptateur individuels.

Le pool d'adresses MAC prédéfinies suivant est disponible :
- Pool d'adresses MAC Lenovo

Pour obtenir la liste des plages d'adresses MAC dans ce pool, voir Pools d'adresses Ethernet (MAC).

Pools d'adresses Fibre Channel

Les pools d'adresse Fibre Channel sont des collections d'adresses WWNN et WWPN uniques qui peuvent être affectées aux cartes Fibre Channel lors de la configuration des serveurs. Vous pouvez

utiliser ou personnaliser des pools d'adresses prédéfinis si nécessaire, ou vous pouvez créer de nouveaux pools. Lors de la création de modèles de serveur, vous pouvez choisir le pool d'adresses Fibre Channel à utiliser lors du déploiement. Lorsque le modèle de serveur est déployé, des adresses sont allouées depuis le pool sélectionné et affectées aux ports d'adaptateur individuels.

Les pools d'adresses Fibre Channel suivants sont disponibles :
- Pools d'adresses WWN Lenovo
- Adresses WWN Brocade
- Adresses WWN Emulex
- Adresses WWN QLogic

Pour obtenir la liste des plages d'adresses WWN dans ces pools, voir Pools d'adresses Fibre Channel (WWN).

La plage d'adresses dans les pools d'adresses doit être unique au sein du domaine de XClarity Administrator. XClarity Administrator garantit que les plages définies et les adresses affectées sont uniques au sein de son domaine de gestion.

Important : Dans les environnements de grande envergure dotés de plusieurs instances de XClarity Administrator, vérifiez que des plages d'adresse uniques sont utilisées par chaque instance de XClarity Administrator afin d'éviter la duplication d'adresse.

Des pools d'adresses Ethernet et Fibre Channel sont utilisés avec l'adressage virtuel de carte d'E-S pour affecter des adresses d'E-S unique au sein de l'organisation. Lorsque vous créez un modèle de serveur pour un nœud de traitement, vous pouvez activer l'adressage virtuel dans le cadre de la configuration des appareils et des cartes d'E-S. Lorsque l'adressage virtuel est activé, des adresses sont affectées depuis les pools d'adresses Ethernet et Fibre Channel afin d'éviter les conflits d'adresses.

Restriction : L'adressage virtuel est pris en charge uniquement pour les nœuds de traitement de Flex System. Les serveurs rack et au format tour autonomes ne sont pas pris en charge.

Pour plus d'informations sur la création de modèles de serveur, voir Création d'un modèle de serveur.

Créer un pool d'adresses IP

Un *pool d'adresses IP* définit une plage d'adresses IP à utiliser lors de la configuration de l'interface réseau du contrôleur de gestion de la carte mère de vos serveurs. Lorsque le modèle de serveur associé est déployé, des adresses IP sont allouées depuis le pool spécifié et affectées à des serveurs individuels.

À propos de cette tâche

Les données du tableau Informations réseau globales dans la boîte de dialogue Nouveau pool d'adresses IP sont dérivées du masque de sous-réseau et de la passerelle spécifiés ou de la plage initiale. Vous pouvez créer des pools de différentes tailles selon le masque de sous-réseau spécifique, mais les plages de pool globales doivent être uniques au sein du domaine de gestion. Les plages sont ensuite créées à partir de la plage de pool globale. Toutes les plages doivent faire partie du même sous-réseau et sont déterminées par les limites indiquées dans le tableau Informations réseau globales.

Le pool et les plages ont une portée Lenovo XClarity Administrator. Dans les environnements de grande envergure dotés de plusieurs instances de XClarity Administrator, créez des pools et des plages uniques pour chaque instance de XClarity Administrator afin d'éviter les conflits d'adresses en général et plus précisément, des conflits d'adresses avec des outils de gestion IP existants. Les plages peuvent également être utilisées pour séparer les hôtes (par exemple, par type de système d'exploitation, type de charge de travail et fonction métier) et pour resserrer les règles réseau d'une organisation.

Procédure

Pour créer un pool d'adresses IP, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Pools d'adresses**. La page Modèles de configuration : Pools d'adresses s'affiche.

Etape 2. Cliquez sur l'onglet **Pools d'adresses IP**.

Etape 3. Cliquez sur l'icône **Créer** ( ). La boîte de dialogue Assistant de création de pools d'adresses IP s'affiche.

Etape 4. Entrez les informations ci-après.

- Nom et description du pool d'adresses.
- Choisissez d'utiliser des adresses IPv4 ou IPv6.
- Sélectionnez un masque de sous-réseau (pour IPv4) ou une longueur de préfixe de routage (pour IPv6).
- Indiquez l'adresse de passerelle.Les valeurs des informations réseau sont dérivées du masque de sous-réseau et de la passerelle spécifiés ou de la plage initiale et sont indiquées dans le tableau.
- Ajoutez une ou plusieurs plages d'adresses :
  1. Cliquez sur **Ajouter une plage** pour ajouter une plage d'adresses. La boîte de dialogue Ajouter une plage d'adresses IP s'affiche.
  2. Entrez un nom de plage, la première adresse, ainsi que la taille de la plage.La dernière adresse est calculée automatiquement.
  3. Cliquez sur **OK**.La plage est ajoutée au tableau **Définir des plages d'adresses de pool IP** et les zones de la section récapitulative sont mises à jour automatiquement.

  Vous pouvez modifier la plage en cliquant sur l'icône **Éditer** ( ) ou retirer la plage en cliquant sur l'icône **Retirer** ( ).

Etape 5. Cliquez sur **Créer**.

Après avoir terminé

Le nouveau pool d'adresses IP est répertorié dans le tableau de la page Pools d'adresses IP :

Depuis cette page, vous pouvez exécuter les actions suivantes sur un pool d'adresses sélectionné :

- Modifier le pool d'adresses en cliquant sur l'icône **Éditer** ( ).
- Renommer le pool d'adresses en cliquant sur l'icône **Renommer**.
- Supprimer le pool d'adresses en cliquant sur l'icône **Supprimer** ( ).

- View Afficher des détails sur le pool d'adresses, y compris un mappage entre les adresses virtuelles et les ports de la carte installée et les adresses virtuelles réservées, en cliquant sur le nom de pool dans la colonne **Nom du pool**.

Création d'un pool d'adresses Ethernet

Les pools d'adresse Ethernet sont des collections d'adresses MAC (Media Access Control) uniques qui peuvent être affectées aux cartes réseau. Vous pouvez utiliser ou personnaliser des pools d'adresses prédéfinis si nécessaire, ou vous pouvez créer de nouveaux pools d'adresses. Lors de la création d'un modèle de serveur, si vous activez l'adressage virtuel pour les cartes Ethernet, vous pouvez choisir le pool d'adresses Ethernet à utiliser lorsque le modèle est déployé. Lorsque le modèle de serveur associé est déployé, des adresses MAC sont allouées depuis le pool d'adresses sélectionné et affectées à des cartes réseau sur les serveurs.

Procédure

Pour créer un pool d'adresses Ethernet, procédez comme suit.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Distribution → Pools d'adresses**. La page Modèles de configuration : Pools d'adresses s'affiche.

Etape 2. Cliquez sur l'onglet **Pools d'adresses Ethernet**.

Etape 3. Cliquez sur l'icône **Créer** ( ). La boîte de dialogue Nouveaux pools d'adresses Ethernet (MAC) s'affiche.

Etape 4. Entrez un nom et une description pour le pool d'adresses.

Etape 5. Ajoutez une ou plusieurs plages d'adresses :

a. Cliquez sur **Ajouter une plage** pour ajouter une plage d'adresses. La boîte de dialogue d'ajout Plage d'adresses Ethernet (MAC).

b. Entrez un nom de plage, la première adresse MAC, ainsi que la taille de la plage.

La dernière adresse MAC est calculée automatiquement.

c. Cliquez sur **Ajouter**.

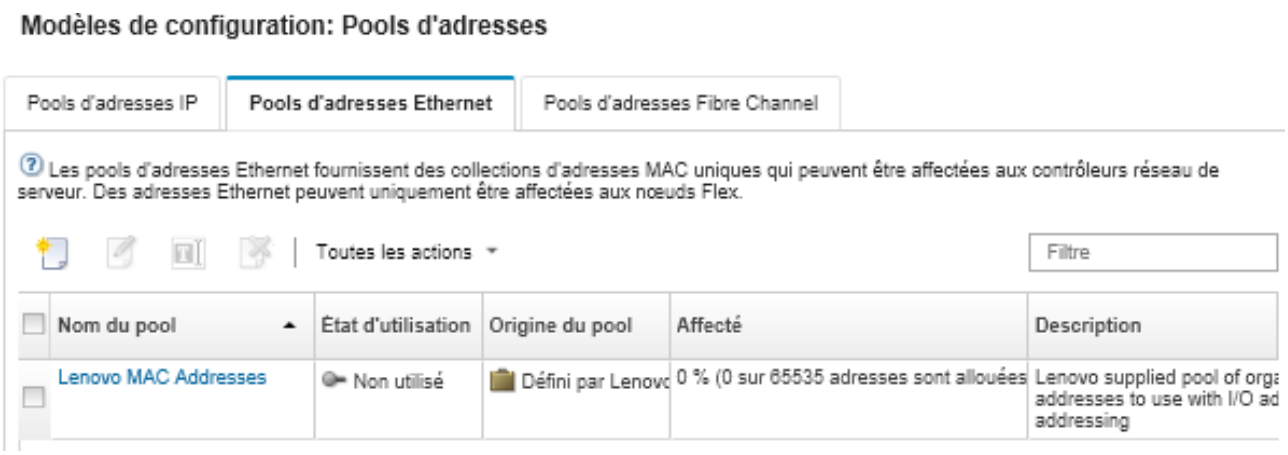
La plage est ajoutée au tableau **Définir des plages d'adresses de pool Ethernet (MAC)** et les zones de la section récapitulative sont mises à jour automatiquement.

Vous pouvez modifier la plage en cliquant sur l'icône **Éditer** ( ) ou retirer la plage en cliquant sur l'icône **Retirer** ( ).

Etape 6. Cliquez sur **Enregistrer**.

Après avoir terminé

Le nouveau pool d'adresses Ethernet est répertorié dans la page Pools d'adresses Ethernet.



Depuis cette page, vous pouvez exécuter les actions suivantes sur un pool d'adresses sélectionné :

- Modifier le pool d'adresses en cliquant sur l'icône **Éditer** ( ).
- Renommer le pool d'adresses en cliquant sur l'icône **Renommer**.
- Supprimer le pool d'adresses en cliquant sur l'icône **Supprimer** ( ).
- View Afficher des détails sur le pool d'adresses, y compris un mappage entre les adresses virtuelles et les ports de la carte installée et les adresses virtuelles réservées, en cliquant sur le nom de pool dans la colonne **Nom du pool**.

Pools d'adresses Ethernet (MAC)

Les pools d'adresses Ethernet sont des collections d'adresses MAC (Media Access Control) uniques qui peuvent être affectées aux cartes réseau. Vous pouvez utiliser le pool d'adresses prédéfini suivant dans vos modèles de serveur.

Tableau 3. Pool d'adresses MAC Lenovo

Plage prédéfinie	Adresse de début	Adresse de fin
Plage 1	00:1A:64:76:00:00	00:1A:64:76:1C:70
Plage 2	00:1A:64:76:1C:71	00:1A:64:76:38:E1
Plage 3	00:1A:64:76:38:E2	00:1A:64:76:55:52
Plage 4	00:1A:64:76:55:53	00:1A:64:76:71:C3
Plage 5	00:1A:64:76:71:C4	00:1A:64:76:8E:34
Plage 6	00:1A:64:76:8E:35	00:1A:64:76:AA:A5
Plage 7	00:1A:64:76:AA:A6	00:1A:64:76:C7:16
Plage 8	00:1A:64:76:C7:17	00:1A:64:76:E3:87
Plage 9	00:1A:64:76:E3:88	00:1A:64:76:FF:F8

Création d'un pool d'adresses Fibre Channel

Les Pools d'adresses Fibre Channel sont des collections d'adresses World Wide Node Name (WWNN) et World Wide Port Name (WWPN) uniques qui peuvent être affectées à des cartes Fibre Channel. Vous pouvez utiliser ou personnaliser des pools d'adresses prédéfinis si nécessaire, ou vous pouvez créer de nouveaux pools. Lors de la création de modèles de serveur, si vous activez l'adressage virtuel pour les cartes Ethernet, vous pouvez choisir le pool d'adresses Fibre Channel à utiliser lorsque le modèle est déployé. Lorsque le modèle de serveur associé est déployé, des adresses WWNN et WWPN sont allouées depuis le pool et affectées à des serveurs individuels.

Procédure

Pour créer un pool d'adresses Fibre Channel, procédez comme suit.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Distribution → Pools d'adresses**. La page Modèles de configuration : Pools d'adresses s'affiche.

Etape 2. Cliquez sur l'onglet **Pools d'adresses Fibre Channel**.

Etape 3. Cliquez sur l'icône **Créer** ( ). La boîte de dialogue Pools d'adresses Fibre Channel s'affiche.

Etape 4. Entrez un nom et une description pour le pool d'adresses.

Etape 5. Ajoutez une ou plusieurs plages d'adresses :

a. Cliquez sur **Ajouter une plage** pour ajouter une plage d'adresses. La boîte de dialogue Plage d'adresses Fibre Channel (WWN) s'affiche.

b. Entrez un nom de plage, une taille de plage, ainsi que la première adresse de chaque matrice.

Les dernières adresses sont calculées automatiquement.

c. Cliquez sur **Ajouter**.

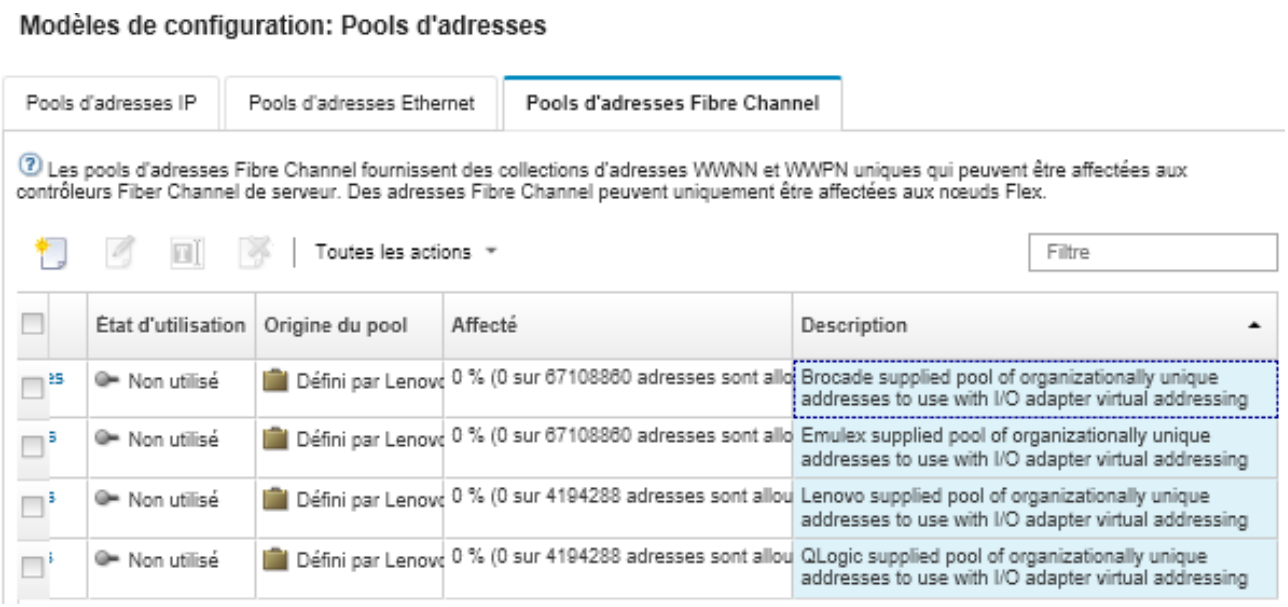
La plage est ajoutée au tableau **Définir les plages d'adresses de Fibre Channel (WWN)**, et les zones de la section récapitulative sont mises à jour automatiquement.

Vous pouvez modifier la plage en cliquant sur l'icône **Éditer** ( ) ou retirer la plage en cliquant sur l'icône **Retirer** ( ).

Etape 6. Cliquez sur **Enregistrer**.

Après avoir terminé

Le nouveau pool d'adresses Fibre Channel est répertorié dans le tableau Pools d'adresses Fibre Channel :



Depuis cette page, vous pouvez exécuter les actions suivantes sur un pool d'adresses sélectionné :

- Modifier le pool d'adresses en cliquant sur l'icône **Éditer** ( ).
- Supprimer le pool d'adresses en cliquant sur l'icône **Supprimer** ( ).

- View Afficher des détails sur le pool d'adresses, y compris un mappage entre les adresses virtuelles et les ports de la carte installée et les adresses virtuelles réservées, en cliquant sur le nom de pool dans la colonne **Nom du pool**.

Pools d'adresses Fibre Channel (WWN)

Les pools d'adresses Fibre Channel sont des collections d'adresses WWNN (World Wide Node Name) et WWPN (World Wide Port Name) uniques qui peuvent être affectées à des adaptateurs Fibre Channel. Vous pouvez utiliser les pools d'adresses prédéfinis suivants dans vos modèles de serveur.

Tableau 4 « Pool d'adresses WWN Brocade » à la page 353 répertorie les pools d'adresses WWN (World Wide Name) Brocade. Chaque plage Brocade contient 1 864 135 adresses.

Tableau 5 « Pool d'adresses WWN Emulex » à la page 354 répertorie les pools d'adresses WWN Emulex. Chaque plage Emulex contient 1 864 135 adresses.

Tableau 6 « Pools d'adresses WWN Lenovo » à la page 355 répertorie les pools d'adresses WWN Lenovo. Chaque plage WWN Lenovo contient 116 508 adresses.

Tableau 7 « Pool d'adresses WWN QLogic » à la page 356 répertorie les pools d'adresses WWN QLogic. Chaque plage WWN QLogic contient 116 508 adresses.

Tableau 4. Pool d'adresses WWN Brocade

Plage prédéfinie	Adresse de début WWNN	Adresse de fin WWNN	Adresse de début WWPN	Adresse de fin WWPN
Matrice A				
Plage 1	2B:FA:00:05:1E:00:00:00	2B:FA:00:05:1E:1C:71:C6	2B:FC:00:05:1E:00:00:00	2B:FC:00:05:1E:1C:71:C6
Plage 2	2B:FA:00:05:1E:1C:71:C7	2B:FA:00:05:1E:38:E3:8D	2B:FC:00:05:1E:1C:71:C7	2B:FC:00:05:1E:38:E3:8D
Plage 3	2B:FA:00:05:1E:38:E3:8E	2B:FA:00:05:1E:55:55:54	2B:FC:00:05:1E:38:E3:8E	2B:FC:00:05:1E:55:55:54
Plage 4	2B:FA:00:05:1E:55:55:55	2B:FA:00:05:1E:71:C7:1B	2B:FC:00:05:1E:55:55:55	2B:FC:00:05:1E:71:C7:1B
Plage 5	2B:FA:00:05:1E:71:C7:1C	2B:FA:00:05:1E:8E:38:E2	2B:FC:00:05:1E:71:C7:1C	2B:FC:00:05:1E:8E:38:E2
Plage 6	2B:FA:00:05:1E:8E:38:E3	2B:FA:00:05:1E:AA:AA:A9	2B:FC:00:05:1E:8E:38:E3	2B:FC:00:05:1E:AA:AA:A9
Plage 7	2B:FA:00:05:1E:AA:AA:AA	2B:FA:00:05:1E:C7:1C:70	2B:FC:00:05:1E:AA:AA:AA	2B:FC:00:05:1E:C7:1C:70
Plage 8	2B:FA:00:05:1E:C7:1C:71	2B:FA:00:05:1E:E3:8E:37	2B:FC:00:05:1E:C7:1C:71	2B:FC:00:05:1E:E3:8E:37
Plage 9	2B:FA:00:05:1E:E3:8E:38	2B:FA:00:05:1E:FF:FF:FE	2B:FC:00:05:1E:E3:8E:38	2B:FC:00:05:1E:FF:FF:FE
Matrice B				
Plage 1	2B:FB:00:05:1E:00:00:00	2B:FB:00:05:1E:1C:71:C6	2B:FD:00:05:1E:00:00:00	2B:FD:00:05:1E:1C:71:C6
Plage 2	2B:FB:00:05:1E:1C:71:C7	2B:FB:00:05:1E:38:E3:8D	2B:FD:00:05:1E:1C:71:C7	2B:FD:00:05:1E:38:E3:8D
Plage 3	2B:FB:00:05:1E:38:E3:8E	2B:FB:00:05:1E:55:55:54	2B:FD:00:05:1E:38:E3:8E	2B:FD:00:05:1E:55:55:54

Tableau 4. Pool d'adresses WWN Brocade (suite)

Plage prédéfinie	Adresse de début WWNN	Adresse de fin WWNN	Adresse de début WWPN	Adresse de fin WWPN
Plage 4	2B:FB:00:05:1E:55:55:55	2B:FB:00:05:1E:71:C7:1B	2B:FD:00:05:1E:55:55:55	2B:FD:00:05:1E:71:C7:1B
Plage 5	2B:FB:00:05:1E:71:C7:1C	2B:FB:00:05:1E:8E:38:E2	2B:FD:00:05:1E:71:C7:1C	2B:FD:00:05:1E:8E:38:E2
Plage 6	2B:FB:00:05:1E:8E:38:E3	2B:FB:00:05:1E:AA:AA:A9	2B:FD:00:05:1E:8E:38:E3	2B:FD:00:05:1E:AA:AA:A9
Plage 7	2B:FB:00:05:1E:AA:AA:AA	2B:FB:00:05:1E:C7:1C:70	2B:FD:00:05:1E:AA:AA:AA	2B:FD:00:05:1E:C7:1C:70
Plage 8	2B:FB:00:05:1E:C7:1C:71	2B:FB:00:05:1E:E3:8E:37	2B:FD:00:05:1E:C7:1C:71	2B:FD:00:05:1E:E3:8E:37
Plage 9	2B:FB:00:05:1E:E3:8E:38	2B:FB:00:05:1E:FF:FF:FE	2B:FD:00:05:1E:E3:8E:38	2B:FD:00:05:1E:FF:FF:FE

Tableau 5. Pool d'adresses WWN Emulex

Plage prédéfinie	Adresse de début WWNN	Adresse de fin WWNN	Adresse de début WWPN	Adresse de fin WWPN
Matrice A				
Plage 1	2F:FE:00:00:C9:00:00:00	2F:FE:00:00:C9:1C:71:C6	2F:FC:00:00:C9:00:00:00	2F:FC:00:00:C9:1C:71:C6
Plage 2	2F:FE:00:00:C9:1C:71:C7	2F:FE:00:00:C9:38:E3:8D	2F:FC:00:00:C9:1C:71:C7	2F:FC:00:00:C9:38:E3:8D
Plage 3	2F:FE:00:00:C9:38:E3:8E	2F:FE:00:00:C9:55:55:54	2F:FC:00:00:C9:38:E3:8E	2F:FC:00:00:C9:55:55:54
Plage 4	2F:FE:00:00:C9:55:55:55	2F:FE:00:00:C9:71:C7:1B	2F:FC:00:00:C9:55:55:55	2F:FC:00:00:C9:71:C7:1B
Plage 5	2F:FE:00:00:C9:71:C7:1C	2F:FE:00:00:C9:8E:38:E2	2F:FC:00:00:C9:71:C7:1C	2F:FC:00:00:C9:8E:38:E2
Plage 6	2F:FE:00:00:C9:8E:38:E3	2F:FE:00:00:C9:AA:AA:A9	2F:FC:00:00:C9:8E:38:E3	2F:FC:00:00:C9:AA:AA:A9
Plage 7	2F:FE:00:00:C9:AA:AA:AA	2F:FE:00:00:C9:C7:1C:70	2F:FC:00:00:C9:AA:AA:AA	2F:FC:00:00:C9:C7:1C:70
Plage 8	2F:FE:00:00:C9:C7:1C:71	2F:FE:00:00:C9:E3:8E:37	2F:FC:00:00:C9:C7:1C:71	2F:FC:00:00:C9:E3:8E:37
Plage 9	2F:FE:00:00:C9:E3:8E:38	2F:FE:00:00:C9:FF:FF:FE	2F:FC:00:00:C9:E3:8E:38	2F:FC:00:00:C9:FF:FF:FE
Matrice B				
Plage 1	2F:FF:00:00:C9:00:00:00	2F:FF:00:00:C9:1C:71:C6	2F:FD:00:00:C9:00:00:00	2F:FD:00:00:C9:1C:71:C6
Plage 2	2F:FF:00:00:C9:1C:71:C7	2F:FF:00:00:C9:38:E3:8D	2F:FD:00:00:C9:1C:71:C7	2F:FD:00:00:C9:38:E3:8D
Plage 3	2F:FF:00:00:C9:38:E3:8E	2F:FF:00:00:C9:55:55:54	2F:FD:00:00:C9:38:E3:8E	2F:FD:00:00:C9:55:55:54
Plage 4	2F:FF:00:00:C9:55:55:55	2F:FF:00:00:C9:71:C7:1B	2F:FD:00:00:C9:55:55:55	2F:FD:00:00:C9:71:C7:1B

Tableau 5. Pool d'adresses WWN Emulex (suite)

Plage prédéfinie	Adresse de début WWNN	Adresse de fin WWNN	Adresse de début WWPN	Adresse de fin WWPN
Plage 5	2F:FF:00:00:C9:71:C7:1C	2F:FF:00:00:C9:8E:38:E2	2F:FD:00:00:C9:71:C7:1C	2F:FD:00:00:C9:8E:38:E2
Plage 6	2F:FF:00:00:C9:8E:38:E3	2F:FF:00:00:C9:AA:AA:A9	2F:FD:00:00:C9:8E:38:E3	2F:FD:00:00:C9:AA:AA:A9
Plage 7	2F:FF:00:00:C9:AA:AA:AA	2F:FF:00:00:C9:C7:1C:70	2F:FD:00:00:C9:AA:AA:AA	2F:FD:00:00:C9:C7:1C:70
Plage 8	2F:FF:00:00:C9:C7:1C:71	2F:FF:00:00:C9:E3:8E:37	2F:FD:00:00:C9:C7:1C:71	2F:FD:00:00:C9:E3:8E:37
Plage 9	2F:FF:00:00:C9:E3:8E:38	2F:FF:00:00:C9:FF:FF:FE	2F:FD:00:00:C9:E3:8E:38	2F:FD:00:00:C9:FF:FF:FE

Tableau 6. Pools d'adresses WWN Lenovo

Plage prédéfinie	Adresse de début WWNN	Adresse de fin WWNN	Adresse de début WWPN	Adresse de fin WWPN
Matrice A				
Plage 1	20:80:00:50:76:00:00:00	20:80:00:50:76:01:C7:1B	21:80:00:50:76:00:00:00	21:80:00:50:76:01:C7:1B
Plage 2	20:80:00:50:76:01:C7:1C	20:80:00:50:76:03:8E:37	21:80:00:50:76:01:C7:1C	21:80:00:50:76:03:8E:37
Plage 3	20:80:00:50:76:03:8E:38	20:80:00:50:76:05:55:53	21:80:00:50:76:03:8E:38	21:80:00:50:76:05:55:53
Plage 4	20:80:00:50:76:05:55:54	20:80:00:50:76:07:1C:6F	21:80:00:50:76:05:55:54	21:80:00:50:76:07:1C:6F
Plage 5	20:80:00:50:76:07:1C:70	20:80:00:50:76:08:E3:8B	21:80:00:50:76:07:1C:70	21:80:00:50:76:08:E3:8B
Plage 6	20:80:00:50:76:08:E3:8C	20:80:00:50:76:0A:AA:A7	21:80:00:50:76:08:E3:8C	21:80:00:50:76:0A:AA:A7
Plage 7	20:80:00:50:76:0A:AA:A8	20:80:00:50:76:0C:71:C3	21:80:00:50:76:0A:AA:A8	21:80:00:50:76:0C:71:C3
Plage 8	20:80:00:50:76:0C:71:C4	20:80:00:50:76:0E:38:DF	21:80:00:50:76:0C:71:C4	21:80:00:50:76:0E:38:DF
Plage 9	20:80:00:50:76:0E:38:E0	20:80:00:50:76:0F:FF:FB	21:80:00:50:76:0E:38:E0	21:80:00:50:76:0F:FF:FB
Matrice B				
Plage 1	20:81:00:50:76:20:00:00	20:81:00:50:76:21:C7:1B	21:81:00:50:76:20:00:00	21:81:00:50:76:21:C7:1B
Plage 2	20:81:00:50:76:21:C7:1C	20:81:00:50:76:23:8E:37	21:81:00:50:76:21:C7:1C	21:81:00:50:76:23:8E:37
Plage 3	20:81:00:50:76:23:8E:38	20:81:00:50:76:25:55:53	21:81:00:50:76:23:8E:38	21:81:00:50:76:25:55:53
Plage 4	20:81:00:50:76:25:55:54	20:81:00:50:76:27:1C:6F	21:81:00:50:76:25:55:54	21:81:00:50:76:27:1C:6F
Plage 5	20:81:00:50:76:27:1C:70	20:81:00:50:76:28:E3:8B	21:81:00:50:76:27:1C:70	21:81:00:50:76:28:E3:8B

Tableau 6. Pools d'adresses WWN Lenovo (suite)

Plage prédéfinie	Adresse de début WWNN	Adresse de fin WWNN	Adresse de début WWPN	Adresse de fin WWPN
Plage 6	20:81:00:50:76:28:E3:8C	20:81:00:50:76:2A:AA:A7	21:81:00:50:76:28:E3:8C	21:81:00:50:76:2A:AA:A7
Plage 7	20:81:00:50:76:2A:AA:A8	20:81:00:50:76:2C:71:C3	21:81:00:50:76:2A:AA:A8	21:81:00:50:76:2C:71:C3
Plage 8	20:81:00:50:76:2C:71:C4	20:81:00:50:76:2E:38:DF	21:81:00:50:76:2C:71:C4	21:81:00:50:76:2E:38:DF
Plage 9	20:81:00:50:76:2E:38:E0	20:81:00:50:76:2F:FF:FB	21:81:00:50:76:2E:38:E0	21:81:00:50:76:2F:FF:FB

Tableau 7. Pool d'adresses WWN QLogic

Plage prédéfinie	Adresse de début WWNN	Adresse de fin WWNN	Adresse de fin WWPN	Adresse de fin WWPN
Matrice A				
Plage 1	20:80:00:E0:8B:00:00:00	20:80:00:E0:8B:01:C7:1B	21:80:00:E0:8B:00:00:00	21:80:00:E0:8B:01:C7:1B
Plage 2	20:80:00:E0:8B:01:C7:1C	20:80:00:E0:8B:03:8E:37	21:80:00:E0:8B:01:C7:1C	21:80:00:E0:8B:03:8E:37
Plage 3	20:80:00:E0:8B:03:8E:38	20:80:00:E0:8B:05:55:53	21:80:00:E0:8B:03:8E:38	21:80:00:E0:8B:05:55:53
Plage 4	20:80:00:E0:8B:05:55:54	20:80:00:E0:8B:07:1C:6F	21:80:00:E0:8B:05:55:54	21:80:00:E0:8B:07:1C:6F
Plage 5	20:80:00:E0:8B:07:1C:70	20:80:00:E0:8B:08:E3:8B	21:80:00:E0:8B:07:1C:70	21:80:00:E0:8B:08:E3:8B
Plage 6	20:80:00:E0:8B:08:E3:8C	20:80:00:E0:8B:0A:AA:A7	21:80:00:E0:8B:08:E3:8C	21:80:00:E0:8B:0A:AA:A7
Plage 7	20:80:00:E0:8B:0A:AA:A8	20:80:00:E0:8B:0C:71:C3	21:80:00:E0:8B:0A:AA:A8	21:80:00:E0:8B:0C:71:C3
Plage 8	20:80:00:E0:8B:0C:71:C4	20:80:00:E0:8B:0E:38:DF	21:80:00:E0:8B:0C:71:C4	21:80:00:E0:8B:0E:38:DF
Plage 9	20:80:00:E0:8B:0E:38:E0	20:80:00:E0:8B:0F:FF:FB	21:80:00:E0:8B:0E:38:E0	21:80:00:E0:8B:0F:FF:FB
Matrice B				
Plage 1	20:81:00:E0:8B:20:00:00	20:81:00:E0:8B:21:C7:1B	21:81:00:E0:8B:20:00:00	21:81:00:E0:8B:21:C7:1B
Plage 2	20:81:00:E0:8B:21:C7:1C	20:81:00:E0:8B:23:8E:37	21:81:00:E0:8B:21:C7:1C	21:81:00:E0:8B:23:8E:37
Plage 3	20:81:00:E0:8B:23:8E:38	20:81:00:E0:8B:25:55:53	21:81:00:E0:8B:23:8E:38	21:81:00:E0:8B:25:55:53
Plage 4	20:81:00:E0:8B:25:55:54	20:81:00:E0:8B:27:1C:6F	21:81:00:E0:8B:25:55:54	21:81:00:E0:8B:27:1C:6F
Plage 5	20:81:00:E0:8B:27:1C:70	20:81:00:E0:8B:28:E3:8B	21:81:00:E0:8B:27:1C:70	21:81:00:E0:8B:28:E3:8B
Plage 6	20:81:00:E0:8B:28:E3:8C	20:81:00:E0:8B:2A:AA:A7	21:81:00:E0:8B:28:E3:8C	21:81:00:E0:8B:2A:AA:A7

Tableau 7. Pool d'adresses WWN QLogic (suite)

Plage prédéfinie	Adresse de début WWNN	Adresse de fin WWNN	Adresse de fin WWPN	Adresse de fin WWPN
Plage 7	20:81:00:E0:8B:2A:AA:A8	20:81:00:E0:8B:2C:71:C3	21:81:00:E0:8B:2A:AA:A8	21:81:00:E0:8B:2C:71:C3
Plage 8	20:81:00:E0:8B:2C:71:C4	20:81:00:E0:8B:2E:38:DF	21:81:00:E0:8B:2C:71:C4	21:81:00:E0:8B:2E:38:DF
Plage 9	20:81:00:E0:8B:2E:38:E0	20:81:00:E0:8B:2F:FF:FB	21:81:00:E0:8B:2E:38:E0	21:81:00:E0:8B:2F:FF:FB

Utilisation de modèles de serveur

Un *modèle de serveur* représente la configuration d'un serveur pré-système d'exploitation, notamment les paramètres du stockage local, de la carte d'E-S, de l'amorçage SAN, ainsi que d'autres paramètres de contrôleur de gestion de la carte mère et de microprogramme UEFI. Les modèles de serveur intègrent également une prise en charge de la virtualisation des adresses d'E-S. Vous pouvez ainsi virtualiser les connexions de matrice de serveur ou réaffecter des serveurs sans interruption. Un modèle de serveur est un modèle global utilisé pour configurer rapidement plusieurs serveurs simultanément.

À propos de cette tâche

Vous pouvez définir plusieurs modèles de serveur pour représenter les différentes configurations qui sont utilisées dans votre centre de données.

Lorsque vous définissez un modèle de serveur, sélectionnez ou créer des modèles de catégorie et des pools d'adresses selon vos besoins pour construire la configuration souhaitée pour un groupe de serveurs spécifique. Un *modèle de catégorie* définit des paramètres de microprogramme spécifiques réutilisables par plusieurs modèles de serveur. Vous pouvez utiliser des pools d'adresses pour définir des plages d'adresses à utiliser pour affecter des adresses à des serveurs individuels lors du déploiement de modèles de serveur. Il existe des pools d'adresses IP, des pools d'adresses Ethernet (MAC) et des pools d'adresses Fibre Channel (WWN).

Lorsqu'un modèle de serveur est déployé sur plusieurs serveurs, plusieurs profils de serveur sont automatiquement générés (un profil par serveur). Chaque profil hérite des paramètres du modèle de serveur parent, de sorte que vous pouvez contrôler une configuration commune à partir d'un seul emplacement.

Vous pouvez créer un modèle de serveur de toute pièce, en définissant la configuration souhaitée avant l'arrivée de votre matériel. Vous pouvez également créer un modèle de serveur à partir d'un serveur existant, puis utiliser ce modèle pour mettre à disposition vos autres serveurs. Si vous créez un modèle de serveur à partir d'un serveur existant, les modèles de catégorie étendus sont obtenus et créés de façon dynamique à partir des paramètres actuels du serveur. Si vous souhaitez modifier les paramètres de catégorie, vous pouvez les éditer directement à partir des modèles de serveur.

Attention : Lorsque vous créez un modèle de serveur de toute pièce, vous devez définir les paramètres d'amorçage pour les serveurs. Lorsque vous déployez le modèle de serveur sur des serveurs, l'ordre d'amorçage existant sur les serveurs est remplacé par les paramètres d'ordre d'amorçage par défaut définis dans le modèle de serveur. Si les serveurs ne démarrent pas après le déploiement d'un modèle de serveur sur ces serveurs, il se peut que les paramètres d'amorçage d'origine aient été remplacés par les paramètres d'ordre d'amorçage par défaut spécifiés dans le nouveau modèle de serveur. Pour restaurer les paramètres d'amorçage d'origine sur les serveurs, voir Récupération de paramètres d'amorçage après le déploiement d'un modèle de serveur.

Important : Lorsque vous créez des modèles de serveur, veillez à les créer pour chaque type de serveur. Par exemple, créez un modèle de serveur pour tous les nœuds de traitement x240 Flex System et un autre modèle de serveur pour tous les nœuds de traitement x440 Flex System. Ne déployez pas un modèle de serveur créé pour un type de serveur sur un autre type de serveur.

Important : Si le nœud de gestion est défaillant, vous risquez de perdre vos modèles de serveur. Créez toujours une sauvegarde du logiciel de gestion après avoir créé ou modifié des modèles de serveur (voir Sauvegarde de Lenovo XClarity Administrator).

Paramètres pour les dispositifs réseau

Certains dispositifs réseau Flex System offrent plus d'options de configuration que d'autres dans les modèles de serveurs.

Bien que les modèles de serveur puissent être appliqués à n'importe quel dispositif réseau, certaines fonctionnalités des modèles de serveur sont limitées à certaines cartes réseau. De plus, certains paramètres avancés pour les cartes réseau Ethernet (par exemple les préférences de compatibilité de port et de carte) ne sont actuellement pas pris en charge.

Les modèles de serveur peuvent obtenir des données et des paramètres de configuration existants pour les cartes réseau prises en charge, et peuvent modifier les paramètres de configuration via le déploiement de modèle.

Modèles de catégorie

Les paramètres de microprogramme sont organisés en catégories qui regroupent des paramètres associés. Pour chaque catégorie, vous pouvez créer un *modèle de catégorie* qui contient les paramètres de microprogramme communs pouvant être réutilisés par plusieurs modèles de serveur. La plupart des paramètres de microprogramme que vous pouvez configurer directement sur le contrôleur de gestion de la carte mère et l'interface UEFI peuvent également être configurés via des modèles de catégorie. Les paramètres de microprogramme disponibles dépendent du type de serveur, de votre environnement Flex System, ainsi que de la portée du modèle de serveur.

Vous pouvez créer des modèles de catégorie séparément des modèles de serveur.

Les modèles de catégorie peuvent être prédéfinis, obtenus à partir de serveurs existants ou définis par l'utilisateur.

- **Modèles de catégorie étendus**

  Les *modèles de catégorie étendus* sont des modèles pour certains ports de carte d'E-S, l'interface UEFI (Unified Extensible Firmware Interface) avancée et les paramètres de contrôleur de gestion de la carte mère qui sont obtenus et créés de façon dynamique à partir d'un serveur géré spécifique. Lenovo XClarity Administrator crée ces modèles lorsque vous créez un modèle de serveur à partir d'un serveur existant. Vous ne pouvez pas créer manuellement des modèles de catégorie étendus. Toutefois, vous pouvez éditer les modèles une fois qu'ils sont créés.

  Les modèles UEFI étendu suivants sont prédéfinis par XClarity Administrator pour optimiser vos serveurs pour des environnements spécifiques.
  - **Options d'installation ESXi**
  - **Efficience – Favoriser les performances**
  - **Efficience – Favoriser l'énergie**
  - **Performance maximale**
  - **Energie minimale**
- **Modèles de catégorie définis par l'utilisateur**

Les *modèles de catégorie définis par l'utilisateur* sont des modèles que vous pouvez créer, en y incluant des informations système, des interfaces de gestion, des appareils et des ports d'E-S, des cibles d'amorçage Fibre Channel, ainsi que des ports de carte d'E-S. Vous pouvez créer les modèles de catégorie suivants :

- **Informations système**. Les paramètres incluent le nom du système généré automatiquement, l'emplacement et les informations de contact.
- **Interface de gestion**. Les paramètres incluent le nom d'hôte généré automatiquement, l'adresse IP, l'espace de nom de domaine (DNS), la vitesse d'interface et les affectations de port pour l'interface de gestion.Les paramètres duplex ne sont pas pris en charge par les modèles de serveur.
- **Appareils et ports d'E-S**. Les paramètres incluent les ports COM et de réacheminement de la console. Vous pouvez utiliser des modèles de serveur pour activer la fonctionnalité Serial over LAN dans la zone de réacheminement de la console. Toutefois, lorsque la fonctionnalité Serial over LAN est activée, le seul paramètre de mode d'accès de port série pris en charge par les modèles de serveur est **Dédié**. Les paramètres IPMI **Partagé** et **Pré-amorçage** pour le mode d'accès de port série ne sont pas disponibles dans les modèles de serveur.

  Important : Si vous créez un modèle de serveur à partir d'un serveur existant et que ce dernier est défini avec le paramètre de mode d'accès de port série **Partagé** ou **Pré-amorçage**, le modèle Appareils et ports d'E-S obtenu à partir du serveur a le paramètre de mode d'accès de port série **Dédié**.
- **Cibles d'amorçage Fibre Channel**. Les paramètres incluent des cibles d'amorçage WWN et Fibre Channel principales et secondaires spécifiques.
- **Ports**. Les paramètres incluent des cartes d'E-S et des ports pour la configuration d'interconnexions de matrices.

Création d'un modèle de serveur

Lorsque vous créez un modèle de serveur, vous définissez les caractéristiques de configuration pour un type spécifique de serveur. Vous pouvez créer un modèle de serveur en partant de zéro en utilisant les paramètres par défaut ou les paramètres d'un serveur existant.

À propos de cette tâche

Avant de créer un modèle de serveur, tenez compte des suggestions ci-dessous.

- La première fois que vous créez un modèle de serveur, envisagez de le faire à partir d'un serveur existant. Lorsque vous créez un modèle de serveur à partir d'un serveur existant, Lenovo XClarity Administrator mémorise et crée des modèles de catégorie étendus pour certains ports de carte d'E-S, UEFI, et paramètres de contrôleur de gestion de la carte mère. Ensuite, ces modèles de catégorie sont disponibles pour une utilisation dans un modèle de serveur que vous créez ultérieurement. Pour plus d'informations sur les modèles de catégorie, voir Définition de paramètres de microprogramme.
- Identifiez les groupes de serveurs qui comportent les mêmes options matérielles et que vous souhaitez configurer de la même manière. Vous pouvez utiliser un modèle de serveur pour appliquer les mêmes paramètres de configuration à plusieurs serveurs, ce qui vous permet de contrôler une configuration commune depuis un seul emplacement.
- Identifiez les aspects de la configuration que vous souhaitez personnaliser pour le modèle de serveur (par exemple, stockage local, cartes réseau, contrôleur de gestion, paramètres, paramètres UEFI).
- Vous ne pouvez pas gérer des comptes utilisateur locaux ou configurer le serveur LDAP à l'aide de modèles de configuration.

Important : Si le nœud de gestion est défaillant, vous risquez de perdre vos modèles de serveur. Créez toujours une sauvegarde du logiciel de gestion après avoir créé ou modifié les modèles de serveur (voir Sauvegarde de Lenovo XClarity Administrator.

Procédure

Pour créer un modèle de serveur, procédez comme suit.

Etape 1. Depuis la barre de menus XClarity Administrator, cliquez sur **Distribution → Modèles de configuration de serveur**. La page Modèles de configuration de serveur s'affiche.

Etape 2. Cliquez sur l'onglet **Modèles de serveur**.

Etape 3. Cliquez sur l'icône **Créer** ( ). L'Assistant de création d'un modèle serveur s'affiche.

Etape 4. Pour créer le modèle de serveur, exécutez l'une des actions suivantes.

- Cliquez sur **Créer un modèle à partir d'un serveur existant** pour utiliser les paramètres d'un serveur existant. Ensuite, sélectionnez le serveur géré sur lequel le nouveau modèle doit être basé dans la liste affichée.

  Lorsque vous créez un modèle de serveur à partir d'un serveur existant, XClarity Administrator obtient les paramètres du serveur géré indiqué (y compris les paramètres de port étendu, UEFI et les paramètres de contrôleur de gestion de la carte mère) et crée dynamiquement des modèles de catégorie pour ces paramètres. Dans le cas d'un tout nouveau serveur, Lenovo XClarity Administrator mémorise les paramètres d'usine. Si XClarity Administrator gère le serveur, XClarity Administrator utilise les paramètres personnalisés. Vous pouvez ensuite personnaliser les paramètres en fonction des serveurs sur lequel ce modèle doit être déployé.
- Cliquez sur **Créer un modèle à partir de zéro** pour utiliser les paramètres par défaut. Ensuite, sélectionnez le type de serveur dans la zone **Format**.

Remarque : Les options qui sont présentées sur les onglets restants diffèrent selon le type de serveur pour lequel vous créez un modèle.

Etape 5. Entrez le nom du nouveau modèle ainsi qu'une description.

Etape 6. Personnalisez le nom de profil de serveur en sélectionnant le bouton **Personnalisé** puis en choisissant un ou plusieurs éléments à inclure dans le schéma de désignation (par exemple, un texte personnalisé, un nom de serveur et un nombre d'incrémentation) et l'ordre.

Etape 7. Cliquez sur **Suivant**

Etape 8. Choisissez la configuration de stockage local à appliquer lorsque ce modèle est déployé sur un serveur, puis cliquez sur **Suivant**.

Pour plus d'informations sur les paramètres de stockage local, voir Définition d'un stockage local.

Etape 9. **Facultatif :** Modifiez l'adressage de carte d'E-S et définissez des cartes d'E-S supplémentaires qui correspondent au matériel que vous prévoyez de configurer avec ce modèle, puis cliquez sur **Suivant**.

Pour plus d'informations sur les paramètres de carte d'E-S, voir Définition de cartes d'E-S.

Etape 10. Définissez l'ordre d'amorçage à appliquer lorsque ce modèle est déployé sur un serveur, puis cliquez sur **Suivant**.

Pour plus d'informations sur les paramètres des cibles d'amorçage SAN, voir Définition d'options d'amorçage.

Etape 11. Sélectionnez les paramètres du microprogramme dans la liste des modèles de catégorie existants.

Vous pouvez créer de nouveaux modèles de catégorie en cliquant sur l'icône **Créer** ( ).

Pour plus d'informations sur les paramètres de microprogramme, voir Définition de paramètres de microprogramme.

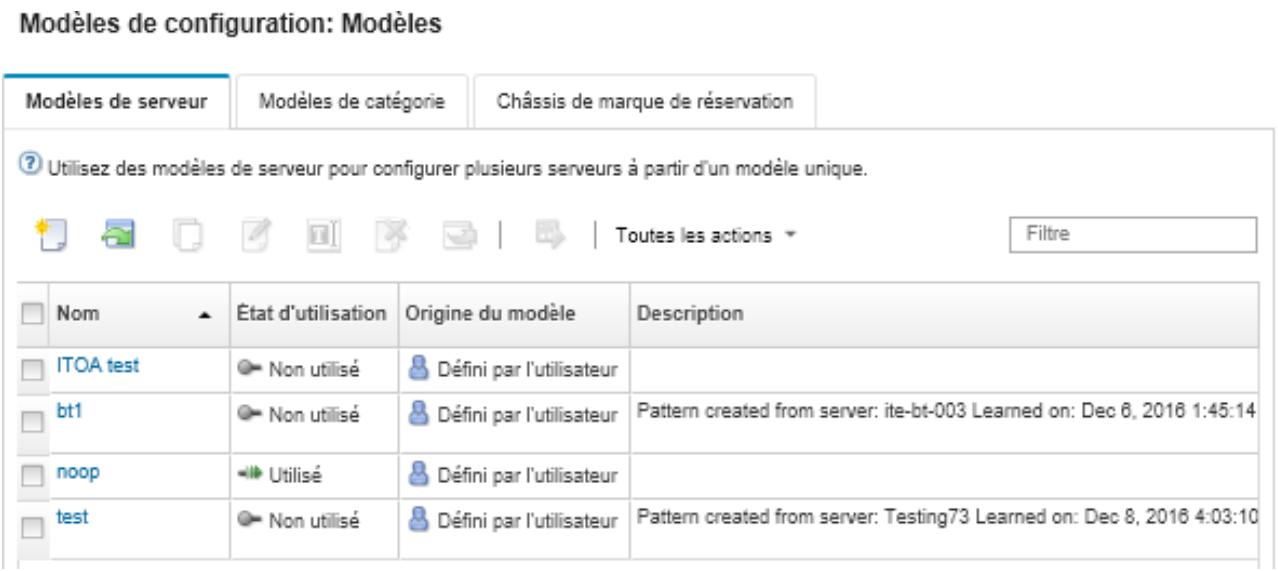
Etape 12. Cliquez sur **Enregistrer** pour enregistrer le modèle, ou cliquez sur **Enregistrer et déployer** pour enregistrer et déployer immédiatement le modèle sur un ou plusieurs serveurs.

Pour plus d'informations sur le déploiement d'un modèle de serveur, voir Déploiement d'un modèle de serveur sur un serveur.

Après avoir terminé

Si vous avez cliqué sur **Enregistrer et déployer**, la page Déployer un modèle de serveur s'affiche. Depuis cette page, vous pouvez déployer le modèle de serveur sur des serveurs spécifiques.

Si vous avez cliqué sur **Enregistrer**, le modèle de serveur et tous modèles de catégorie sont enregistrés sur la page Modèles de serveur.



Depuis cette page, vous pouvez exécuter les actions suivantes sur les modèles de serveur sélectionnés :

- Pour afficher des détails sur le modèle, cliquez sur le nom de modèle dans la colonne **Nom**.
- Déployez le modèle (voir Déploiement d'un modèle de serveur sur un serveur).
- Copiez le modèle en cliquant sur l'icône **Copier** ( ).
- Éditez le modèle (voir Modification d'un modèle de serveur).
- Renommez le modèle en cliquant sur l'icône **Renommer** ( ).
- Supprimez le modèle en cliquant sur l'icône **Supprimer** ( ).
- Exportez et importez des modèles de serveur (voir Exportation et importation de modèles de serveur et de catégorie).

Définition d'un stockage local

Vous pouvez définir la configuration de stockage local à appliquer aux serveurs cibles lors du déploiement de ce modèle.

À propos de cette tâche

Remarques :

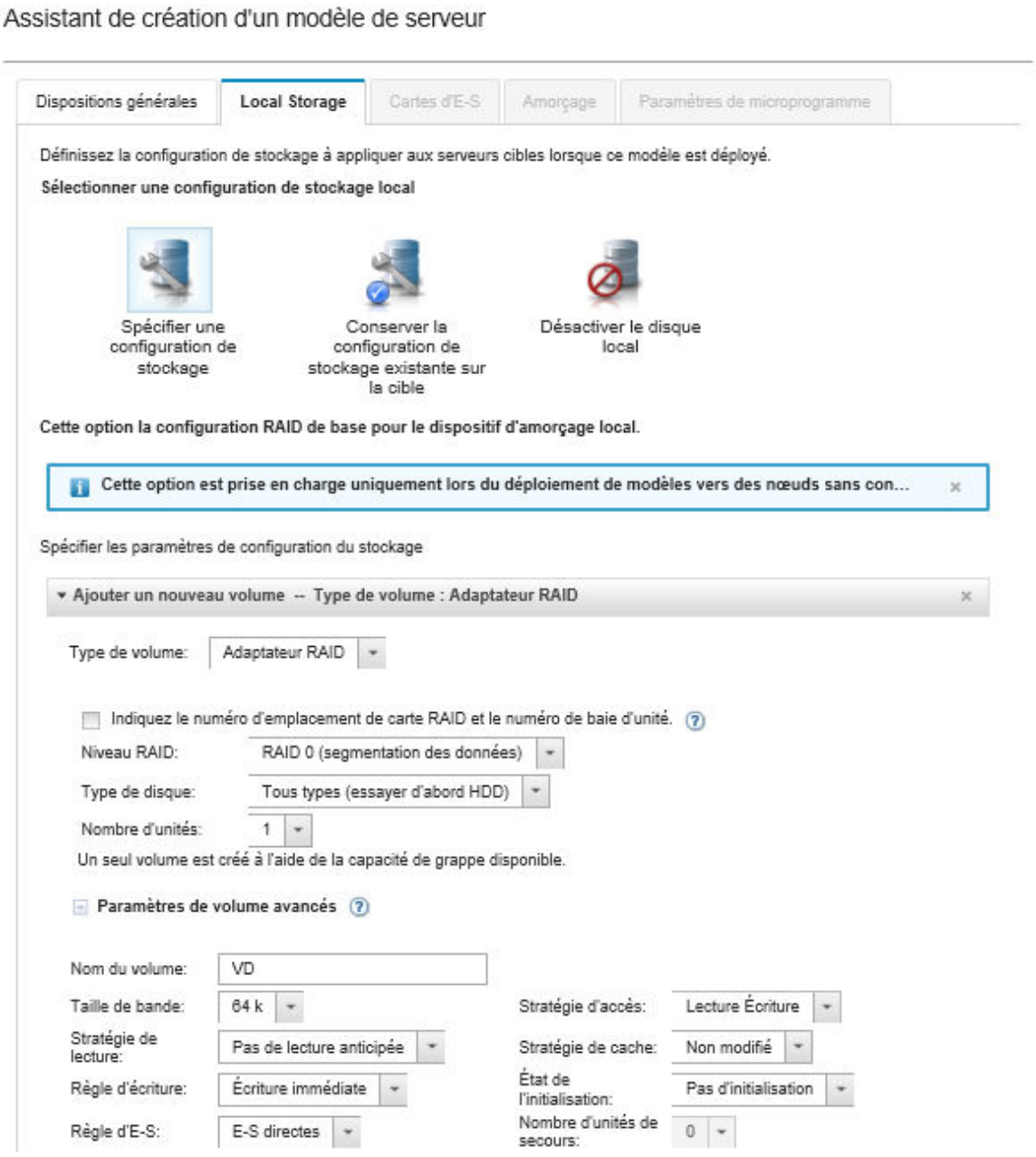
- Les contrôleurs de stockage intégrés sur des serveurs Flex System x220, Flex System x222 et ThinkSystem prennent en charge RAID basé sur un logiciel. Toutefois, la configuration du logiciel RAID à l'aide de modèles de configuration n'est pas prise en charge.

- Lors de la configuration RAID à l'aide de Modèles de configuration, si le serveur est mis hors tension, le serveur s'amorce sur la configuration BIOS/UEFI automatiquement avant d'activer le profil de serveur.

Procédure

Pour définir la configuration de stockage local, procédez comme suit.

Etape 1. Dans l'Assistant de création d'un modèle serveur, cliquez sur l'onglet **Stockage local**.



Etape 2. Pour définir les paramètres de stockage local, choisissez l'une des options suivantes.

- **Spécifier une configuration de stockage**. (Appareils sans configurations RAID de sortie uniquement) Les paramètres RAID de base sont configurés sur le dispositif d'amorçage local lors du déploiement

Indiquez la configuration de stockage en fonction de l'option de stockage. Vous pouvez ajouter des options de stockage supplémentaires en cliquant sur **Ajouter** ( ).

- **Adaptateur RAID**. Choisissez le niveau RAID, characteristics, ainsi que le nombre d'unités qui sont installés dans le serveur. RAID 0, 1, 5 sont pris en charge. En outre, vous pouvez choisir des paramètres de volume avancés, tels que la taille des segments, les stratégies et le nombre d'unités de secours.

  Serveurs ThinkSystem avec XCC version 2.1 et versions suivantes (ThinkSystem SR950 requiert XCC version 1.4 ou suivante), vous pouvez également indiquer le numéro d'emplacement de l'adaptateur RAID et les numéros de baie d'unité pour créer un seul volume en utilisant la capacité de grappe disponible. Dans ce cas, le niveau RAID 0, 1, 5, 6, 10, 50, 60 et 00 sont pris en charge. En outre, vous pouvez choisir des paramètres de volume avancés, tels que la taille des segments, les stratégies et les unités de secours.

  Remarque : Sur le serveur cible, assurez-vous que les unités du type spécifié disponibles sont suffisamment nombreuses, puis vérifiez que l'état RAID des unités est « Non configuré », comme indiqué dans la section **Unités** dans la page Détails d'inventaire des serveurs (voir Affichage des détails d'un serveur géré).
- **Adaptateur de support SD Lenovo**. Choisissez l'emplacement où créer le volume et la taille de volume. Vous pouvez aussi choisir des paramètres de volume avancés, tels que le type de support et la stratégie d'accès.
- **ThinkSystem M.2 avec mise en miroir**. Sélectionnez le niveau RAID de l'emplacement PCI, le nom du volume et la taille des segments pour créer un seul volume à l'aide de la capacité de grappe disponible.

  - Vous pouvez définir plusieurs ThinkSystem M.2 avec des adaptateurs de stockage mis en miroir, chacun dans un emplacement PCI distinct.
  - Pour les serveurs ThinkSystem Edge, vous devez indiquer un numéro d'emplacement PCI spécifique. Pour les autres serveurs ThinkSystem sur lesquels un seul adaptateur RAID M.2 est installé, vous pouvez choisir la première correspondance (valeur par défaut) ou indiquer un numéro d'emplacement PCI spécifique.
- **Mémoire persistante Intel Optane DC**. Sélectionnez le type de mémoire persistante, le seuil d'alerte pour le pourcentage de capacité restante et le pourcentage de la capacité totale à utiliser en tant que mémoire. (La mémoire restante sera utilisée comme stockage persistant).

  Attention :
  - Pour configurer les modules de mémoire DIMM persistante Intel Optane DC, la sécurité doit être désactivée ou aucun espace de nom ne doit être créé.
  - L'activation de la sécurité est uniquement prise en charge lorsque l'état de sécurité est défini sur « Désactivé » pour tous les modules de mémoire DIMM persistante Intel Optane DC du serveur.
  - La désactivation de la sécurité et de l'effacement sécurisé sont uniquement pris en charge lorsque l'état de sécurité est défini sur « Verrouillé » et que la phrase passe est la même pour tous les modules de mémoire DIMM persistante Intel Optane DC du serveur.
  - L'état de sécurité Intel Optane DC PMEM n'est pas inclus dans l'inventaire XClarity Administrator. Vous pouvez vérifier manuellement l'état de la sécurité dans UEFI.

- **Conserver la configuration de stockage existante sur la cible**. La configuration de stockage existante n'est pas modifiée lors du déploiement. Choisissez cette option pour utiliser la configuration de stockage qui est déjà en place sur le serveur cible.
- **Désactiver le disque local**. (Nœud de traitement x240 Flex System uniquement) Le contrôleur de stockage intégré et la mémoire morte en option du stockage (à la fois UEFI et héritée) sont

désactivés pendant le déploiement. La désactivation de l'unité de disque locale diminue la durée d'initialisation globale en démarrant à partir d'un réseau SAN.

Définition de cartes d’E-S

Vous pouvez définir les paramètres de port d'E-S et le mode d'adressage à appliquer aux serveurs cibles lors du déploiement de ce modèle.

À propos de cette tâche

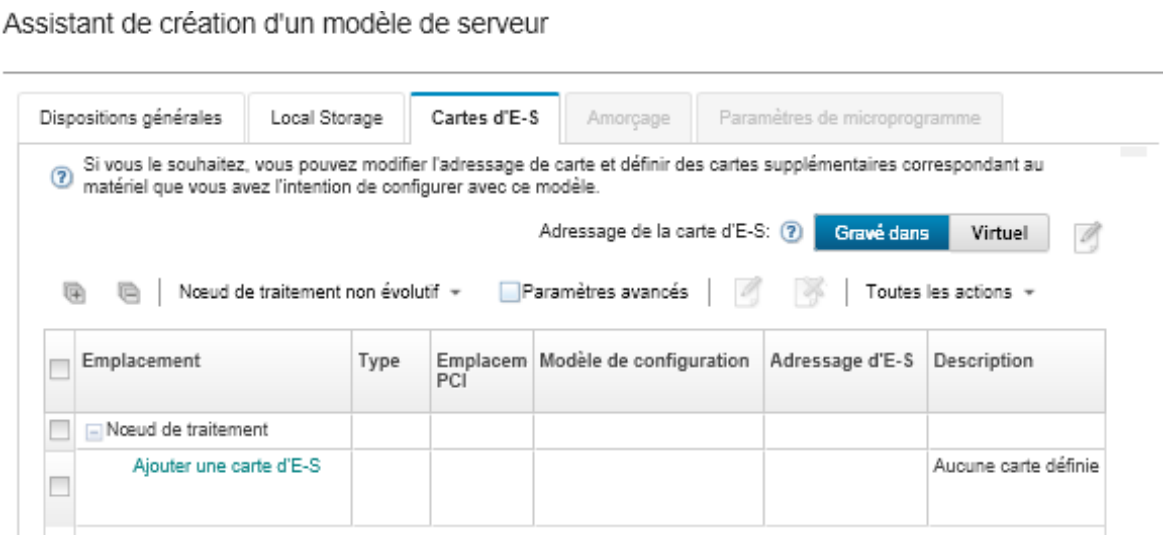
Si vous avez l'intention de virtualiser ou de réattribuer vos adresses de carte d’E-S, vous pouvez configurer ce modèle pour l'utilisation de l'adressage de carte d’E-S virtuelle.

Si vous créez un modèle à partir d'un serveur existant, certaines informations de carte peuvent être récupérées automatiquement. Vous pouvez définir des modèles de cartes d’E-S supplémentaires correspondant au matériel que vous avez l'intention d'utiliser sur les serveurs lors du déploiement de ce modèle. En définissant des modèles de cartes d’E-S, vous pouvez configurer des paramètres de port de carte pour votre carte prise en charge. Si vous utilisez des adresses de carte d’E-S virtuelles, vous pouvez également définir des cibles d'amorçage SAN pour les cartes Fibre Channel que vous ajoutez (voir Définition d'options d'amorçage).

Procédure

Pour définir des paramètres de carte d’E-S, procédez comme suit.

Etape 1. Dans l'Assistant de création d'un modèle serveur, cliquez sur l'onglet **Cartes d’E-S**.



Remarque : Vous pouvez afficher des informations supplémentaires relatives aux cartes d’E-S en cliquant sur **Paramètres avancés**.

Etape 2. Si vous créez un modèle de serveur pour un serveur dans un châssis Flex System, choisissez le type de mode d'adressage de carte d’E-S :

- **Gravé dans**. Utilisez des adresses WWN (World Wide Name) et MAC (Media Access Control) existantes fournies avec la carte par le fabricant.
- **Virtuel**. Utilisez l'adressage de carte d’E-S virtuelle pour simplifier la gestion des connexions SAN et LAN. La virtualisation des adresses d'E-S réaffecte les adresses matérielles gravées avec des adresses MAC Ethernet et Fibre Channel WWN virtualisées. Cela peut accélérer le déploiement en préconfigurant l'appartenance à la zone SAN et en facilitant le basculement

grâce à la suppression de la nécessité de reconfigurer les affectations de la segmentation SAN et du masquage LUN lors d'un remplacement de matériel.

Lorsque l'adressage virtuel est activé, les adresses Ethernet et Fibre Channel sont allouées par défaut indépendamment des adaptateurs définis. Vous pouvez choisir le pool à partir duquel les adresses Ethernet et Fibre Channel sont allouées.

Vous pouvez également modifier les paramètres d'adresse virtuelle en cliquant sur l'icône **Éditer** () en regard des modes d'adresse.

Restriction : L'adressage virtuel est pris en charge uniquement pour les serveurs dans les châssis Flex System. Les serveurs rack et au format tour ne sont pas pris en charge.

Etape 3. Si vous créez un modèle de serveur pour un serveur dans un châssis Flex System, sélectionnez l'une des options d'évolutivité suivantes. Les lignes affichées dans la table changent en fonction de ce qui est sélectionné.
- Flex System non évolutif
- Flex System évolutif à 2 nœuds
- Flex System évolutif à 4 nœuds

Etape 4. Choisissez les cartes d'E-S qui doivent être installées sur les serveurs sur lesquels le modèle doit être déployé. Pour ajouter une carte :

a. Cliquez sur le lien **Ajouter une carte d'E-S** dans la table pour afficher la boîte de dialogue Ajouter carte d'E-S 1 ou LOM.

b. Sélectionnez l'emplacement PCI correspondant à la carte.

c. Sélectionnez le type de carte dans la table.

Remarque : Par défaut, la table répertorie uniquement les cartes d'E-S qui sont actuellement installées sur les serveurs gérés. Pour répertorier toutes les cartes d'E-S prises en charge, cliquez sur **Toutes les cartes prises en charge**.

d. Sélectionnez le modèle de port initial à affecter à tous les ports du groupe de ports lors du déploiement du modèle.

Les *modèles de port* sont utilisés pour modifier des paramètres de port obtenus à partir du serveur. Ces modèles de port initiaux sont affectés lors de l'ajout initial de la carte. Une fois la carte ajoutée, vous pouvez affecter des modèles différents à des ports individuels à partir de la page relative à la carte d'E-S.

Vous pouvez créer un modèle de port en cliquant sur l'icône **Créer** (). Vous pouvez créer un modèle de port basé sur un modèle existant en cliquant sur l'icône **Éditer** ().

Pour plus d'informations sur les modèles de port, voir Définition de paramètres de ports.

e. Cliquez sur **Ajouter** pour ajouter le modèle de port à la table affichée dans la page relative à la carte d'E-S.

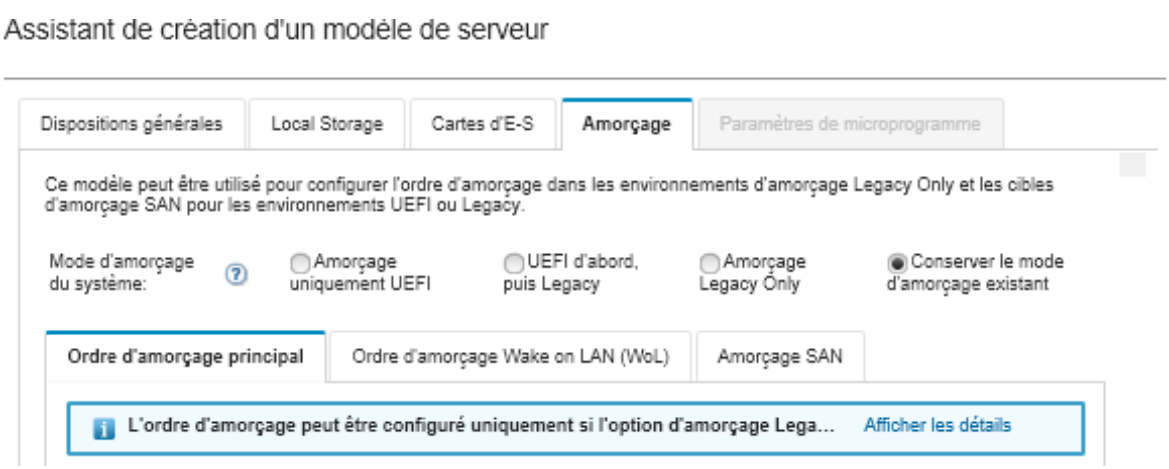
Définition d'options d'amorçage

Vous pouvez définir l'ordre d'amorçage à appliquer aux serveurs cibles lorsque ce modèle est déployé.

Procédure

Pour créer un modèle d'options d'amorçage, procédez comme suit.

Etape 1. Depuis l'Assistant de création d'un modèle serveur, cliquez sur l'onglet **Amorçage**.



Etape 2. Sélectionnez l'un des modes d'amorçage système suivants :

- **Amorçage uniquement UEFI**. Sélectionnez cette option pour configurer un serveur qui prend en charge l'interface UEFI (Unified Extensible Firmware Interface). Si vous amorcez les systèmes d'exploitation UEFI, cette option peut réduire le temps d'amorçage en désactivant les mémoires ROM en option existantes.

  Si le modèle est appris à partir d'un serveur Thinksystem, vous pouvez cliquer sur l'onglet **Ordre d'amorçage principal** pour spécifier l'ordre d'amorçage. Vous pouvez conserver l'ordre d'amorçage spécifié sur le serveur sur lequel le modèle doit être déployé, ou configurer l'ordre d'amorçage afin d'indiquer l'ordre dans lequel les options d'amorçage doivent être appliquées. Toutefois, la priorité d'amorçage des dispositifs d'amorçage dans un groupe d'appareils (option d'amorçage) n'est pas prise en charge.

- **UEFI d'abord, puis Legacy**. Sélectionnez cette option pour configurer un serveur qui essaie d'amorcer avec UEFI en premier. En cas de problème, le serveur essaie d'amorcer en mode Legacy.

  Si le modèle est appris à partir d'un serveur Thinksystem, vous pouvez cliquer sur l'onglet **Ordre d'amorçage principal** pour spécifier l'ordre d'amorçage. Vous pouvez conserver l'ordre d'amorçage spécifié sur le serveur sur lequel le modèle doit être déployé, ou configurer l'ordre d'amorçage afin d'indiquer l'ordre dans lequel les options d'amorçage doivent être appliquées. Toutefois, la priorité d'amorçage des dispositifs d'amorçage dans un groupe d'appareils (option d'amorçage) n'est pas prise en charge.

- **Amorçage Legacy only**. Sélectionnez cette option si vous configurez un serveur qui amorce un système d'exploitation nécessitant le microprogramme (BIOS) existant. Sélectionnez cette option uniquement si vous amorcez des systèmes d'exploitation non compatibles UEFI.

  Astuce : Si vous sélectionnez le mode d'amorçage Legacy Only (qui accélère la durée d'amorçage), vous ne pouvez activer aucune clé FoD (Features on Demand).

  Si vous choisissez cette option, vous pouvez spécifier :

  – **Ordre d'amorçage principal**. Choisissez de conserver l'ordre d'amorçage indiqué sur le serveur sur lequel le modèle doit être déployé. Vous pouvez aussi choisir de configurer l'ordre d'amorçage Legacy Only pour indiquer l'ordre dans lequel les options d'amorçage doivent être appliquées.

  – **Ordre d'amorçage Wake on LAN (WoL)**. Choisissez de conserver l'ordre d'amorçage WoL actuellement indiqué sur le serveur sur lequel le modèle doit être déployé. Vous pouvez aussi choisir de configurer l'ordre d'amorçage Legacy Only pour indiquer l'ordre dans lequel les options d'amorçage WoL doivent être appliquées.

- **Conserver le mode d'amorçage existant**. Sélectionnez cette option pour conserver les paramètres existants sur le serveur cible. Aucune modification de l'ordre d'amorçage n'est apportée lors du déploiement du modèle.

Etape 3. Sélectionnez l'onglet **Amorçage SAN** pour choisir un modèle cible d'amorçage et spécifier des cibles de dispositif d'amorçage.

Remarque : Si vous avez défini des cartes Fibre et activé l'adressage virtuel lors de la définition des cartes d'E-S, vous pouvez définir des cibles d'amorçage principales et secondaires SAN pour les cartes Fibre Channel. Vous pouvez spécifier plusieurs identificateurs WWPN et LUN pour les cibles de stockage.

Définition de paramètres de microprogramme

Vous pouvez spécifier les paramètres de contrôleur de gestion de la carte mère et de microprogramme UEFI à appliquer aux serveurs cibles lors du déploiement de ce modèle.

À propos de cette tâche

Les paramètres de microprogramme sont organisés en catégories qui regroupent des paramètres associés. Pour chaque catégorie, vous pouvez créer un *modèle de catégorie* qui contient les paramètres de microprogramme communs pouvant être réutilisés par plusieurs modèles de serveur. La plupart des paramètres de microprogramme que vous pouvez configurer directement sur le contrôleur de gestion de la carte mère et l'interface UEFI peuvent également être configurés via des modèles de catégorie. Les paramètres de microprogramme disponibles dépendent du type de serveur, de votre environnement Flex System, ainsi que de la portée du modèle de serveur.

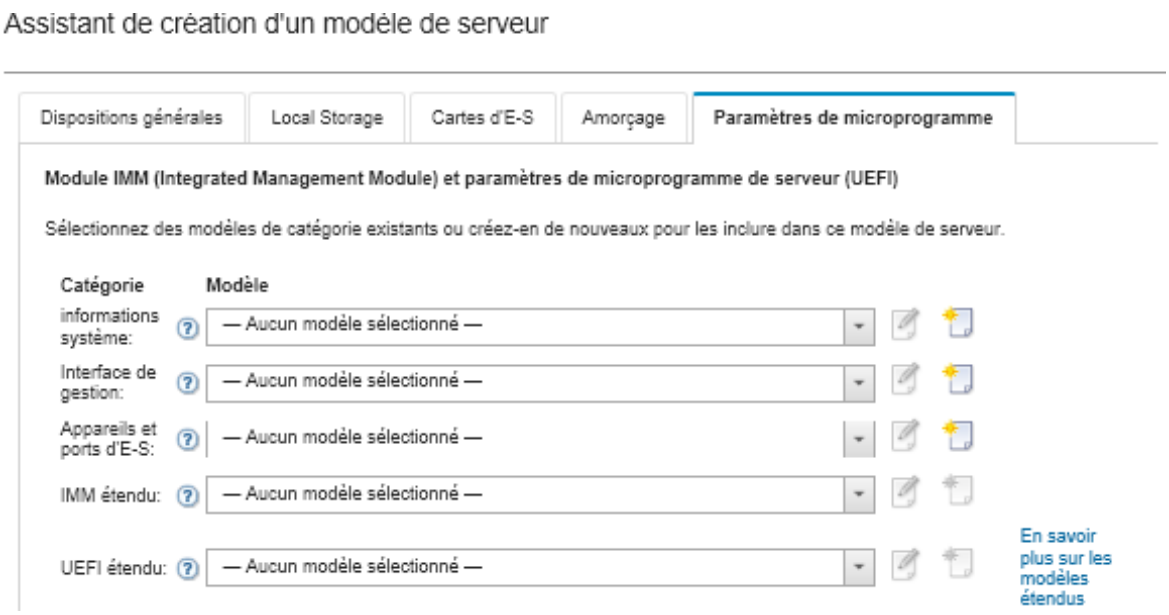
Les modèles de catégorie peuvent être prédéfinis, définis par l'utilisateur ou obtenus à partir de serveurs existants :

- Les *modèles de catégorie étendus* sont des modèles pour certains ports de carte d'E-S, l'interface UEFI (Unified Extensible Firmware Interface) avancée et les paramètres de contrôleur de gestion de la carte mère qui sont obtenus et créés de façon dynamique à partir d'un serveur géré spécifique. Lenovo XClarity Administrator crée ces modèles lorsque vous créez un modèle de serveur à partir d'un serveur existant. Vous ne pouvez pas créer manuellement des modèles de catégorie étendus. Toutefois, vous pouvez éditer les modèles une fois qu'ils sont créés.
- Les *modèles de catégorie définis par l'utilisateur* sont des modèles que vous pouvez créer, en y incluant des informations système, des interfaces de gestion, des appareils et des ports d'E-S, des cibles d'amorçage Fibre Channel, ainsi que des ports de carte d'E-S.

Procédure

Pour définir des paramètres de microprogramme, procédez comme suit.

Etape 1. Dans l'Assistant de création d'un modèle serveur, cliquez sur l'onglet **Paramètres de microprogramme**.



Etape 2. Choisissez le type de modèle de catégorie qui inclut les paramètres que vous voulez définir.

- **Informations système**. Utilisez ce modèle de catégorie pour définir la génération automatique du nom du système, les noms de contact et emplacements. Pour plus d'informations sur les modèles d'informations système, voir Définition de paramètres d'informations système.
- **Interfaces de gestion**. Utilisez ce modèle de catégorie pour définir la génération automatique du nom d'hôte, les affectations d'adresses IP de gestion, les paramètres Domain Name System (DNS) et les paramètres de vitesse Internet. Pour plus d'informations sur les modèles d'interfaces de gestion, voir Définition de paramètres d'interface de gestion.
- **Appareils et ports d'E-S**. Utilisez ce modèle de catégorie pour définir la redirection de la console et les ports COM, la vitesse PCIe, les dispositifs intégrés, la mémoire ROM en option de la carte et l'ordre d'exécution de la mémoire ROM en option. Pour plus d'informations sur les modèles d'appareils et ports d'E-S, voir Définition de paramètres d'appareils et de ports d'E-S.
- **BMC étendu**. Utilisez ce modèle de catégorie pour définir d'autres paramètres de contrôleur de gestion de la carte mère. Les modèles de contrôleur de gestion étendus sont automatiquement créés lorsque vous créez un modèle de serveur à partir d'un serveur existant. Vous ne pouvez pas créer manuellement un modèle de contrôleur de gestion étendu. Pour plus d'informations sur les modèles d'interfaces de gestion, voir Définition de paramètres de contrôleur de gestion étendus.).
- **UEFI étendu**. Utilisez ce modèle de catégorie pour définir d'autres paramètres UEFI (Unified Extensible Firmware Interface). Les modèles UEFI étendu sont automatiquement créés lorsque vous créez un modèle de serveur à partir d'un serveur existant. Vous ne pouvez pas créer manuellement un modèle UEFI étendu. Pour plus d'informations sur les modèles d'interfaces de gestion, voir Définition de paramètres UEFI étendu.

Etape 3. Pour créer des modèles de catégorie, cliquez sur l'icône **Créer** ( ) en regard du type de modèle de catégorie souhaité.

Vous pouvez également modifier un modèle de catégorie existant en sélectionnant un modèle spécifique dans la liste déroulante, puis en cliquant sur l'icône **Éditer** ( ) en regard du type de modèle de catégorie correspondant. Vous pouvez également copier un modèle de catégorie existant en modifiant le modèle, puis en cliquant sur **Enregistrer sous** pour l'enregistrer sous un nouveau nom.

Définition de paramètres d'informations système

Vous pouvez définir les informations relatives au nom de système, au contact et à l'emplacement lors de la création d'un modèle d'informations système.

Procédure

Pour créer un modèle d'informations système, procédez comme suit.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Distribution → Modèles**. La page Modèles de configuration : Modèles s'affiche.

Etape 2. Cliquez sur l'onglet **Modèles de catégorie**.

Etape 3. Cliquez sur l'onglet vertical **Modèles d'informations système**, puis cliquez sur l'icône **Créer** ( ).

Conseil : Vous pouvez également créer un nouveau modèle d'informations système depuis la page Paramètres de microprogramme de l'assistant Nouveau modèle de serveur en cliquant sur l'icône **Créer** en regard de la sélection **Informations système**.

Etape 4. Dans la boîte de dialogue Nouveau modèle d'informations système, indiquez les informations suivantes.

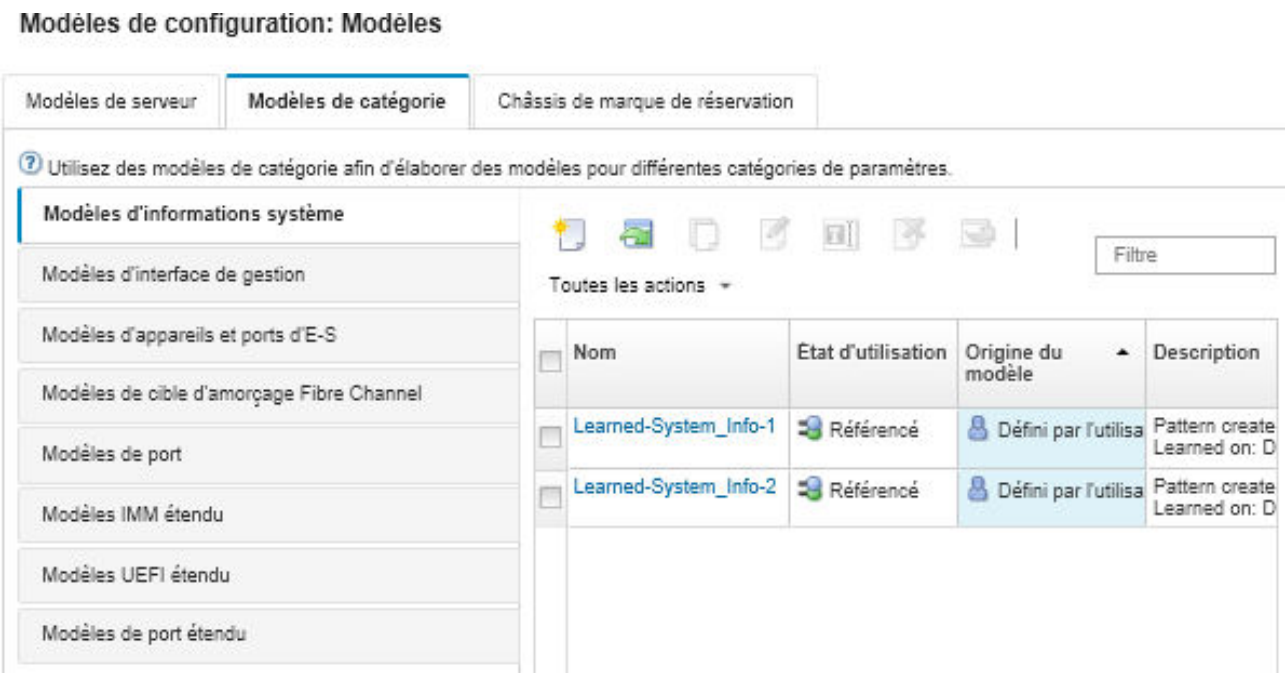
- Entrez un nom et une description pour le modèle.
- Indiquez si générer les noms de système doivent être générés automatiquement. Si vous cliquez sur **Personnalisé**, vous pouvez spécifier comment les noms doivent être générés lorsque le modèle est déployé. Si vous cliquez sur **Désactiver**, le nom du système demeure inchangé sur chaque serveur lorsque le modèle est déployé. Pour la plupart des appareils, le nom est limité à 256 caractères anglais par le contrôleur de gestion de la carte mère. Les noms générés automatiquement sont tronqués à 256 caractères.
- Indiquez la personne à contacter pour ce serveur et l'emplacement du serveur.

  Remarque : Si SNMP est activé, vous devez spécifier un contact et un emplacement système.

Etape 5. Cliquez sur **Créer**.

Résultats

Le nouveau modèle est répertorié sous l'onglet **Modèles d'informations système** dans la page Modèles de configuration : Modèle de catégorie :



Depuis cette page, vous pouvez aussi exécuter les actions suivantes sur un modèle de catégorie sélectionné :

- Modifiez les paramètres de modèle en cours en cliquant sur l'icône **Éditer** ( ).
- Copiez un modèle existant en cliquant sur l'icône **Copier** ( ).
- Supprimez un modèle en cliquant sur l'icône **Supprimer** ( ).
- Renommez un modèle en cliquant sur l'icône **Renommer** ( ).
- Importez et exportez des modèles (voir Exportation et importation de modèles de serveur et de catégorie).

Définition de paramètres d'interface de gestion

Vous pouvez définir les noms d'hôte, l'adresse IP, le système DNS (Domain Name System), la vitesse d'interface et les affectations de port pour l'interface de gestion en créant un modèle d'interface de gestion.

Procédure

Pour créer un modèle d'interface de gestion, procédez comme suit.

Remarque : Les paramètres duplex ne sont pas pris en charge par les modèles de serveur.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Distribution → Modèles**. La page Modèles de configuration : Modèles s'affiche.

Etape 2. Cliquez sur l'onglet **Modèles de catégorie**.

Etape 3. Cliquez sur l'onglet vertical **Modèles d'interface de gestion**, puis cliquez sur l'icône **Créer** ( ).

Conseil : Vous pouvez également créer une nouvelle interface de gestion depuis la page Paramètres de microprogramme de l'assistant Nouveau modèle de serveur en cliquant sur l'icône **Créer** ( ) en regard de la sélection **Interface de gestion**.

Etape 4. Dans la boîte de dialogue Nouveau modèle d'interface de gestion, indiquez les informations suivantes.

- Entrez un nom et une description pour le modèle.

- Cliquez sur l'onglet **Nom d'hôte**, puis indiquez si les noms d'hôte doivent être générés automatiquement. Si vous cliquez sur **Personnalisé**, vous pouvez spécifier comment les noms doivent être générés lorsque le modèle est déployé. Si vous cliquez sur **Désactiver**, le nom d'hôte demeure inchangé sur chaque serveur lorsque le modèle est déployé.

  Les noms d'hôte sont limités à 63 caractères anglais par le contrôleur de gestion de la carte mère. Les noms générés automatiquement sont tronqués à 63 caractères.
- Cliquez sur l'onglet **Adresses IP de gestion**, puis configurez les paramètres d'adresse IPv4 et IPv6.

  Pour les adresses **IPv4**, vous pouvez choisir l'une des options suivantes :
  - **Obtenir une adresse IP dynamique du serveur DHCP**.
  - **Tout d'abord par DHCP**. Si cela échoue, obtenez une adresse IP statique depuis le pool d'adresses.
  - **Obtenez une adresse IP statique depuis le pool d'adresses.**

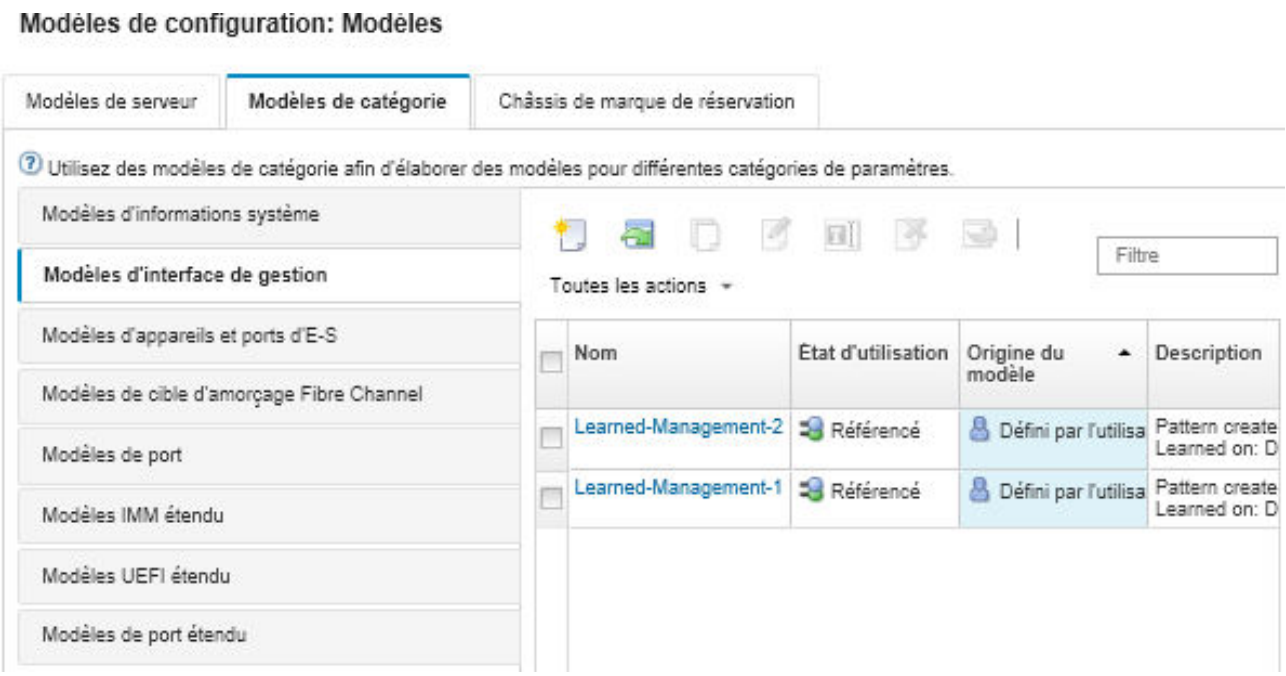
  Pour les adresses **IPv6**, vous pouvez choisir de :
  - **Utiliser la configuration automatique d'adresse sans état**.
  - **Obtenir une adresse IP dynamique depuis un serveur DHCP**.
  - **Obtenir une adresse IP statique du pool d'adresses IP**.

  Sous l'onglet **Domain Name System (DNS)**, choisissez d'activer ou de désactiver Dynamic Domain Name Services (DDNS). Si vous activez DDNS, vous pouvez choisir l'une des options suivantes :
  - Obtenir le nom de domaine d'un serveur DHCP.
  - Spécifiez un nom de domaine.
- Cliquez sur l'onglet **Paramètres d'interface**, puis indiquez l'unité MTU (unité de transmission maximale). La valeur par défaut est 1500.
- Cliquez sur l'onglet **Affectations de port**, puis indiquez les numéros à utiliser pour les ports suivants :
  - HTTP
  - HTTPS
  - CLI Telnet
  - CLI SSH
  - Agent SNMP
  - Alertes SNMP
  - Console de contrôle à distance
  - CIM via HTTP
  - CIM via HTTPS

Etape 5. Cliquez sur **Créer**.

Résultats

Le nouveau modèle est répertorié sous l'onglet **Modèles d'interface de gestion** dans la page Modèles de configuration : Modèle de catégorie :



Depuis cette page, vous pouvez aussi exécuter les actions suivantes sur un modèle de catégorie sélectionné :

- Modifiez les paramètres de modèle en cours en cliquant sur l'icône **Éditer** ( ).
- Copiez un modèle existant en cliquant sur l'icône **Copier** ( ).
- Supprimez un modèle en cliquant sur l'icône **Supprimer** ( ).
- Renommez un modèle en cliquant sur l'icône **Renommer** ( ).
- Importez et exportez des modèles (voir Exportation et importation de modèles de serveur et de catégorie).

Définition de paramètres d'appareils et de ports d'E-S

Vous pouvez activer la redirection de console, puis activer et définir les caractéristiques du port COM 1 en créant un modèle Appareils et ports d'E-S.

Procédure

Pour créer un modèle Appareil et ports d'E-S, procédez comme suit.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Distribution → Modèles**. La page Modèles de configuration : Modèles s'affiche.

Etape 2. Cliquez sur l'onglet **Modèles de catégorie**.

Etape 3. Cliquez sur l'onglet vertical **Modèles d'appareil et de ports d'E-S**, puis cliquez sur l'icône **Créer** ( ).

Conseil : Vous pouvez également créer un modèle d'appareils et de ports d'E-S depuis la page Paramètres de microprogramme de l'assistant Nouveau modèle de serveur en cliquant sur l'icône **Créer** ( ) en regard de la sélection **Appareils et ports d'E-S**.

Etape 4. Dans la boîte de dialogue Nouveaux modèles d'appareils et de ports d'E-S, indiquez les informations suivantes.

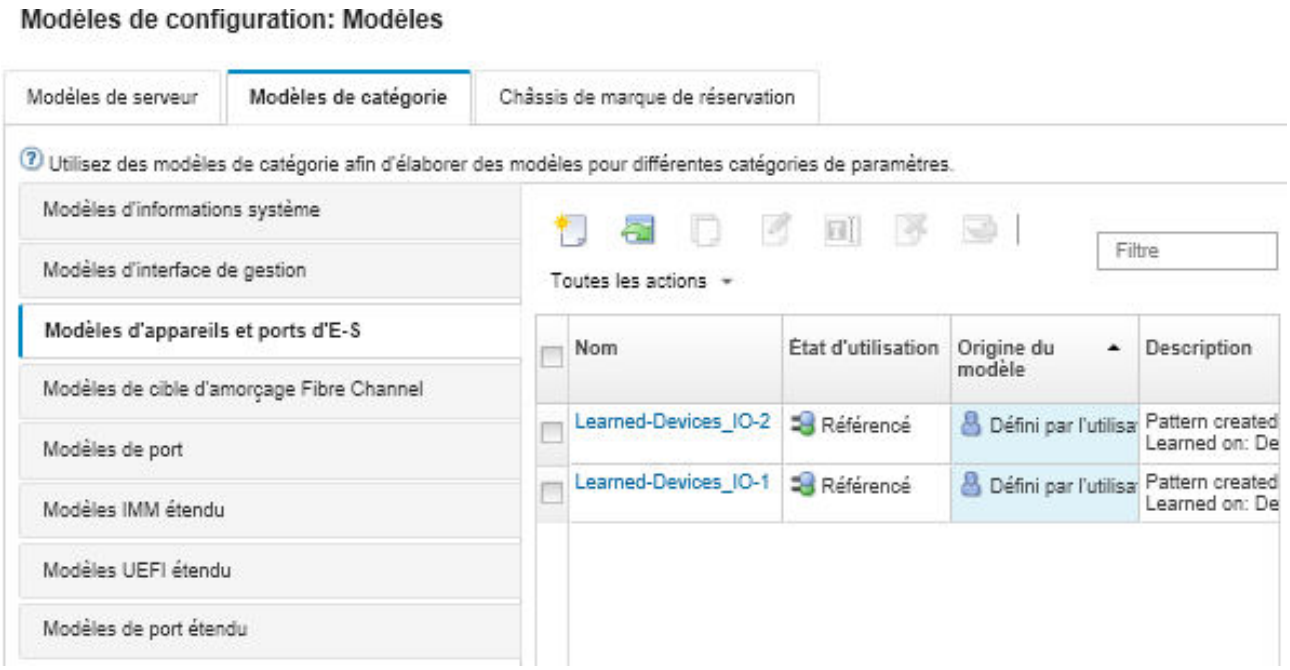
- Entrez un nom et une description pour le modèle.
- Choisissez d'activer ou de désactiver la redirection de console. Si vous activez la redirection de la console, vous pouvez choisir d'activer ou de désactiver ce qui suit :

  - **Serial over LAN**.
  - **Réacheminement du processeur de maintenance**. Si vous activez le réacheminement du processeur de maintenance, vous pouvez choisir d'utiliser le port COM 1 ou 2 pour le port de données en option existant. Notez que si cette option est désactivée, le port COM 1 est toujours utilisé.Vous pouvez aussi choisir l'un des modes CLI suivants :
    - Désactiver
    - Activer avec une séquence de touches définies par l'utilisateur
    - Activer avec une séquence de touches compatible EMS
- Choisissez d'activer ou de désactiver les ports COM 1 et 2. Si vous choisissez d'activer les ports COM, indiquez les paramètres suivants :
  - Débit en bauds
  - Bits de données
  - Parity
  - Bits d'arrêt
  - Émulation de texte
  - Activer après amorçage
  - Contrôle du flux

Etape 5. Cliquez sur **Créer**.

Résultats

Le nouveau modèle est répertorié sous l'onglet **Modèle d'appareil et de ports d'E-S** dans la page Modèles de configuration : Modèle de catégorie :



Depuis cette page, vous pouvez aussi exécuter les actions suivantes sur un modèle de catégorie sélectionné :

- Modifiez les paramètres de modèle en cours en cliquant sur l'icône **Éditer** ( ).
- Copiez un modèle existant en cliquant sur l'icône **Copier** ( ).
- Supprimez un modèle en cliquant sur l'icône **Supprimer** ( ).
- Renommez un modèle en cliquant sur l'icône **Renommer** ( ).

- Importez et exportez des modèles (voir Exportation et importation de modèles de serveur et de catégorie).

Définition de paramètres de cible d'amorçage Fibre Channel

Vous pouvez configurer le serveur afin qu'il s'amorce depuis un dispositif de réseau de stockage (SAN) au lieu d'une unité de disque local en créant un modèle cible d'amorçage Fibre Channel.

Procédure

Pour créer un modèle de cible d'amorçage Fibre Channel, procédez comme suit.

Restriction : Les cibles d'amorçage Fibre Channel sont prises en charge pour les nœuds de traitement Flex seulement. Les serveurs rack et au format tour autonomes ne sont pas pris en charge.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Distribution → Modèles**. La page Modèles de configuration : Modèles s'affiche.

Etape 2. Cliquez sur l'onglet **Modèles de catégorie**.

Etape 3. Cliquez sur l'onglet vertical **Modèles de cible d'amorçage Fibre Channel**, puis sur l'icône **Créer** ( ).

Etape 4. Dans la boîte de dialogue Nouveau modèle de cible d'amorçage Fibre Channel, indiquez les informations suivantes.

- Entrez un nom et une description pour le modèle.
- Spécifiez une ou plusieurs adresses WWPN et identificateurs d'unité logique à utiliser en tant que cibles d'amorçage. En outre, vous pouvez aussi spécifier une ou plusieurs adresses WWPN et identificateurs d'unité logique à utiliser en tant que cibles d'amorçage secondaires.

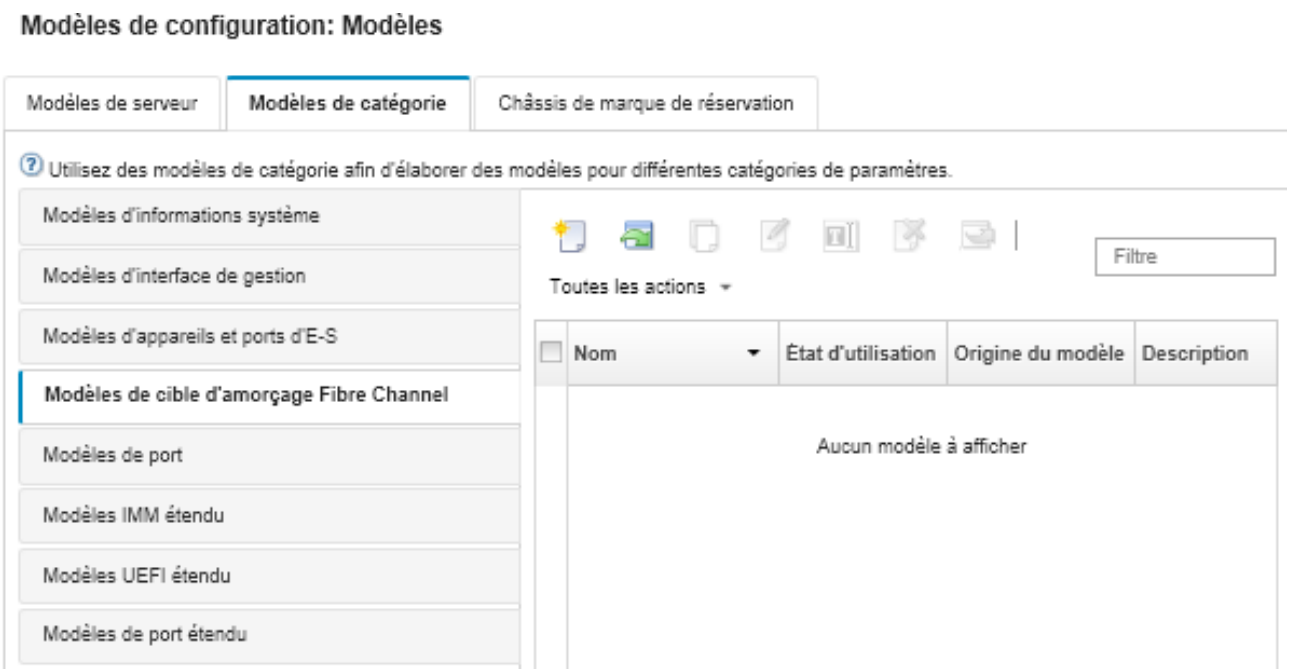
  Par exemple, vous pouvez ajouter des chemins principaux de stockage en tant que cibles principales, et des chemins secondaires de stockage en tant que cibles secondaires. Grâce à différents groupes cibles dans différents modèles de serveur, vous pouvez équilibrer la charge de stockage durant les demandes d'amorçage simultanées depuis plusieurs hôtes.

  Conseil : Si vous spécifiez `00:00:00:00:00:00:00:00` pour le WWPN, XClarity Administrator essaie d'amorcer depuis la première cible reconnue.

Etape 5. Cliquez sur **Créer**.

Résultats

Le nouveau modèle est répertorié sous l'onglet **Modèles de cible d'amorçage Fibre Channel** de la page Modèles de configuration : Modèle de catégorie :



Depuis cette page, vous pouvez aussi exécuter les actions suivantes sur un modèle de catégorie sélectionné :

- Modifiez les paramètres de modèle en cours en cliquant sur l'icône **Éditer** ( ).
- Copiez un modèle existant en cliquant sur l'icône **Copier** ( ).
- Supprimez un modèle en cliquant sur l'icône **Supprimer** ( ).
- Renommez un modèle en cliquant sur l'icône **Renommer** ( ).
- Importez et exportez des modèles (voir Exportation et importation de modèles de serveur et de catégorie).

Définition de paramètres de ports

Vous pouvez définir des paramètres de port classiques pour un type de carte d'E-S spécifique en créant un modèle de port.

À propos de cette tâche

Vous pouvez utiliser des paramètres réseau dans les modèles de port afin de configurer des ports internes de commutateur. Cependant, vous ne pouvez pas utiliser des modèles de port pour configurer des paramètres globaux de commutateur, tels que des ID VLAN, le mode UFP global, le mode CEE global et les FIPS globaux. Vous devez configurer manuellement les paramètres globaux à l'aide des règles suivantes qui sont compatibles avec les paramètres des ports internes que vous souhaitez déployer avant de déployer les modèles de port. Vous ne pouvez pas non plus utiliser des modèles de port pour configurer le marquage PVID. Consultez la documentation fournie avec votre commutateur pour déterminer les vérifications de compatibilité entre les paramètres globaux et les paramètres des ports internes et pour plus de détails sur la configuration des paramètres de ce commutateur.

- Vérifiez que **globalCEEState** est défini sur « On » lorsque PFC est configuré.
- Vérifiez que **globalCEEState** est défini sur « On » lorsque vport est défini sur le mode « FCoE ».
- Vérifiez que **globalCEEState** est défini sur « On » et que **globalFIPsState** est défini sur « On » lorsque des FIPs sont configurés.

- Vérifiez que **globalUFPMode** est défini sur « Enable » lorsque le port interne de commutateur est défini sur le mode « UFP ».
- Vérifiez que l'ID VLAN est créé avant d'ajouter un port à un réseau VLAN spécifique.

Procédure

Pour créer un modèle de port de carte d'E-S, procédez comme suit.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Distribution → Modèles**. La page Modèles de configuration : Modèles s'affiche.

Etape 2. Cliquez sur l'onglet **Modèles de catégorie**.

Etape 3. Cliquez sur l'onglet vertical **Modèle de port**, puis cliquez sur l'icône **Créer** ( ).

Conseil : Vous pouvez également créer un nouveau modèle de port depuis la page Ajouter une carte d'E-S en cliquant sur l'icône **Créer** ( ) en regard de la sélection **Modèle de port initial**.

Etape 4. Dans la boîte de dialogue Nouveau modèle de port, indiquez les informations suivantes.

- Entrez un nom et une description pour le modèle.
- Indiquez les paramètres d'adaptateur et de compatibilité de port ci-après. Lors de l'affectation de modèles aux cartes et aux ports, les paramètres de modèle sont filtrés en fonction de la compatibilité avec la carte ou le port cible.
  - Type de carte cible
  - Mode opérationnel de port cible, y compris :
    - Mode pNIC
    - Mode Virtual Fabric vNIC
    - Mode indépendant de commutation vNIC
    - Mode de protocole vNIC Unified Fabric

    Ces paramètres permettent la virtualisation NIC. Pour plus d'informations, voir Virtualisation NIC dans Flex System Fabric Solutions.
  - Protocoles de port cible, notamment :
    - Ethernet seulement
    - Ethernet et FCoE
    - Ethernet et iSCSI
  - Modèle de paramètres étendus de port, qui est utilisé pour configurer des paramètres de port supplémentaires qui sont obtenus du serveur
- Si vous définissez le mode opérationnel de port cible sur **Mode pNIC**, choisissez d'appliquer les paramètres correspondants aux ports internes de commutateur Flex, le cas échéant. Si cette option est sélectionnée, vous pouvez configurer des paramètres VLAN et des paramètres avancés supplémentaires :
  - Indiquez le protocole de port cible.
  - Si vous utilisez le protocole de port cible sur **Ethernet et FCoE**, sélectionnez et indiquez éventuellement l'ID de priorité 2.
- Si vous définissez le mode opérationnel de port cible sur **Mode Virtual Fabric vNIC**, configurez les paramètres de fonction physique, y compris le type et le marquage VLAN pour chaque fonction.
- Si vous définissez le mode opérationnel de port cible sur **Mode indépendant de commutation vNIC**, indiquez le type, la bande passante minimum et le marquage VLAN pour chaque fonction activée. Vous pouvez aussi choisir d'appliquer les paramètres correspondants aux ports internes de commutateur Flex le cas échéant Si cette option est sélectionnée, vous pouvez configurer un port interne de commutateur supplémentaire et des paramètres avancés :

- Indiquez le réseau local par défaut, qui est utilisé uniquement par le système d'exploitation lorsque celui-ci envoie des paquets non marqués.
- Indiquez une liste de réseaux VLAN séparées par des virgules.
- Choisissez de configurer le contrôle manuel et indiquez les déclencheurs.
- Choisissez de configurer le type de contrôle de flux, y compris
  - Conserver le contrôle de flux existant
  - Contrôle de flux basé sur la priorité
  - Contrôle de flux basé sur la liaison

  Pour plus d'informations sur ces types de contrôle de flux, consultez la documentation fournie avec votre commutateur Flex.

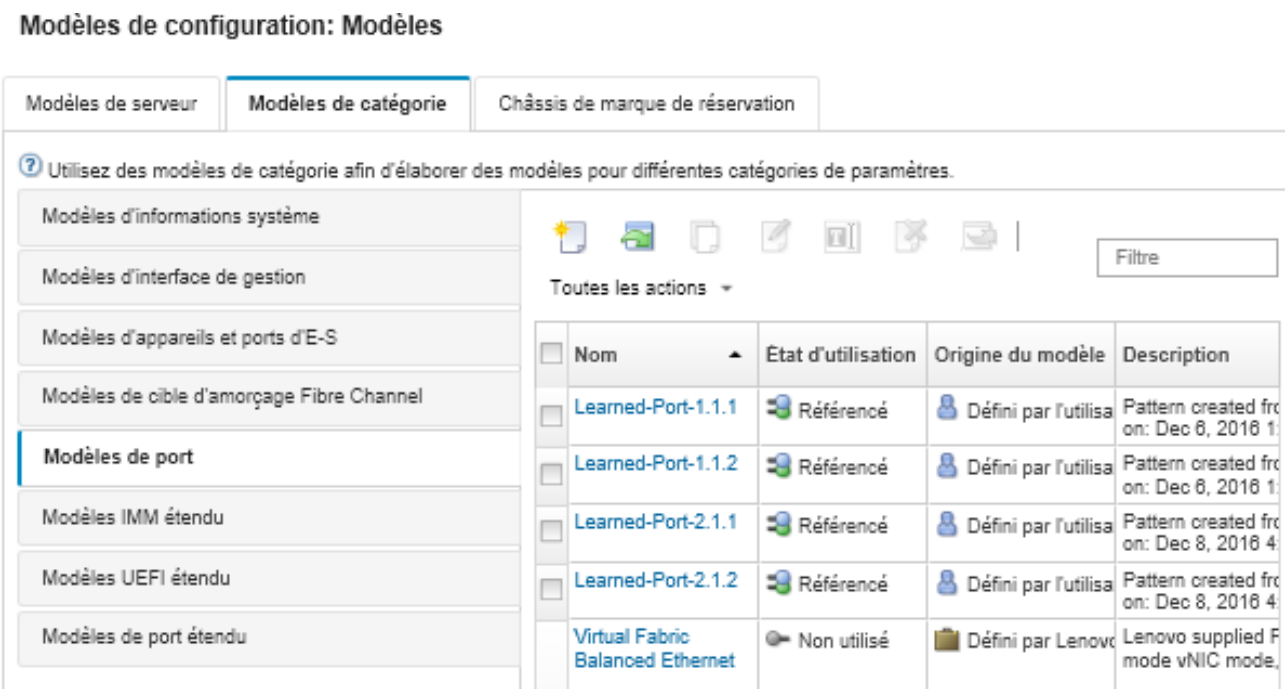
- Si vous définissez le mode opérationnel de port cible sur **Mode de protocole vNIC Unified Fabric**, choisissez d'appliquer les paramètres correspondants aux ports internes de commutateur Flex, le cas échéant. Si cette option est sélectionnée, vous pouvez configurer une fonction UFP et des paramètres avancés supplémentaires :
  - Indiquez le mode QoS (bande passante ou priorité).
  - Choisissez d'activer le marquage d'ID VLAN par défaut et Indiquez le mode, la bande passante minimum et le marquage VLAN pour chaque fonction activée.
  - Choisissez de configurer une défaillance de couche 2 et indiquez le nombre de déclencheurs pour chaque fonction.
  - Pour le mode QoS de la bande passante, indiquez le type de contrôle de flux (basé sur la priorité, le niveau de liaison ou le contrôle de flux existant).
  - Pour le mode QoS de la bande passante, choisissez si la priorité 4 est activé lorsque iSCSI est sélectionné.

  Remarque : Assurez-vous que le basculement global est défini sur « On » en définissant des déclencheurs de basculement.

Etape 5. Cliquez sur **Créer**.

Résultats

Le nouveau modèle est répertorié sous l'onglet **Modèles de port** dans la page Modèles de configuration : Modèle de catégorie :



Depuis cette page, vous pouvez aussi exécuter les actions suivantes sur un modèle de catégorie sélectionné :

- Modifiez les paramètres de modèle en cours en cliquant sur l'icône **Éditer** ( ).
- Copiez un modèle existant en cliquant sur l'icône **Copier** ( ).
- Supprimez un modèle en cliquant sur l'icône **Supprimer** ( ).
- Renommez un modèle en cliquant sur l'icône **Renommer** ( ).
- Importez et exportez des modèles (voir Exportation et importation de modèles de serveur et de catégorie).

Définition de paramètres de contrôleur de gestion étendus

Les paramètres de contrôleur de gestion de la carte mère sont obtenus et créés de façon dynamique à partir d'un serveur géré spécifique. Lenovo XClarity Administrator crée ces modèles lorsque vous créez un modèle de serveur à partir d'un serveur existant. Vous ne pouvez pas créer manuellement des modèles de contrôleur de gestion étendus. Toutefois, vous pouvez copier et modifier les modèles déjà créés.

Avant de commencer

Remarque : Le paramètre thermique du module IMM peut être en conflit avec le paramètre de mode de fonctionnement UEFI. S'il y a conflit, les paramètres UEFI l'emportent sur le paramètre du module IMM au redémarrage de l'appareil. Les paramètres thermiques que vous aurez définis dans un modèle étendu de contrôleur de gestion de la carte mère ne seront plus conformes. Pour résoudre ce problème de non-conformité, supprimez le paramètre du modèle étendu de contrôleur de gestion de la carte mère ou sélectionnez un paramètre qui ne sera pas en conflit avec le paramètre de mode de fonctionnement UEFI en cours.

Procédure

Pour modifier des modèles de contrôleur de gestion étendus, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Modèles**. La page Modèles de configuration : Modèles s'affiche.

Etape 2. Cliquez sur l'onglet **Modèles de catégorie**.

Etape 3. Cliquez sur l'onglet vertical **Modèles BMC étendus**.

Etape 4. Sélectionnez le modèle à modifier, puis cliquez sur l'icône **Éditer** ().

Etape 5. Modifiez les zones appropriées.

Vous pouvez sélectionner les paramètres que vous voulez inclure dans le modèle de catégorie en cliquant sur les paramètres **Inclure/Exclure**.

- Pour configurer les paramètres DNS, cliquez sur **Interface de paramètres réseau → Configuration DNS**. Vous pouvez activer DNS, sélectionner le protocole IP et indiquer jusqu'à trois adresses IPv4 ou IPv6, puis activer la reconnaissance des adresses IP de XClarity Administrator.

  Remarque : Pour les appareils Flex System, vous pouvez configurer uniquement l'adresse IP à utiliser pour reconnaître le serveur XClarity Administrator.

- Pour configurer les paramètres NTP, cliquez sur **Interface de paramètres réseau → Paramètres du module NTP intégré**. Vous pouvez indiquer le nom d'hôte pour un maximum de 4 serveurs NTP et la fréquence.

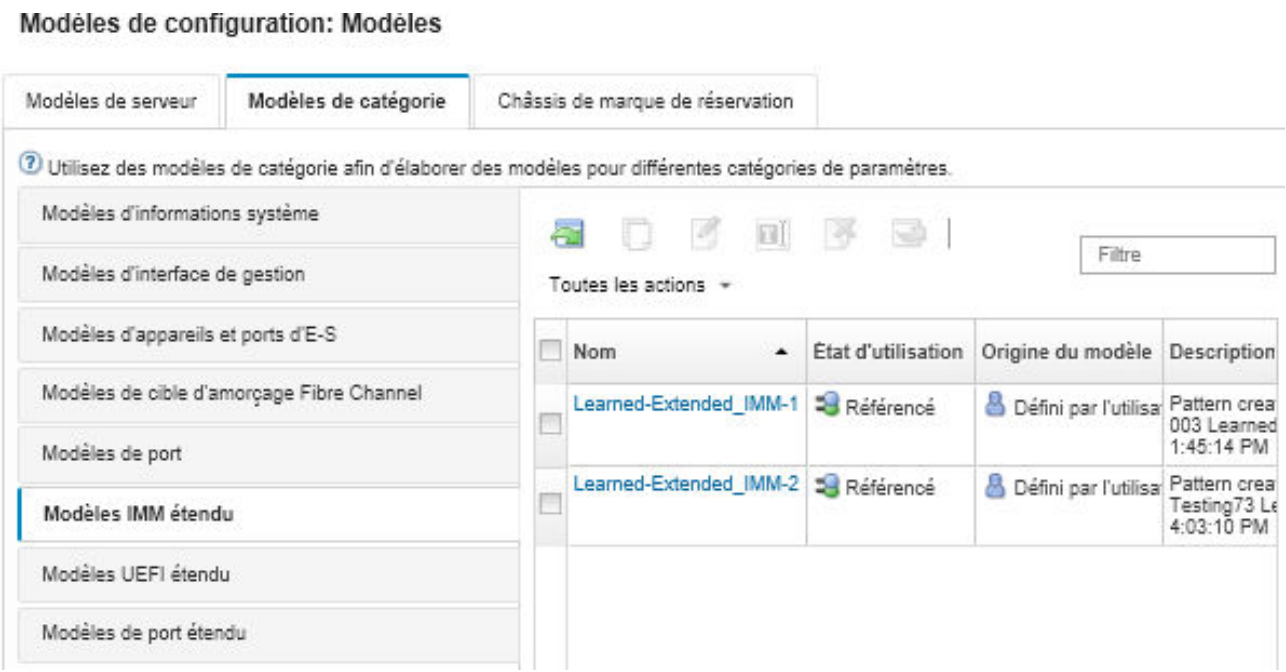
  Remarque : Pour les appareils Flex System, vous ne pouvez pas configurer les paramètres NTP.

- (Serveurs rack uniquement) Sur les paramètres de date et d’heure, cliquez sur **Paramètres généraux → Paramètres d'horloge du module intégré**. Vous pouvez indiquer le fuseau horaire (décalage UTC), activer ou désactiver l’heure d’été (DST), puis choisir d’utiliser ou non l’heure UTC ou l’heure locale sur l’hôte.
- Pour modifier les paramètres de sécurité d'un compte utilisateur, cliquez sur **Configuration de sécurité du compte**.

Etape 6. Cliquez sur **Enregistrer** pour enregistrer les modifications apportées au modèle de catégorie actuel, ou cliquez sur **Enregistrer sous** pour enregistrer les modifications dans un nouveau modèle de catégorie.

Résultats

Le modèle de catégorie modifié est répertorié sous l'onglet **Modèles BMC étendus** dans la page Modèles de configuration : Modèles de catégorie :



Depuis cette page, vous pouvez aussi exécuter les actions suivantes sur un modèle de catégorie sélectionné :

- Copiez un modèle existant en cliquant sur l'icône **Copier** ( ).
- Supprimez un modèle en cliquant sur l'icône **Supprimer** ( ).
- Renommez un modèle en cliquant sur l'icône **Renommer** ( ).
- Importez et exportez des modèles (voir Exportation et importation de modèles de serveur et de catégorie).

Définition de paramètres UEFI étendu

Les paramètres UEFI (Unified Extensible Firmware Interface) étendu sont obtenus et créés de façon dynamique à partir d'un serveur géré spécifique. Lenovo XClarity Administrator crée ces modèles lorsque vous créez un modèle de serveur à partir d'un serveur existant. Vous ne pouvez pas créer manuellement des modèles UEFI étendu. Toutefois, vous pouvez copier et modifier les modèles déjà créés.

À propos de cette tâche

Les modèles UEFI étendu suivants sont prédéfinis par Lenovo XClarity Administrator pour optimiser vos serveurs pour des environnements spécifiques.

- **Options d'installation ESXi**
- **Efficience – Favoriser les performances**
- **Efficience – Favoriser l'énergie**
- **Performance maximale**
- **Energie minimale**

Remarques :

- La modification des paramètres de sécurité UEFI (notamment l'amorçage sécurisé, le module TPM (Trusted Platform Module) et la configuration de stratégie de présence physique) n'est pas prise en charge à l'aide de modèles UEFI étendu.
- Vous pouvez modifier le mot de passe administrateur UEFI de certains serveurs ThinkSystem et ThinkAgile depuis la page Serveurs, en cliquant sur **Toutes les actions → Sécurité → Mot de passe administrateur UEFI**. Le microprogramme Lenovo XClarity Controller doit être au niveau 20A.

Procédure

Pour modifier des modèles UEFI étendu, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Modèles**. La page Modèles de configuration : Modèles s'affiche.

Etape 2. Cliquez sur l'onglet **Modèles de catégorie**.

Etape 3. Cliquez sur l'onglet vertical **Modèles UEFI étendus**.

Etape 4. Sélectionnez le modèle à modifier, puis cliquez sur l'icône **Éditer** ( ).

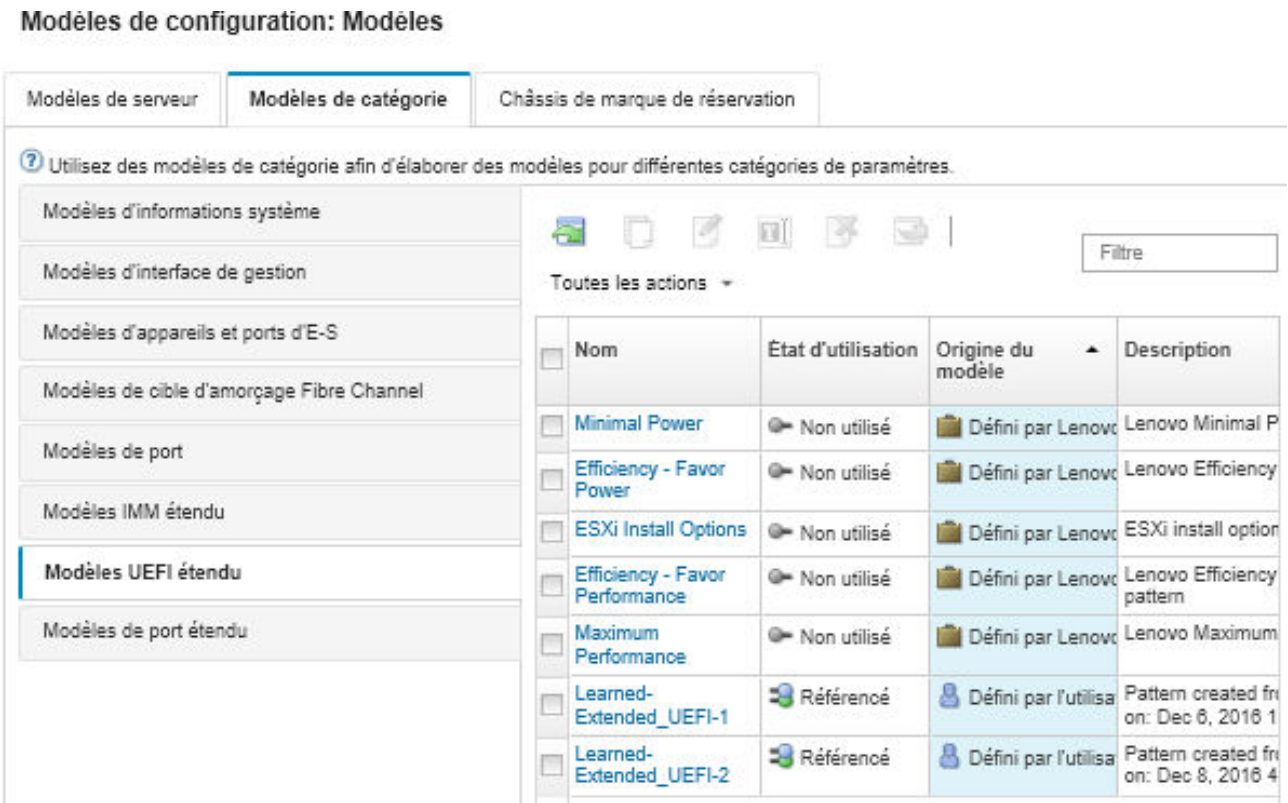
Etape 5. Modifiez les zones appropriées.

Vous pouvez sélectionner les paramètres que vous voulez inclure dans le modèle de catégorie en cliquant sur les paramètres **Inclure/Exclure**.

Etape 6. Cliquez sur **Enregistrer** pour enregistrer les modifications apportées au modèle de catégorie actuel, ou cliquez sur **Enregistrer sous** pour enregistrer les modifications dans un nouveau modèle de catégorie.

Résultats

Le modèle de catégorie modifié est répertorié sous l'onglet **Modèles UEFI étendus** dans la page Modèles de configuration : Modèles de catégorie :



Depuis cette page, vous pouvez aussi exécuter les actions suivantes sur un modèle de catégorie sélectionné :

- Copiez un modèle existant en cliquant sur l'icône **Copier** ( ).
- Supprimez un modèle en cliquant sur l'icône **Supprimer** ( ).
- Renommez un modèle en cliquant sur l'icône **Renommer** ( ).

- Importez et exportez des modèles (voir Exportation et importation de modèles de serveur et de catégorie).

Définition de paramètres de port étendu

Les paramètres de port étendu sont obtenus et créés de façon dynamique à partir d'un serveur géré spécifique. Lenovo XClarity Administrator crée ces modèles lorsque vous créez un modèle de serveur à partir d'un serveur existant. Vous ne pouvez pas créer manuellement des modèles de port étendu. Toutefois, vous pouvez copier et modifier les modèles déjà créés.

À propos de cette tâche

XClarity Administrator fournit le modèle de port étendu prédéfini suivant :

- **Ethernet équilibré Virtual Fabric**. Lenovo a fourni un modèle de port pour le mode Virtual Fabric, le mode vNIC et Ethernet seulement

Certains paramètres de niveau appareil sur les cartes d'E-S Mellanox et Broadcom doivent être configurés avec la même valeur sur tous les ports. Si les paramètres sont définis avec une valeur différente sur les différents ports, les paramètres d'un port sont utilisés et les paramètres des autres ports ne sont pas conformes. Pour résoudre le problème de non conformité, sélectionnez la même valeur pour ces paramètres de niveau appareil.

Pour les cartes d'E-S Mellanox, les paramètres suivants doivent être définis sur tous les ports.
- Paramètres avancés d'alimentation
- Fonctions virtuelles PCI publiées
- Emplacement du limitateur d'alimentation
- Mode virtualisation

Pour les cartes d'E-S Broadcom, les paramètres suivants doivent être définis sur tous les ports.
- Message bannière d'expiration
- Limite BW
- Limite BW valide
- Réservation BW
- Réservation BW valide
- Activer la fonctionnalité PME
- Nombre maximum de vecteurs PF MSI-X
- Mode multifonction
- Nombre de vecteurs MSI-X Vectors par VF
- Nombre de VF par PF
- Option ROM
- SR-IOV
- Support RDMA

Procédure

Pour modifier des modèles de port étendu, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Modèles**. La page Modèles de configuration : Modèles s'affiche.

Etape 2. Cliquez sur l'onglet **Modèles de catégorie**.

Etape 3. Cliquez sur l'onglet vertical **Modèles de port étendu**.

Etape 4. Sélectionnez le modèle à modifier, puis cliquez sur l'icône **Éditer** ( ).

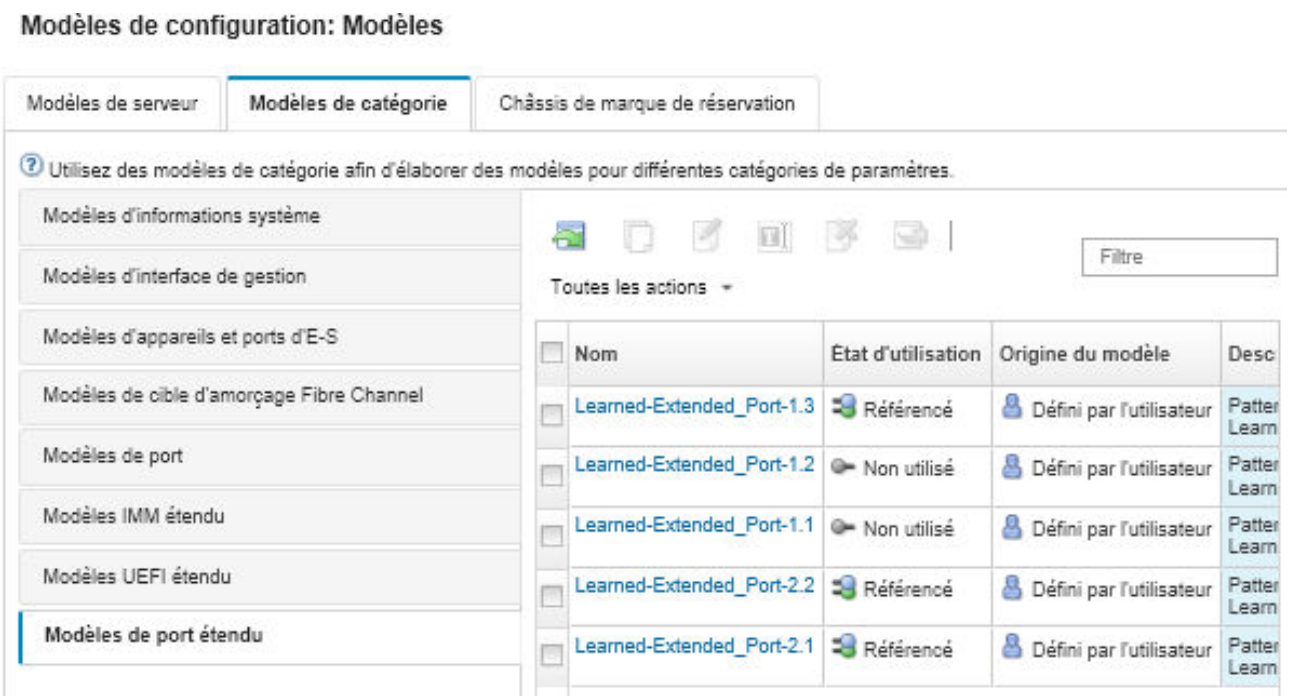
Etape 5. Modifiez les zones appropriées.

Vous pouvez sélectionner les paramètres que vous voulez inclure dans le modèle de catégorie en cliquant sur les paramètres **Inclure/Exclure**.

Etape 6. Cliquez sur **Enregistrer** pour enregistrer les modifications apportées au modèle de catégorie actuel, ou cliquez sur **Enregistrer sous** pour enregistrer les modifications dans un nouveau modèle de catégorie.

Résultats

Le modèle de catégorie modifié est répertorié sous l'onglet **Modèles de port étendu** dans la page Modèles de configuration : Modèles de catégorie :



Depuis cette page, vous pouvez aussi exécuter les actions suivantes sur un modèle de catégorie sélectionné :

- Copiez un modèle existant en cliquant sur l'icône **Copier** ( ).
- Supprimez un modèle en cliquant sur l'icône **Supprimer** ( ).
- Renommez un modèle en cliquant sur l'icône **Renommer** ( ).
- Importez et exportez des modèles (voir Exportation et importation de modèles de serveur et de catégorie).

Définition de paramètres du BIOS SR635/SR655 étendu

Les paramètres du BIOS SR635/SR655 étendu sont obtenus et créés de façon dynamique à partir d'un serveur géré spécifique. Lenovo XClarity Administrator crée ces modèles lorsque vous créez un modèle de serveur à partir d'un serveur ThinkSystem SR635 ou SR655 existant. Vous ne pouvez pas créer manuellement des modèles du BIOS SR635/SR655 étendu. Toutefois, vous pouvez copier et modifier les modèles déjà créés.

Procédure

Pour modifier des modèles du BIOS SR635/SR655 étendu, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Modèles**. La page Modèles de configuration : Modèles s'affiche.

Etape 2. Cliquez sur l'onglet **Modèles de catégorie**.

Etape 3. Cliquez sur l'onglet vertical **Modèles du BIOS SR635/SR655 étendu**.

Etape 4. Sélectionnez le modèle à modifier, puis cliquez sur l'icône **Éditer** ().

Etape 5. Modifiez les zones appropriées.

Vous pouvez sélectionner les paramètres que vous voulez inclure dans le modèle de catégorie en cliquant sur les paramètres **Inclure/Exclure**.

Etape 6. Cliquez sur **Enregistrer** pour enregistrer les modifications apportées au modèle de catégorie actuel, ou cliquez sur **Enregistrer sous** pour enregistrer les modifications dans un nouveau modèle de catégorie.

Résultats

Le modèle de catégorie modifié est répertorié sous l'onglet **Modèles du SR635/SR655 étendu** à la page Modèles de configuration : modèles de catégorie :

Depuis cette page, vous pouvez aussi exécuter les actions suivantes sur un modèle de catégorie sélectionné :

- Copiez un modèle existant en cliquant sur l'icône **Copier** ().
- Supprimez un modèle en cliquant sur l'icône **Supprimer** ().
- Renommez un modèle en cliquant sur l'icône **Renommer** ().
- Importez et exportez des modèles (voir Exportation et importation de modèles de serveur et de catégorie).

Définition des paramètres de BIOS ThinkServer CPlus étendus

Les paramètres de BIOS ThinkServer CPlus étendus sont obtenus et créés de façon dynamique à partir d'un serveur géré spécifique. Lenovo XClarity Administrator crée ces modèles lorsque vous créez un modèle de serveur à partir d'un serveur ThinkServer CPlus existant. Vous ne pouvez pas créer manuellement des modèles de BIOS ThinkServer CPlus étendus. Toutefois, vous pouvez copier et modifier les modèles déjà créés.

Procédure

Pour modifier des modèles de BIOS ThinkServer CPlus étendus, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Modèles**. La page Modèles de configuration : Modèles s'affiche.

Etape 2. Cliquez sur l'onglet **Modèles de catégorie**.

Etape 3. Cliquez sur l'onglet vertical **Modèles de BIOS ThinkServer CPlus étendus**.

Etape 4. Sélectionnez le modèle à modifier, puis cliquez sur l'icône **Éditer** ().

Etape 5. Modifiez les zones appropriées.

Vous pouvez sélectionner les paramètres que vous voulez inclure dans le modèle de catégorie en cliquant sur les paramètres **Inclure/Exclure**.

Etape 6. Cliquez sur **Enregistrer** pour enregistrer les modifications apportées au modèle de catégorie actuel, ou cliquez sur **Enregistrer sous** pour enregistrer les modifications dans un nouveau modèle de catégorie.

Résultats

Le modèle de catégorie modifié est répertorié sous l'onglet **Modèles de BIOS ThinkServer CPlus étendus** à la page Modèles de configuration : modèles de catégorie :

Depuis cette page, vous pouvez aussi exécuter les actions suivantes sur un modèle de catégorie sélectionné :

- Copiez un modèle existant en cliquant sur l'icône **Copier** ().
- Supprimez un modèle en cliquant sur l'icône **Supprimer** ().
- Renommez un modèle en cliquant sur l'icône **Renommer** ().
- Importez et exportez des modèles (voir Exportation et importation de modèles de serveur et de catégorie).

Déploiement d'un modèle de serveur sur un serveur

Vous pouvez déployer un modèle de serveur sur un ou plusieurs serveurs gérés. Vous pouvez également déployer un modèle de serveur sur une ou plusieurs baies vides d'un châssis géré par Lenovo XClarity Administrator ou dans un châssis de marque de réservation. Le déploiement d'un modèle de serveur avant que le serveur soit installé réserve des adresses IP de gestion, réserve des adresses Fibre Channel ou Ethernet virtuelles, et transmet le paramètre réseau aux ports internes de commutation relatifs.

Avant de commencer

Lisez les considérations de configuration du serveur avant de tenter d'appliquer un modèle de serveur à vos appareils gérés (voir Déploiement d'un modèle de serveur sur un serveur).

Procédure

Pour déployer un modèle de serveur sur un serveur géré, procédez comme suit.

Etape 1. Depuis la barre de menus Lenovo XClarity Administrator, cliquez sur **Distribution → Modèles de configuration de serveur**. La page Modèles de configuration de serveur s'affiche.

Etape 2. Cliquez sur l'onglet **Modèles de serveur**.

Etape 3. Sélectionnez le modèle de serveur à déployer, puis cliquez sur l'icône **Déployer** ().

La boîte de dialogue Déployer un modèle de serveur s'affiche avec le modèle de serveur sélectionné répertorié dans la liste **Modèle à déployer**.

Etape 4. Choisissez le moment auquel activer les configurations :

- **Complet**. Met immédiatement sous tension ou redémarre le serveur pour activer les configurations de serveur, de contrôleur de gestion de la carte mère et UEFI (Unified Extensible Firmware Interface).
- **Partiel**. (réglage par défaut) Active immédiatement les configurations de contrôleur de gestion, mais reporte l'activation des configurations de serveur et UEFI jusqu'au prochain redémarrage du serveur. Le serveur doit être mis sous tension ou redémarré manuellement pour que le profil soit complètement activé.

  Remarque : Lorsque vous déployez des modèles de serveur qui incluaient uniquement les paramètres IMM (y compris les informations système, l'interface de gestion et les modèles de catégorie BMC étendus), il n'est pas nécessaire de redémarrer le serveur.
- **Reporté**. Génère un profil pour les configurations de serveur, de contrôleur de gestion et UEFI, mais n'active pas les paramètres de configuration sur le serveur. Vous devez activer manuellement le profil de serveur en redémarrant le serveur pour que le profil soit complètement activé.

Remarque : Les paramètres réseau sur les ports internes de commutation relatifs sont transmis au commutateur immédiatement après le déploiement, quelle que soit la configuration de l'activation.

Etape 5. Choisissez un ou plusieurs serveurs ou une plusieurs baies de châssis vides sur lesquels vous voulez déployer le modèle de serveur.

Remarque : Pour afficher une liste de baies de châssis vide, sélectionnez **Afficher les baies vides**.

Etape 6. Cliquez sur **Déployer**. Une boîte de dialogue répertoriant l'état de déploiement de chaque baie sélectionnée s'affiche.

Etape 7. Cliquez à nouveau sur **Déployer** pour démarrer le processus de déploiement.

Remarque : Le déploiement peut prendre plusieurs minutes. Pendant le déploiement, un profil de serveur est créé et affecté à chaque serveur ou baie de châssis sélectionné.

Etape 8. Cliquez sur **Fermer**.

Après avoir terminé

Vous pouvez surveiller la progression du déploiement en cliquant sur **Surveillance → Travaux** dans la barre de menus XClarity Administrator. Vous pouvez également surveiller la création d'un profil de serveur en cliquant sur **Distribution → Profils de serveur**. Une fois le déploiement terminé, consultez les profils de serveur générés, puis enregistrez l'adresse IP de gestion et toutes les adresses Fibre Channel ou Ethernet virtualisées.

Si vous avez déployé un modèle de serveur sur un serveur existant et que vous avez sélectionné :

- l'activation **Complet**, un profil de serveur est créé pour chaque serveur, la configuration est propagée à chaque serveur et chaque serveur est réamorcé pour activer les modifications de configuration.
- l'activation **Partiel**, un profil de serveur est créé pour chaque serveur, et la configuration est propagée à chaque serveur. Pour activer complètement les modifications de configuration, vous devez mettre sous tension ou redémarrer manuellement chaque serveur (voir Mise sous tension et hors tension d'un serveur).
- l'activation **Reporté**, un profil de serveur est créé pour chaque serveur. Vous devez activer manuellement le profil de serveur sur le serveur (voir Activation d'un profil de serveur).

Si vous avez déployé un modèle de serveur sur une baie vide dans un châssis géré ou un châssis de marque de réservation, une fois que les nœuds de traitement ont été physiquement installés dans les baies de châssis appropriées puis reconnus et gérés par Lenovo XClarity Administrator, vous devez déployer et activer le profil de serveur sur des nœuds de traitement nouvellement installés (voir Activation d'un profil de serveur).

Si un ou plusieurs serveurs ne démarrent pas après le déploiement d'un nouveau modèle de serveur sur ces serveurs, il se peut que les paramètres d'amorçage aient été remplacés par les paramètres d'amorçage par défaut spécifiés dans le modèle de serveur. Pour les systèmes d'exploitation installés en mode UEFI, la restauration des paramètres par défaut peut nécessiter des étapes de configuration supplémentaires pour restaurer la configuration d'amorçage. Pour obtenir des exemples de récupération de paramètres d'amorçage sur des serveurs qui s'exécutent sur Windows ou Linux, voir Récupération de paramètres d'amorçage après le déploiement d'un modèle de serveur.

Modification d'un modèle de serveur

Vous pouvez apporter ultérieurement des modifications de configuration à un modèle de serveur existant. Si le modèle de serveur d'origine est déployé sur les serveurs (s'il est utilisé), vous pouvez déployer à nouveau le modèle de serveur modifié sur tous ces serveurs ou sur un sous-ensemble de serveurs.

À propos de cette tâche

Remarque : Si vous choisissez de ne pas déployer à nouveau le modèle de serveur modifié sur un ensemble de serveurs, ces derniers doivent rester associés au modèle de serveur d'origine, non modifié.

Si vous modifiez un modèle de serveur, vous pouvez contrôler une configuration commune depuis un seul et même emplacement et conserver l'ensemble original d'attributions d'adresses virtuelles.

Procédure

Pour modifier un modèle de serveur, procédez comme suit.

Etape 1. Depuis la barre de menus Lenovo XClarity Administrator, cliquez sur **Distribution → Modèles de configuration de serveur**. La page Modèles de configuration de serveur s'affiche.

Etape 2. Cliquez sur l'onglet **Modèles de serveur**.

Etape 3. Sélectionnez le modèle de serveur à modifier, puis cliquez sur l'icône **Éditer** (). L'Assistant d'édition des modèles de serveur s'affiche.

Etape 4. Entrez le nom du nouveau modèle ainsi qu'une description.

Etape 5. Choisissez la configuration de stockage local à appliquer lorsque ce modèle est déployé sur un serveur, puis cliquez sur **Suivant**.

Pour plus d'informations sur les paramètres de stockage local, voir Définition d'un stockage local.

Etape 6. **Facultatif :** Modifiez l'adressage de carte d'E-S et définissez des cartes d'E-S supplémentaires qui correspondent au matériel que vous prévoyez de configurer avec ce modèle, puis cliquez sur **Suivant**.

Pour plus d'informations sur les paramètres de carte d'E-S, voir Définition de cartes d'E-S.

Etape 7. Définissez l'ordre d'amorçage à appliquer lorsque ce modèle est déployé sur un serveur, puis cliquez sur **Suivant**.

Pour plus d'informations sur les paramètres des cibles d'amorçage SAN, voir Définition d'options d'amorçage.

Etape 8. Sélectionnez les paramètres du microprogramme dans la liste des modèles de catégorie existants.

Vous pouvez créer de nouveaux modèles de catégorie en cliquant sur l'icône **Créer** ().

Pour plus d'informations sur les paramètres de microprogramme, voir Définition de paramètres de microprogramme.

Etape 9. Cliquez sur **Enregistrer** pour enregistrer les modifications de configuration apportées au modèle de serveur actuel, ou cliquez sur **Enregistrer sous** pour enregistrer les modifications de configuration dans un nouveau modèle de serveur.

Etape 10. Choisissez d'enregistrer les modifications apportées au modèle de serveur actuel, ou au nouveau modèle de serveur.

- Cliquez sur **Enregistrer** pour enregistrer les modifications dans le modèle de serveur actuel. Dans la boîte de dialogue Enregistrer et déployer le modèle à nouveau, procédez comme suit :
  1. Choisissez le moment auquel activer les configurations.
     - **Complet**. Met immédiatement sous tension ou redémarre le serveur pour activer les configurations de serveur, de contrôleur de gestion de la carte mère et UEFI (Unified Extensible Firmware Interface).
     - **Partiel**. (réglage par défaut) Active immédiatement les configurations de contrôleur de gestion, mais reporte l'activation des configurations de serveur et UEFI jusqu'au prochain redémarrage du serveur. Le serveur doit être mis sous tension ou redémarré manuellement pour que le profil soit complètement activé.

Remarque : Lorsque vous déployez des modèles de serveur qui incluaient uniquement les paramètres IMM (y compris les informations système, l'interface de gestion et les modèles de catégorie BMC étendus), il n'est pas nécessaire de redémarrer le serveur.

Remarque : Les paramètres réseau sur les ports internes de commutation relatifs sont transmis au commutateur immédiatement après le déploiement, quelle que soit la configuration de l'activation.

2. Sélectionnez les serveurs cibles auxquels vous souhaitez déployer à nouveau les modifications de configuration. Vous pouvez choisir tous les serveurs sur lesquels le modèle de serveur d'origine a été déployé ou un sous-ensemble de ces serveurs.
3. Cliquez sur **Déployer à nouveau**.

- Cliquez sur **Enregistrer sous** pour enregistrer les modifications dans le nouveau modèle de serveur. Pour déployer le nouveau modèle, voir Déploiement d'un modèle de serveur sur un serveur.

Exportation et importation de modèles de serveur et de catégorie

Si vous avez plusieurs instances de Lenovo XClarity Administrator, vous pouvez exporter des modèles de serveur et de catégorie à partir d'une instance de XClarity Administrator et les importer dans une autre instance de XClarity Administrator.

À propos de cette tâche

Vous pouvez uniquement exporter des modèles de serveur et de catégorie. Les stratégies, les pools d'adresses et les profils ne peuvent pas être exportés. Les modèles exportés sont dissociés de tous les pools d'adresses de référence. Pour tirer parti des pools d'adresses dans un modèle importé, éditez le modèle et réassociez-le dans XClarity Administrator aux pools dans lesquels ils sont importés.

Remarque : Lorsque vous exportez un modèle de serveur, les modèles de catégorie associés sont également exportés.

Procédure

- Pour exporter un ou plusieurs modèles :
  1. Depuis la barre de menus XClarity Administrator, cliquez sur **Distribution → Modèles de configuration de serveur**. La page Modèles de configuration de serveur s'affiche.
  2. Cliquez sur l'onglet **Modèles de serveur** ou sur **Modèles de catégorie**.
  3. Sélectionnez un ou plusieurs modèles à exporter.
  4. Cliquez sur l'icône **Exporter** ().
  5. Cliquez sur **Exporter** pour exporter les modèles.
  6. Enregistrez le fichier de données de modèle sur votre système local.

     Remarque : Si un modèle exporté fait référence à des pools d'adresses, ces références sont retirées du modèle exporté pour éviter des conflits lors de l'importation du modèle dans une autre instance de XClarity Administrator. Lorsque le modèle est réimporté, vous pouvez éditer le modèle importé et affecter les pools d'adresses souhaités.
- Pour importer un ou plusieurs modèles :
  1. Depuis la barre de menus XClarity Administrator, cliquez sur **Distribution → Modèles de configuration de serveur**. La page Modèles de configuration de serveur s'affiche.
  2. Cliquez sur l'icône **Importer** () pour importer les modèles. La boîte de dialogue Importer des modèles s'affiche.

3. Cliquez sur **Sélectionner un fichier**, puis sélectionnez un fichier de données de modèle à importer. Répétez l'opération pour les fichiers de données de modèle supplémentaires.
4. Cliquez sur **Importer** pour importer les fichiers sélectionnés.

   Un rapport récapitulatif s'affiche avec la liste des modèles qui ont été importés, les modèles qui ont été renommés pour éviter les conflits de noms et les modèles qui ont été ignorés car ils existent déjà.

Utilisation de profils de serveur

Un *profil de serveur* est une instance d'un modèle de serveur qui est appliquée à un serveur spécifique. Les profils de serveur sont générés et affectés automatiquement lorsqu'un modèle de serveur est déployé sur un ou plusieurs serveurs. Un profil de serveur est créé pour chaque serveur cible. Chaque profil de serveur contient la configuration spécifique d'un serveur unique, ainsi que des informations (telles que le nom, les adresses IP et les adresses MAC affectés) qui sont uniques pour ce serveur spécifique.

À propos de cette tâche

Le profil de serveur est activé pendant le processus de démarrage du contrôleur de gestion de la carte mère. Vous avez le choix entre les opérations suivantes :
- Redémarrer le serveur lors du déploiement du modèle pour activer immédiatement le profil de serveur.
- Reporter l'activation jusqu'au prochain réamorçage.
- Reporter l'activation du profil de serveur jusqu'à ce que vous l'activiez manuellement.

Plusieurs profils de serveur peuvent hériter d'un modèle de serveur unique. Lorsqu'un modèle de serveur est déployé sur un ou plusieurs serveurs, vous pouvez déployer rapidement des modifications de configuration sur plusieurs serveurs en modifiant le modèle de serveur parent et les modèles de catégorie. Les profils de serveur dépendants sont automatiquement mis à jour et redéployés sur les serveurs auxquels ils sont associés. En modifiant le modèle de serveur, vous pouvez contrôler une configuration commune à partir d'un emplacement unique.

Si vous remplacez un serveur existant ou si vous installez un serveur prédistribué dans une baie vide d'un châssis, vous devez activer le profil de serveur pour ce nouveau serveur afin de distribuer les modifications de configuration sur le nouveau serveur.

Remarque : Vous pouvez déployer un modèle de serveur sur plusieurs serveurs. Toutefois, il n'est pas possible de déployer plusieurs modèles sur un serveur unique.

Vous pouvez modifier le profil de serveur associé à un serveur de plusieurs manières, en fonction de la cause de la modification.

- Si vous voulez déplacer ou réaffecter un serveur :
  1. Désactivez le profil de serveur actuel sur le serveur actuel (voir Désactivation d'un profil de serveur).
  2. Déployez le nouveau modèle de serveur sur le nouveau serveur (voir Déploiement d'un modèle de serveur sur un serveur).
- Si un serveur est défaillant et que vous voulez utiliser un serveur de secours à la place :
  1. Désactivez le profil de serveur actuel sur le serveur défaillant (voir Désactivation d'un profil de serveur).
  2. Activez le même profil de serveur sur le serveur de secours (voir Activation d'un profil de serveur).
  3. Lorsque le serveur défaillant est réparé, vous pouvez répéter les étapes suivantes pour rechanger de profil.
- Si un serveur est défaillant et que vous voulez remplacer le matériel :
  1. Désactivez le profil de serveur actuel sur le serveur défaillant (voir Désactivation d'un profil de serveur).

2. Remplacez le serveur défaillant.
3. Activez le même profil de serveur sur le nouveau serveur (voir Activation d'un profil de serveur).

Important :

- Lorsque vous utilisez la virtualisation d'adresse, un serveur conserve l'adresse WWN ou MAC virtuelle qui lui est affectée jusqu'à ce qu'il soit arrêté. Lorsque vous désactivez un profil pour lequel la virtualisation d'adresse est activée, la case **Mettre le serveur hors tension** est cochée par défaut. Vérifiez que le serveur d'origine est hors tension avant d'activer le profil inactif sur un autre serveur afin d'éviter des conflits d'adresses.
- Si vous supprimez un profil qui n'est pas le plus récemment créé, les adresses MAC et WWN virtuelles *ne sont pas* libérées du pool d'adresses. Pour plus d'informations, voir Suppression d'un profil de serveur.
- Les paramètres d'un serveur peuvent ne plus être conformes au profil du serveur s'ils ont été modifiés sans modèles de configuration ou si un problème s'est produit lors du déploiement, par exemple un problème de microprogramme ou de paramètre non valide. Vous pouvez déterminer l'état de conformité de chaque serveur en consultant la page Modèles de configuration : Profils de serveur.

Activation d'un profil de serveur

Vous pouvez activer un profil de serveur sur un serveur remplacé, réaffecté, ou nouvellement installé et géré.

À propos de cette tâche

Si vous remplacez un serveur existant ou si vous installez un serveur prédistribué dans une baie vide d'un châssis, vous devez activer le profil de serveur pour ce nouveau serveur afin de distribuer les modifications de configuration sur le nouveau serveur.

Important :

- Lorsque vous utilisez la virtualisation d'adresse, un serveur conserve l'adresse WWN ou MAC virtuelle qui lui est affectée jusqu'à ce qu'il soit arrêté. Lorsque vous désactivez un profil pour lequel la virtualisation d'adresse est activée, la case **Mettre le serveur hors tension** est cochée par défaut. Vérifiez que le serveur d'origine est hors tension avant d'activer le profil inactif sur un autre serveur afin d'éviter des conflits d'adresses.
- Si vous supprimez un profil qui n'est pas le plus récemment créé, les adresses MAC et WWN virtuelles *ne sont pas* libérées du pool d'adresses. Pour plus d'informations, voir Suppression d'un profil de serveur.
- Les paramètres d'un serveur peuvent ne plus être conformes au profil du serveur s'ils ont été modifiés sans modèles de configuration ou si un problème s'est produit lors du déploiement, par exemple un problème de microprogramme ou de paramètre non valide. Vous pouvez déterminer l'état de conformité de chaque serveur en consultant la page Modèles de configuration : Profils de serveur.

Procédure

Pour activer un profil de serveur, procédez comme suit.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Distribution → Profils de serveur**. La page Modèles de configuration : Profils de serveur s'affiche.

Etape 2. Sélectionnez un profil de serveur à activer.

Astuces : L'état actuel des profils de serveur est répertorié dans la colonne **État du profil**. Vous pouvez activer le profil de serveur qui se trouve à l'état Inactif ou Activation en attente.

Etape 3. Cliquez sur l'icône **Activer le profil de serveur** ().

Etape 4. Cliquez sur **Activer**.

Si le profil est dans l'état En attente, Actif ou Actif défaillant, vous pouvez choisir le moment auquel activer le déploiement :

- **Complet**. Met immédiatement sous tension ou redémarre le serveur pour activer les configurations de serveur, de contrôleur de gestion de la carte mère et UEFI (Unified Extensible Firmware Interface).
- **Partiel**. (réglage par défaut) Active immédiatement les configurations de contrôleur de gestion, mais reporte l'activation des configurations de serveur et UEFI jusqu'au prochain redémarrage du serveur. Le serveur doit être mis sous tension ou redémarré manuellement pour que le profil soit complètement activé.

  Remarque : Lorsque vous déployez des modèles de serveur qui incluaient uniquement les paramètres IMM (y compris les informations système, l'interface de gestion et les modèles de catégorie BMC étendus), il n'est pas nécessaire de redémarrer le serveur.

Lorsque le profil de serveur est activé pour la première fois, l'état du profil devient « Actif ». Après la vérification de conformité, l'état devient « Compatible » ou « Non compatible ».

Résultats

Le profil de serveur sur la page Modèle de configuration : Profils de serveur passe à l'état Actif.

Désactivation d'un profil de serveur

Vous pouvez annuler l'affectation d'un profil de serveur d'un serveur ou d'une baie de châssis en désactivant le profil.

Procédure

Pour désactiver un profil de serveur, procédez comme suit.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Distribution → Profils de serveur**. La page Modèles de configuration : Profils de serveur s'affiche.

Etape 2. Sélectionnez le profil de serveur à désactiver.

Astuce : L'état actuel du profil de serveur est répertorié dans la colonne **État du profil**.

Etape 3. Cliquez sur l'icône **Désactiver un profil de serveur** ( ).

Etape 4. Choisissez l'une des options de désactivation suivantes :

- **Réinitialiser les paramètres d'identité IMM**. Réinitialise les paramètres d'identité configurés du profil (comme le nom d'hôte du contrôleur de gestion de la carte mère, le nom de l'appareil ou les adresses IP statiques affectées à l'interface de gestion). Seuls les paramètres configurés via le modèle de serveur associé sont réinitialisés.

  Remarque : Pour les serveurs avec des adresses IP affectées de manière statique, cette option active le mode DHCP. Si aucun serveur DHCP n'est activé sur le réseau, le serveur doit être manuellement reconfiguré avec une adresse IP valide. Les serveurs Converged, NeXtScale et System x rack et au format tour doivent ensuite être de nouveau gérés avec XClarity Administrator.
- **Mettre le serveur hors tension**. Met le serveur hors tension. Lorsque le serveur est remis sous tension, les affectations d'adresses virtuelles reviennent aux valeurs gravées par défaut.
- **Forcer la désactivation**. Désactive le profil de serveur même si le serveur a été retiré ou n'est pas accessible.
- **Réinitialiser les paramètres de port interne de commutateur**. Réinitialise les paramètres de port interne de commutateur configuré par profil sur les valeurs par défaut, y compris la désactivation du mode UFP et le retrait de vports de membre associés à partir des définitions VLAN. Seuls les paramètres configurés via le modèle de serveur associé sont réinitialisés.

  Cette option est désactivée par défaut.

  Choisissez cette option pour conserver les ports de commutateur dans un état où le profil de serveur peut ensuite être déployé vers un autre serveur sans les paramètres qui seraient en conflit avec la configuration de port de commutateur précédente.

Etape 5. Cliquez sur **Désactiver**.

Résultats

Le profil de serveur sur la page Modèle de configuration : Profils de serveur passe à l'état Inactif.

Remarque : Si XClarity Administrator ne peut pas communiquer avec le contrôleur de gestion (par exemple, si le contrôleur de gestion est dans un état d'erreur ou en cours de redémarrage), la désactivation du profil de serveur échoue et le profil de serveur n'est pas désactivé. Dans ce cas, relancez la désactivation, puis sélectionnez l'option Forcer la désactivation afin de désactiver le profil. Le serveur préalablement affecté est encore configuré avec l'identité affectée au profil et les affectations d'adresses. Le serveur doit être mis sous tension manuellement et retiré de l'infrastructure afin d'éviter les conflits d'adresses.

Suppression d'un profil de serveur

Vous pouvez uniquement supprimer les profils de serveur qui ont été désactivés.

Avant de commencer

Vérifiez que les profils de serveur à supprimer sont désactivés (voir Désactivation d'un profil de serveur).

Procédure

Pour supprimer un profil de serveur, procédez comme suit.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Distribution → Profils de serveur**. La page Modèles de configuration : Profils de serveur s'affiche.

Etape 2. Sélectionnez le profil de serveur qui se trouve en état Désactivé.

Astuce : L'état actuel du profil de serveur est répertorié dans la colonne **État du profil**.

Etape 3. Cliquez sur l'icône **Supprimer** ( ).

Remarque : Lorsque vous supprimez le profil le plus récemment créé, toute adresse MAC ou WWN virtuelle est libérée du pool d'adresses. Si vous supprimez un profil qui n'est pas le plus récemment créé, les adresses MAC et WWN virtuelles *ne sont pas* libérées du pool d'adresses.

Utilisation de châssis de marque de réservation

Vous pouvez pré-appliquer des serveurs qui seront installés dans un châssis Flex System ultérieurement en définissant un *châssis de marque de réservation* qui agit en tant que cible pour le modèle de serveur jusqu'à l'arrivée du matériel physique.

À propos de cette tâche

Lorsque vous déployez un modèle de serveur sur un châssis de marque de réservation, Lenovo XClarity Administrator crée un profil de serveur pour les 14 baies de serveur dans le châssis Flex System et réserve les adresses IP de gestion et les adresses Fibre Channel ou Ethernet virtuelles pour les serveurs.

Le châssis de marque de réservation regroupe l'ensemble des profils de serveur. Ainsi, lorsque le matériel arrive, vous pouvez déployer ce châssis pour activer les profils de serveur sur les physiques au lieu de déployer individuellement les 14 profils de serveur. Chaque serveur doit être redémarré pour activer complètement le profil de serveur.

Création d'un châssis de marque de réservation

Vous pouvez créer un châssis de marque de réservation qui peut être pré-distribué avant l'installation du matériel. La distribution des nœuds de traitement dans le châssis réserve des adresses IP de gestion et des adresses Fibre Channel ou Ethernet virtuelles.

Procédure

Pour créer un châssis de marque de réservation, procédez comme suit.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Distribution → Modèles**. La page Modèles de configuration : Modèles s'affiche.

Etape 2. Cliquez sur l'onglet **Châssis de marque de réservation**.

Etape 3. Cliquez sur l'onglet vertical **Ajouter un châssis de marque de réservation**.

Etape 4. Entrez un nom et une description pour le châssis de marque de réservation.

Etape 5. Cliquez sur **Ajouter**.

Après avoir terminé

Un onglet vertical est ajouté pour le nouveau châssis de marque de réservation dans la page Modèles de configuration : Châssis de marque de réservation.

Depuis cette page, vous pouvez exécuter les actions suivantes sur un châssis de marque de réservation sélectionné :

- Déployez le châssis de marque de réservation en cliquant sur l'icône **Déployer** ( ).
- Modifiez le nom et la description du châssis de marque de réservation en cliquant sur l'icône **Éditer** ( ).
- Déployez un modèle de serveur sur le châssis de marque de réservation (voir Déploiement d'un modèle de serveur sur un châssis de marque de réservation).
- Désactivez le profil de serveur d'un châssis de marque de réservation (voir Désactivation d'un profil de serveur).
- Supprimez le châssis de marque de réservation en cliquant sur l'icône **Supprimer** ( ).

Déploiement d'un modèle de serveur sur un châssis de marque de réservation

Vous pouvez déployer un modèle de serveur sur chaque baie d'un châssis de marque de réservation. Le déploiement d'un modèle de serveur avant que les serveurs soient installés dans le châssis Flex System crée

un profil de serveur pour chaque baie de serveur du châssis et réserve des adresses IP de gestion et des adresses Fibre Channel ou Ethernet virtuelles.

Procédure

Pour déployer un modèle de serveur sur un châssis de marque de réservation, procédez comme suit.

Etape 1. Depuis la barre de menus Lenovo XClarity Administrator, cliquez sur **Distribution → Modèles de configuration de serveur**. La page Modèles de configuration de serveur s'affiche.

Etape 2. Cliquez sur l'onglet **Modèles de serveur**.

Etape 3. Sélectionnez le modèle de serveur que vous voulez déployer sur le châssis de marque de réservation.

Etape 4. Cliquez sur l'icône **Déployer** (). La boîte de dialogue Déployer un modèle de serveur s'affiche avec la liste des châssis et châssis de marque de réservation disponibles.

Etape 5. Sélectionnez **Reporté** dans la liste **Activation**.

Etape 6. Cliquez sur **Afficher les baies vides**.

Etape 7. Choisissez une ou plusieurs baies de châssis de marque de réservation sur lesquelles vous voulez déployer le modèle de serveur.

Etape 8. Cliquez sur **Déployer**. Une boîte de dialogue répertoriant l'état de déploiement de chaque baie sélectionnée s'affiche.

Etape 9. Cliquez à nouveau sur **Déployer** pour démarrer le processus de déploiement.

Un profil de serveur est créé et affecté pour chaque baie sélectionnée dans le châssis de marque de réservation.

Remarque : Le déploiement peut prendre plusieurs minutes.

Etape 10. Cliquez sur **Fermer**.

Après avoir terminé

Vous pouvez surveiller la progression du déploiement en cliquant sur **Surveillance → Travaux** dans la barre de menus XClarity Administrator. Vous pouvez également surveiller la création d'un profil de serveur en cliquant sur **Distribution → Profils de serveur**. Une fois le déploiement terminé, consultez les profils de serveur générés, puis enregistrez l'adresse IP de gestion et toutes les adresses Fibre Channel ou Ethernet virtualisées.

Une fois le châssis Flex System physiquement installés dans l'armoire, puis reconnu et géré par XClarity Administrator, vous pouvez déployer le châssis de marque de réservation pour mettre à disposition tous les serveurs du châssis (voir Déploiement d'un modèle de serveur sur un châssis de marque de réservation).

Déploiement d'un châssis de marque de réservation

Après avoir préconfiguré un châssis de marque de réservation en déploiement un modèle de serveur sur ce châssis, puis reconnu et géré le châssis réel, vous pouvez déployer le châssis de marque de réservation pour configurer les nœuds de traitement réels.

Procédure

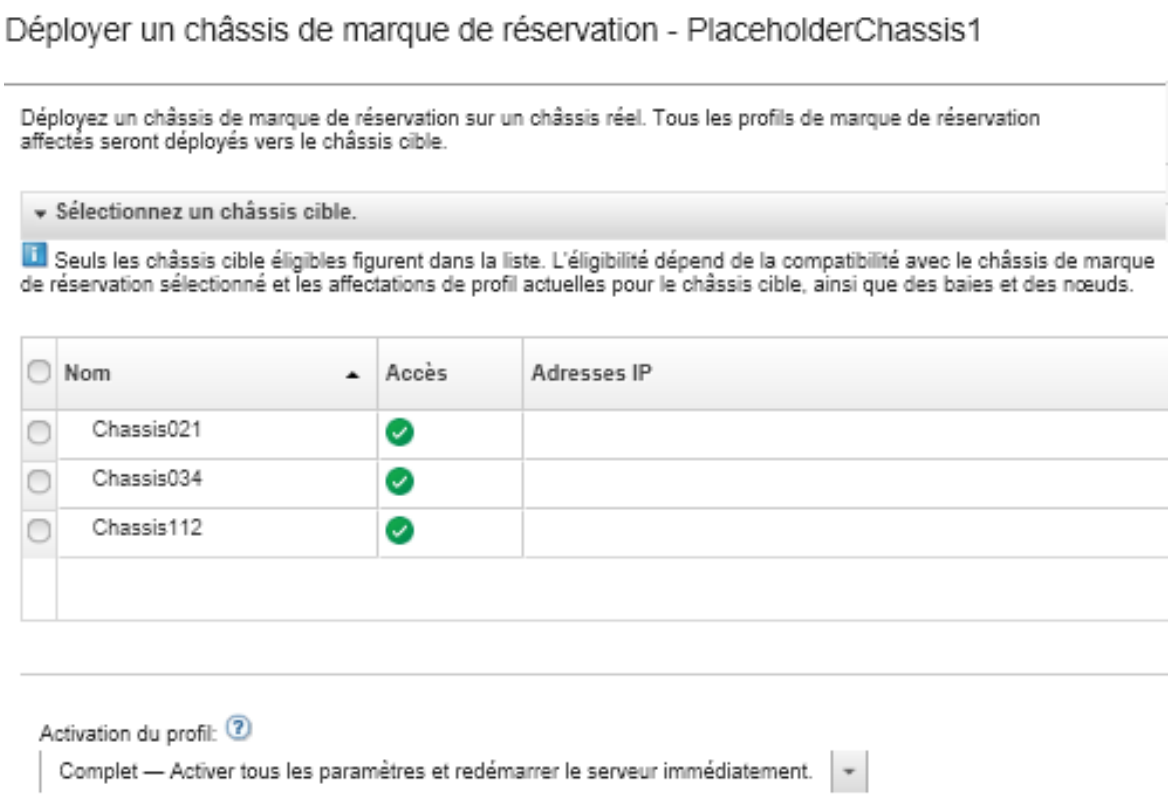
Pour déployer un châssis de marque de réservation, procédez comme suit.

Etape 1. Depuis la barre de menus Lenovo XClarity Administrator, cliquez sur **Distribution → Modèles de configuration de serveur**. La page Modèles de configuration de serveur s'affiche.

Etape 2. Cliquez sur l'onglet **Châssis de marque de réservation**.

Etape 3. Sélectionnez l'onglet vertical correspondant au châssis de marque de réservation que vous voulez déployer.

Etape 4. Cliquez sur l'icône **Déployer un châssis de marque de réservation** ( ) pour afficher la boîte de dialogue Déployer un châssis de marque de réservation.



Etape 5. Choisissez le moment auquel activer les configurations :

Remarque : Les paramètres réseau sur les ports internes de commutation relatifs sont transmis au commutateur immédiatement après le déploiement, quelle que soit la configuration de l'activation.

- **Complet**. Met immédiatement sous tension ou redémarre le serveur pour activer les configurations de serveur, de contrôleur de gestion de la carte mère et UEFI (Unified Extensible Firmware Interface).
- **Partiel**. (réglage par défaut) Active immédiatement les configurations de contrôleur de gestion, mais reporte l'activation des configurations de serveur et UEFI jusqu'au prochain redémarrage du serveur. Le serveur doit être mis sous tension ou redémarré manuellement pour que le profil soit complètement activé.

  Remarque : Lorsque vous déployez des modèles de serveur qui incluaient uniquement les paramètres IMM (y compris les informations système, l'interface de gestion et les modèles de catégorie BMC étendus), il n'est pas nécessaire de redémarrer le serveur.

Etape 6. Cliquez sur **Activer**.

Réinitialisation des adaptateurs de stockage aux valeurs par défaut

Vous pouvez réinitialiser les adaptateurs de stockage local à leurs paramètres d'usine par défaut pour un ou plusieurs serveurs.

À propos de cette tâche

Attention : Cette action efface toutes les données sur les adaptateurs du stockage local.

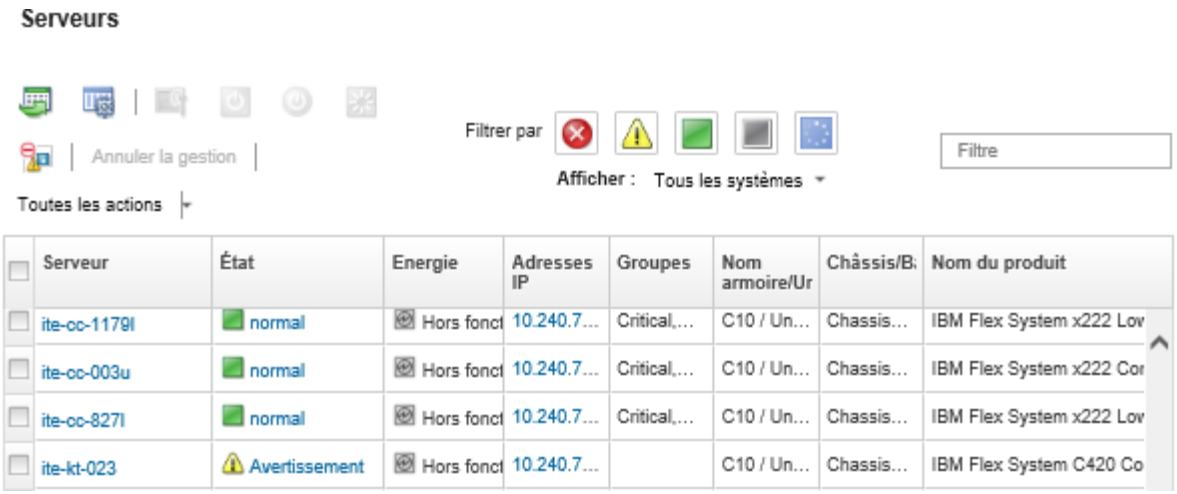
Si le serveur est mis hors tension et la liaison RAID est prise en charge, le serveur est amorcé sur configuration système pour réinitialiser les adaptateurs HDD et SSD.

Procédure

Pour effacer la configuration RAID d'un ou plusieurs serveurs, procédez comme suit.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Matériel → Serveurs**. La page Serveurs s'affiche avec une vue tabulaire de tous les serveurs gérés (serveurs rack et nœuds de traitement).

Vous pouvez trier les colonnes du tableau pour trouver plus facilement le serveur que vous souhaitez gérer. En outre, vous pouvez sélectionner un type de serveur dans la liste déroulante **Tous les systèmes** et saisir un texte (par exemple, un nom ou une adresse IP) dans la zone **Filtre** pour filtrer davantage l'affichage des serveurs.



Etape 2. Sélectionnez un ou plusieurs serveurs

Etape 3. Sélectionnez **Toutes les actions → Service → Réinitialiser le stockage local aux valeurs par défaut**. Une boîte de dialogue s'affiche pour vous demander des informations supplémentaires.

Etape 4. Sélectionnez les adaptateurs de stockage local à réinitialiser.

Etape 5. (Serveurs ThinkSystem uniquement) Convertissez les unités JBOD en unités correctes non configurées.

Etape 6. Cliquez sur **Réinitialiser le stockage**.

Configuration de la mémoire

Vous pouvez chiffrer et déchiffrer de la mémoire persistante pour les modules de mémoire DIMM persistante Intel® Optane™ DC

Procédure

Effectuez la procédure suivante pour chiffrer et déchiffrer la mémoire persistante.

Etape 1. Dans le menu XClarity Administrator, cliquez sur **Matériel → Serveurs**. La page Serveurs s'affiche avec une vue tabulaire de tous les serveurs gérés (serveurs rack et nœuds de traitement).

Etape 2. Sélectionnez un ou plusieurs serveurs à configurer.

Etape 3. Cliquez sur **Toutes les actions → Sécurité → Opération Intel Optane PMEM** pour afficher la boîte de dialogue Opération Intel Optane PMEM.

Etape 4. Sélectionnez l'opération de sécurité que vous souhaitez effectuer.

- **Activer la sécurité**. Les données enregistrées dans la région de la mémoire persistante sont chiffrées à l'aide de la phrase passe spécifiée.

  Important : Notez l'expression de passe de chiffrement. La phrase de passe est requise pour autoriser la désactivation de la sécurité ou pour effacer la phrase passe de chiffrement.

- **Désactiver la sécurité**. Les données sont enregistrées dans la région de la mémoire persistante qui n'est pas chiffrée.

Les données qui sont déjà enregistrées dans la région de la mémoire persistante restent chiffrées et demeurent accessibles.

Remarque : Cette action n'est possible que lorsque la sécurité est activée et qu'une phrase passe est définie. Vous devez autoriser cette opération à l'aide de la phrase passe actuelle. Vous pouvez désactiver la sécurité pour plusieurs modules DIMM de l'appareil si tous les modules DIMM partagent la même phrase passe.

- **Effacement sécurisé**. Efface la phrase passe de chiffrement utilisée pour chiffrer les données stockées dans la région de la mémoire persistante afin de s'assurer que ces données sont irrécupérables.

  Remarque : Cette action n'est possible que lorsque la sécurité est activée et qu'une phrase passe est définie. Vous devez autoriser cette opération à l'aide de la phrase passe actuelle.
- **Effacement sécurisé sans passe de sécurité**. Efface de manière sécurisée toutes les données stockées dans la mémoire persistante des barrettes DIMM spécifiées dans l’appareil. Après l’effacement sécurisé, toutes les données sont irrécupérables.

  Remarque : Cette action n'est possible que lorsque la sécurité est désactivée et qu'une phrase passe n'est pas requise.

Etape 5. Si nécessaire, indiquez et confirmez la phrase passe.

Etape 6. Cliquez sur **OK**.

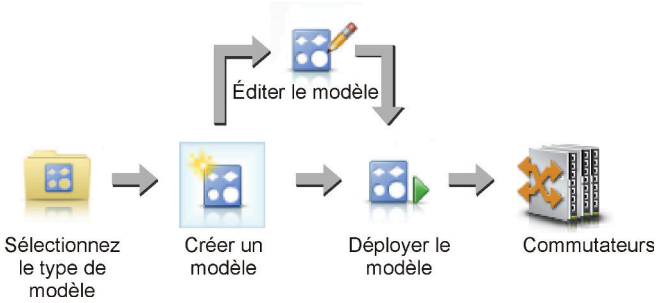
Chapitre 12. Configurer des commutateur à l'aide de modèles de configuration

Vous pouvez utiliser des modèles pour distribuer rapidement plusieurs commutateurs d'armoires CNOS depuis un seul ensemble de paramètres de configuration prédéfinis.

À propos de cette tâche

Vous pouvez utiliser des modèles de configuration de commutateur dans XClarity Administrator pour configurer les paramètres globaux, les canaux de port, les LAN virtuels, les groupes d'agrégation Link Virtual et les topologies feuille et tronc sur les commutateurs gérés. A l'heure actuelle, seuls les commutateurs d'armoire exécutant CNOS sont pris en charge.

La figure suivante illustre le flux de travaux relatif à la configuration de commutateurs d'armoire.



1. **Sélectionnez un type de modèle.**

   Un *modèle de configuration de commutateur* regroupe les paramètres de commutateur associés. Vous pouvez créer les types de modèles de configuration de commutateur suivants.
   - **Global**. configure les paramètres globaux, y compris les propriétés du système, les balises VLAN natives et les interfaces L2.
   - **Canal de port**. Configure les paramètres de canal de port basiques et avancés, retire des ports et supprime un canal de port.
   - **Feuille et tronc**. Déploie une configuration feuille et tronc sur une topologie existante.
   - **LAN virtuel (VLAN)**. Configure les paramètres et les propriétés VLAN et supprime un VLAN.
   - **VLAG**. Configure les paramètres VLAG basiques, avancés et de pair, crée et supprime une instance de VLAG.
2. **Créer un modèle.**

   Vous pouvez créer plusieurs modèles de configuration de commutateur pour représenter les différentes configurations qui sont utilisées dans votre centre de données. Vous utilisez des modèles de configuration de commutateur pour contrôler une configuration de commutateur commune depuis un seul et même emplacement.

   Pour plus d'informations sur la création des modèles de configuration de commutateur, voir Création d'un modèle de configuration de commutateur.
3. **Déploie le modèle sur un ou plusieurs commutateurs.**

   Vous pouvez déployer un modèle de serveur sur un ou plusieurs commutateurs d'armoire exécutant CNOS.

   Pour plus d'informations sur le déploiement d'une configuration de commutateur, voir Déployer des modèles de configuration de commutateur sur un commutateur cible.

4. **Éditer un modèle.**

   Le fait de modifier un modèle de configuration de commutateur ne déploie pas automatiquement les paramètres mis à jour surtout les commutateurs sur lesquels le modèle initial était déployé. Vous devez redéployer manuellement les modèles modifiés. La page de l'historique permet d'établir le suivi des paramètres pour chaque déploiement.

Définition des préférences de configuration du serveur par défaut

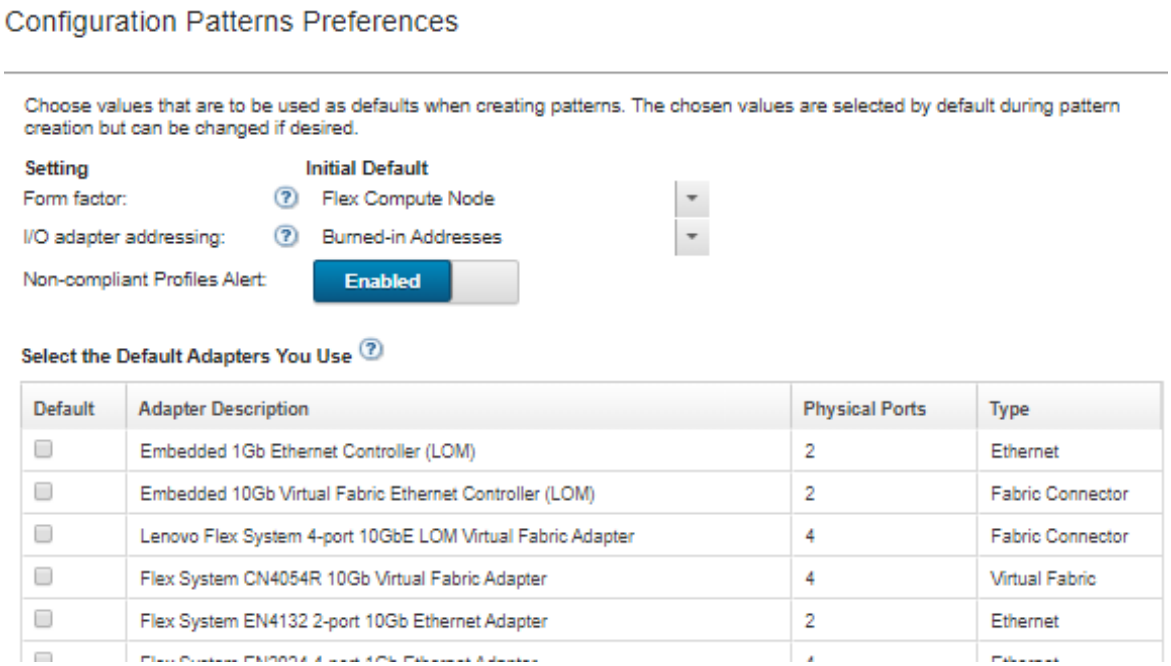
Vous pouvez définir les valeurs à sélectionner par défaut lors de la configuration de modèles de serveur. Les valeurs peuvent être modifiées lors de la création du modèle de serveur.

Procédure

Pour définir des paramètres de configuration par défaut pour les modèles de serveur, procédez comme suit.

Etape 1. Dans la barre de menus Lenovo XClarity Administrator, cliquez sur **Distribution**, puis cliquez sur l'icône d'aide (?) après **Modèles de configuration** pour afficher la page Modèles de configuration : Mise en route.

Etape 2. Cliquez sur **Définir une préférence de modèle de configuration** pour afficher la boîte de dialogue Préférence de modèle de configuration.



Etape 3. Sélectionnez le facteur de forme du serveur par défaut.

Etape 4. Sélectionnez le mode d'adressage de carte d'E-S par défaut.

- **Gravé dans**. Utilisez des adresses WWN (World Wide Name) et MAC (Media Access Control) existantes fournies avec la carte par le fabricant.
- **Virtuel**. Utilisez l'adressage de carte d'E-S virtuelle pour simplifier la gestion des connexions SAN et LAN. La virtualisation des adresses d'E-S réaffecte les adresses matérielles gravées avec des adresses MAC Ethernet et Fibre Channel WWN virtualisées. Cela peut accélérer le déploiement en préconfigurant l'appartenance à la zone SAN et en facilitant le basculement grâce à la suppression de la nécessité de reconfigurer les affectations de la segmentation SAN et du masquage LUN lors d'un remplacement de matériel.

Lorsque l'adressage virtuel est activé, les adresses Ethernet et Fibre Channel sont allouées par défaut indépendamment des adaptateurs définis. Vous pouvez choisir le pool à partir duquel les adresses Ethernet et Fibre Channel sont allouées.

Vous pouvez également modifier les paramètres d'adresse virtuelle en cliquant sur l'icône **Éditer** () en regard des modes d'adresse.

Restriction : L'adressage virtuel est pris en charge uniquement pour les serveurs dans les châssis Flex System. Les serveurs rack et au format tour ne sont pas pris en charge.

Etape 5. Vous pouvez activer ou désactiver la génération d'une alerte lorsque les paramètres de configuration d'un serveur ne correspondent pas au profil de configuration de serveur affecté.

Les alertes sont déclenchées uniquement pour le non-respect d'un profil actif (dans l'état ASSIGNED ou ERROR_ACTIVATING).

Lorsque la configuration du serveur devient compatible ou que le profil de serveur n'est pas affecté, l'alerte de profil non compatible est supprimée.

Etape 6. Sélectionnez une ou plusieurs cartes d'E-S par défaut à utiliser en tant que cartes préférées dans les listes de sélection.

Etape 7. Cliquez sur **Enregistrer**.

Création d'un modèle de configuration de commutateur

Lorsque vous créez un modèle de configuration de commutateur, vous définissez les paramètres pour un type de configuration spécifique.

Avant de commencer

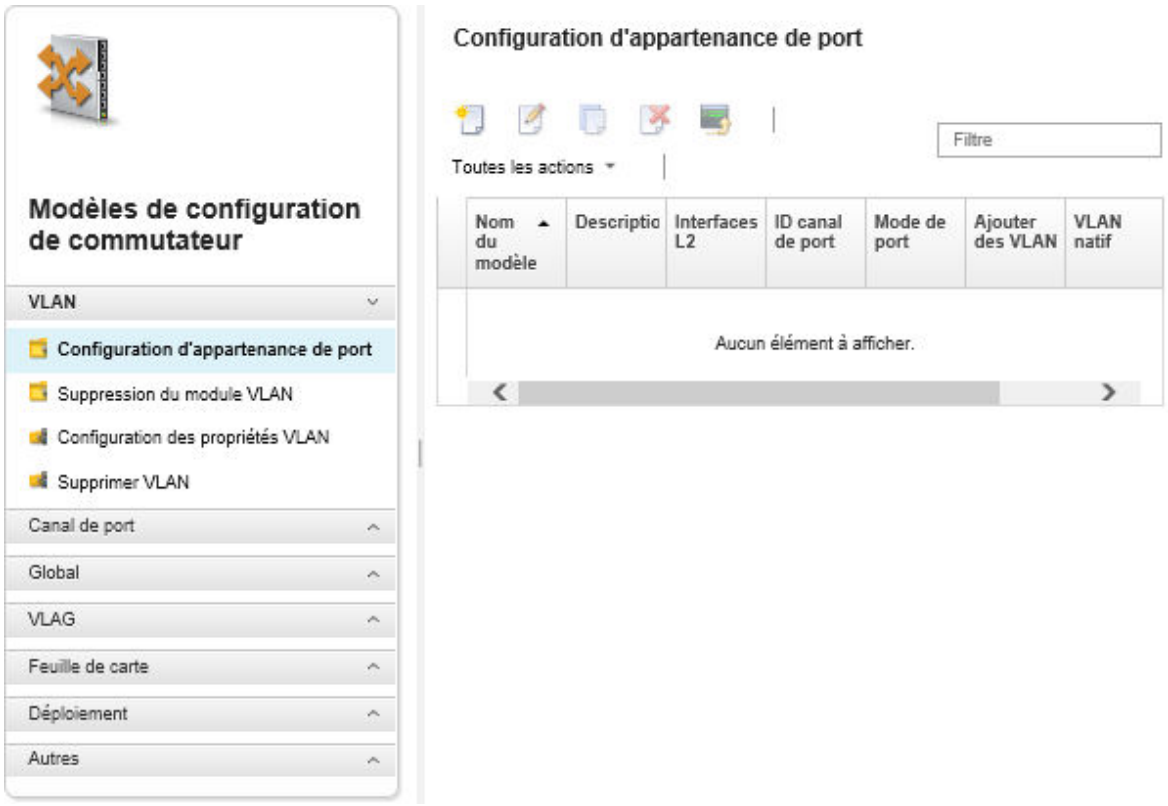
Avant de créer un modèle de configuration de commutateur, tenez compte des suggestions ci-dessous :

- Identifiez les groupes de commutateurs qui comportent les mêmes options matérielles et que vous souhaitez configurer de la même manière. Vous pouvez utiliser un modèle de configuration de commutateur pour appliquer les mêmes paramètres de configuration à plusieurs commutateurs, ce qui vous permet de contrôler une configuration commune depuis un seul emplacement.
- Identifiez les aspects de la configuration que vous souhaitez personnaliser (par exemple, global, canal de port ou paramètres VLAN).

Procédure

Procédez comme suit pour créer un modèle de configuration de commutateur.

Etape 1. Depuis la barre de menus XClarity Administrator, cliquez sur **Distribution → Modèles de configuration de commutateur**. La page Modèles de configuration de commutateur s'affiche.



Etape 2. Sélectionnez le type de modèle que vous souhaitez créer depuis la navigation de gauche.

Etape 3. Cliquez sur l'icône **Créer** ( ) pour afficher la boîte de dialogue Créer un nouveau modèle.

Les champs sont répertoriés dans cette boîte de dialogue varient selon le type de modèle.

Etape 4. Cliquez sur **Enregistrer** pour enregistrer le modèle, ou cliquez sur **Enregistrer et déployer** pour enregistrer et déployer immédiatement le modèle sur un ou plusieurs commutateurs d'armoire gérés

Pour plus d'informations sur le déploiement d'un modèle, voir Déployer des modèles de configuration de commutateur sur un commutateur cible.

Après avoir terminé

Si vous avez cliqué sur **Enregistrer et déployer**, la page Déployer un modèle de commutateur s'affiche. Depuis cette page, vous pouvez déployer le modèle de configuration de commutateur sur des commutateurs spécifiques.

Si vous avez cliqué sur **Enregistrer**, le modèle de configuration du commutateur est enregistré sur la page Modèles de configuration de commutateur. Depuis cette page, vous pouvez exécuter les actions suivantes sur les modèles de serveur sélectionnés :

- Pour afficher des détails sur le modèle, cliquez sur le nom de modèle dans la colonne Nom.
- Pour afficher une liste agrégée de tous les modèles, cliquez sur **Autres → Tous les modèles**.
- Déployez le modèle (voir Déployer des modèles de configuration de commutateur sur un commutateur cible).
- Copiez et modifiez un modèle en cliquant sur l'icône **Copier** ( ).

- Modifiez le modèle en cliquant sur l'icône **Modifier** ().

  Remarque : Les modifications apportées au modèle ne sont *pas automatiquement* redéployées sur les commutateurs sur lesquels le modèle d'origine a été déployé.

- Renommez le modèle en cliquant sur l'icône **Renommer** ().
- Supprimez le modèle en cliquant sur l'icône **Supprimer** ().

Définition de paramètres d'adhésion de port VLAN

Vous pouvez ajouter des ports physiques et des canaux de port à un ou plusieurs VLAN (pour un tronc) à l'aide du modèle de configuration d'appartenance de port VLAN.

Procédure

Procédez comme suit pour créer un modèle de configuration d'appartenance de port VLAN.

Etape 1. Depuis la barre de menus XClarity Administrator, cliquez sur **Distribution → Modèles de configuration de commutateur**. La page Modèles de configuration de commutateur s'affiche.

Etape 2. Cliquez sur **VLAN → Configuration d'adhésion de port** dans la navigation de gauche, puis cliquez sur l'icône **Créer** ().

Etape 3. Dans la boîte de dialogue Nouveau modèle, indiquez les informations suivantes.

Important : Vous devez indiquer une ou plusieurs interfaces physiques L2 ou ID de canal de port.

- Entrez un nom et une description de modèle.
- Indiquez une ou plusieurs interfaces L2 physiques valides. Vous pouvez spécifier une liste d'interfaces séparées par une virgule, une place d'identifiants séparés par un tiret ou une combinaison des deux, par exemple :
  - Ethernet1/10
  - Ethernet1/3,5,7,9
  - Ethernet1/5-10,21-32
  - Ethernet2/2-5,7,9,11-13
- Indiquez un ou plusieurs ID de canal de port valides (interfaces d'agrégation de port). Vous pouvez spécifier une liste de nombres séparés par une virgule, une plage de nombres séparés par un tiret, ou une combinaison des deux. Les valeurs et les plages peuvent être des nombres de 1 à 4096, par exemple :
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13
- Indiquez si le port accepte le trafic balisé ou non balisé. Les valeurs possibles sont les suivantes.
  - **accès**. Le port transporte le trafic d'une VLAN unique.
  - **tronc**. (par défaut) Le port transporte le trafic de tous les VLAN accessibles par le commutateur.
- Spécifiez un ou plusieurs identifiants VLAN à ajouter à la liste d'adhésion VLAN du port. Vous pouvez spécifier une liste de nombres séparés par une virgule, une plage de nombres séparés par un tiret, ou une combinaison des deux. Les valeurs et les plages peuvent être des nombres de 1 à 4096, par exemple :
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13

Remarques :

- Si le mode de port est défini sur « access, » seul le premier identifiant VLAN est utilisé. Par exemple, dans la plage `2-4,5,10-20`, seul `2` est utilisé.
- CNOS réserve les ID VLAN 4000 à 4095 par défaut. L'utilisation d'ID VLAN réservés (par CNOS ou un autre utilisateur) peut entraîner l'échec du déploiement de la configuration de commutateur.

- Indiquez un ID VLAN natif avec lequel le trafic non balisé est balisé. Il peut s'agir d'un nombre compris entre 1 et 4096.

  Remarques :
  - Ce champ est valide uniquement lorsque le mode de port est défini sur « trunk. »
  - Si tel n'est pas le cas, ou si l'ID est à l'extérieur des VLAN d'état final sur un port, le port n'autorisera pas le trafic non balisé.
- Sélectionnez **Créer des VLAN** pour créer des identifiants VLAN actuellement manquants sur le commutateur cible.

  Si un port appartient à un VLAN qui n'est pas créé, le port reste membre de ce VLAN, mais tout le trafic balisé avec cet ID VLAN et atteint le port n'est pas autorisé à passer.

Etape 4. Cliquez sur **Créer** pour enregistrer le modèle, ou cliquez sur **Créer et déployer** pour enregistrer et déployer immédiatement le modèle sur un ou plusieurs commutateurs d'armoire gérés.

Pour plus d'informations sur le déploiement d'un modèle, voir Déployer des modèles de configuration de commutateur sur un commutateur cible.

Définition des propriétés VLAN

Vous pouvez configurer des propriétés VLAN avancées à l'aide du modèle de configuration des propriétés de VLAN.

Procédure

Procédez comme suit pour créer un modèle de configuration des propriétés de VLAN.

Etape 1. Depuis la barre de menus XClarity Administrator, cliquez sur **Distribution → Modèles de configuration de commutateur**. La page Modèles de configuration de commutateur s'affiche.

Etape 2. Cliquez sur **VLAN → Configuration de propriétés VMAN** dans la navigation de gauche, puis cliquez sur l'icône **Créer** ( ).

Etape 3. Dans la boîte de dialogue Nouveau modèle, indiquez les informations suivantes.

- Entrez un nom et une description de modèle.
- Indiquez un ID VLAN sur lequel appliquer les modifications. Il peut s'agir d'un nombre compris entre 1 et 4095.

  Remarque : CNOS réserve les ID VLAN 4000 à 4095 par défaut. L'utilisation d'ID VLAN réservés (par CNOS ou un autre utilisateur) peut entraîner l'échec du déploiement de la configuration de commutateur.
- Indiquez un nom personnalisé pour le VLAN.
- Spécifiez si le VLAN est actif (activé) ou suspendu (désactivé).
- Choisissez si l'alimentation multidiffusion de l'IP (IPMC) sur le VLAN cible est contrôlée (activée) sur les interfaces IPv4 ou IPv6. Les valeurs possibles sont les suivantes.
  - **Désactiver**. IPv4 et IPv6 sont désactivés.
  - **Activer**. IPv4 et IPv6 sont activés.

- **Désactiver IPv4**.
- **Activer IPv4**
- **Désactiver IPv6**
- **Activer IPv6**

Cette action est additive, ce qui signifie que « Activer IPv4 » déployé sur « Désactiver » se traduit par « Activer IPv4, » mais un déploiement sur « Activer IPv6 » se traduit par « Activer. » L'inverse est vrai pour les options de désactivation.

Etape 4. Cliquez sur **Créer** pour enregistrer le modèle, ou cliquez sur **Créer et déployer** pour enregistrer et déployer immédiatement le modèle sur un ou plusieurs commutateurs d'armoire gérés.

Pour plus d'informations sur le déploiement d'un modèle, voir Déployer des modèles de configuration de commutateur sur un commutateur cible.

Suppression des paramètres VLAN

Vous pouvez retirer des interfaces des VLAN à l'aide du modèle de suppression de VLAN.

Procédure

Procédez comme suit pour créer un modèle de suppression VLAN.

Etape 1. Depuis la barre de menus XClarity Administrator, cliquez sur **Distribution → Modèles de configuration de commutateur**. La page Modèles de configuration de commutateur s'affiche.

Etape 2. Cliquez sur **VLAN → Suppression du module VLAN** dans la navigation de gauche, puis cliquez sur l'icône **Créer** ( ).

Etape 3. Dans la boîte de dialogue Nouveau modèle, indiquez les informations suivantes.

Important : Vous devez indiquer une ou plusieurs interfaces physiques L2 ou ID de canal de port.

- Entrez un nom et une description de modèle.
- Indiquez une ou plusieurs interfaces L2 physiques valides. Vous pouvez spécifier une liste d'interfaces séparées par une virgule, une place d'identifiants séparés par un tiret ou une combinaison des deux, par exemple :
  - Ethernet1/10
  - Ethernet1/1,3,5,7
  - Ethernet1/1-10,21-30
  - Ethernet2/1-5,7,9,11-13
- Indiquez un ou plusieurs ID de canal de port valides (interfaces d'agrégation de port). Vous pouvez spécifier une liste de nombres séparés par une virgule, une plage de nombres séparés par un tiret, ou une combinaison des deux. Les valeurs et les plages peuvent être des nombres de 1 à 4096, par exemple :
  - 10
  - 1.3,5,7
  - 1-10,21-32
  - 1-5,7,9,11-13
- Spécifiez un ou plusieurs identifiants VLAN à supprimer de la liste d'adhésion VLAN du port. Vous pouvez spécifier une liste de nombres séparés par une virgule, une plage de nombres séparés par un tiret, ou une combinaison des deux. Les valeurs et les plages peuvent être des nombres de 1 à 4096, par exemple :
  - 10
  - 1.3,5,7
  - 1-10,21-32

– 1-5,7,9,11-13

Remarque : Si le mode de port est défini sur « access », la suppression du VLAN provoque le passage du port dans VLAN 1.

Etape 4. Cliquez sur **Créer** pour enregistrer le modèle, ou cliquez sur **Créer et déployer** pour enregistrer et déployer immédiatement le modèle sur un ou plusieurs commutateurs d'armoire gérés.

Pour plus d'informations sur le déploiement d'un modèle, voir Déployer des modèles de configuration de commutateur sur un commutateur cible.

Suppression de VLAN

Vous pouvez supprimer des configurations VLAN du commutateur à l'aide du modèle de suppression de VLAN.

Procédure

Procédez comme suit pour créer un modèle de suppression de VLAN.

Etape 1. Depuis la barre de menus XClarity Administrator, cliquez sur **Distribution → Modèles de configuration de commutateur**. La page Modèles de configuration de commutateur s'affiche.

Etape 2. Cliquez sur **VLAN → Suppression de VLAN** dans la navigation de gauche, puis cliquez sur l'icône **Créer** ( ).

Etape 3. Dans la boîte de dialogue Nouveau modèle, indiquez les informations suivantes.

- Entrez un nom et une description de modèle.
- Spécifiez un ou plusieurs identifiants VLAN à supprimer de la liste d'adhésion VLAN du port. Vous pouvez spécifier une liste de nombres séparés par une virgule, une plage de nombres séparés par un tiret, ou une combinaison des deux. Les valeurs et les plages peuvent être des nombres de 1 à 4096, par exemple :
  – 10
  – 3,5,7,9
  – 5-10,21-32
  – 2-5,7,9,11-13

  Remarque : Vous ne pouvez pas supprimer des ID VLAN réservés.

Etape 4. Cliquez sur **Créer** pour enregistrer le modèle, ou cliquez sur **Créer et déployer** pour enregistrer et déployer immédiatement le modèle sur un ou plusieurs commutateurs d'armoire gérés.

Pour plus d'informations sur le déploiement d'un modèle, voir Déployer des modèles de configuration de commutateur sur un commutateur cible.

Définition des paramètres de canal de port basiques

Vous pouvez créer des agrégateurs de port et ajouter des ports aux agrégateurs à l'aide d'un modèle de configuration de base de canal de port.

Si le canal de port comporte des ports et que certains de ces ports font partie du modèle, leurs propriétés (priorité de port, mode et dépassement de délai) sont mises à jour avec les paramètres du modèle lorsque le modèle est déployé.

Procédure

Procédez comme suit pour créer un modèle de configuration de base de canal de port.

Etape 1. Depuis la barre de menus XClarity Administrator, cliquez sur **Distribution → Modèles de configuration de commutateur**. La page Modèles de configuration de commutateur s'affiche.

Etape 2. Cliquez sur **Canal de port → Configuration de base** dans la navigation de gauche, puis cliquez sur l'icône **Créer** ( ).

Etape 3. Dans la boîte de dialogue Nouveau modèle, indiquez les informations suivantes.

- Entrez un nom et une description de modèle.
- Indiquez une ou plusieurs interfaces L2 physiques valides. Vous pouvez spécifier une liste d'interfaces séparées par une virgule, une place d'identifiants séparés par un tiret ou une combinaison des deux, par exemple :
  - Ethernet1/10
  - Ethernet1/3,5,7,9
  - Ethernet1/5-10,21-32
  - Ethernet2/2-5,7,9,11-13
- Indiquez l'ID de canal de port (interface d'agrégation de ports) à créer ou à mettre à jour. Il peut s'agir d'un nombre compris entre 1 et 4095.
- Spécifiez le mode de port LACP (Link Aggregation Control Protocol). Les valeurs possibles sont les suivantes.
  - **Active**. (par défaut) Active le LACP sans condition
  - **Passive**. Active le LACP uniquement si un appareil LCAP est détecté.
  - **Static**. Désactive LCAP.

  Remarque : Les paramètres Active et Passive peuvent être associés dans le même agrégateur, mais Static.
- Spécifiez la priorité du port LACP. Il peut s'agir d'un nombre compris entre 1 et 65535.

  Remarque : La priorité de port LACP est utilisée avec le numéro de port pour former l'ID de port LACP.
- Indiquez le mode de dépassement de délai LACP avant que LCAP passe en mode individuel. Les valeurs possibles sont les suivantes.
  - **Long**. (par défaut) 90 secondes
  - **Court**. 3 secondes

Etape 4. Cliquez sur **Créer** pour enregistrer le modèle, ou cliquez sur **Créer et déployer** pour enregistrer et déployer immédiatement le modèle sur un ou plusieurs commutateurs d'armoire gérés.

Pour plus d'informations sur le déploiement d'un modèle, voir Déployer des modèles de configuration de commutateur sur un commutateur cible.

Définition des paramètres avancés port-canal

Vous pouvez configurer des propriétés de canal de port avancées à l'aide du modèle de configuration avancé de canal de port.

Procédure

Procédez comme suit pour créer un modèle de configuration avancé de canal de port.

Etape 1. Depuis la barre de menus XClarity Administrator, cliquez sur **Distribution → Modèles de configuration de commutateur**. La page Modèles de configuration de commutateur s'affiche.

Etape 2. Cliquez sur **Canal de port → Configuration avancée** dans la navigation de gauche, puis cliquez sur l'icône **Créer** ( ).

Etape 3. Dans la boîte de dialogue Nouveau modèle, indiquez les informations suivantes.

- Entrez un nom et une description de modèle.
- Indiquez un ID de canal de port (interface d'agrégation de ports) à mettre à jour. Il peut s'agir d'un nombre compris entre 1 et 4095.
- Indiquez si les ports individuels restent actifs lorsque le protocole LACP échoue. Les valeurs possibles sont les suivantes.
  - **Active**. (par défaut) Active le LACP sans condition.
  - **Interrompre**. Désactive LACP.
- Spécifiez le nombre minimum de liens à configurer pour que le canal de port soit considéré opérationnel. Il peut s'agir d'un nombre compris entre 1 et 32.

Etape 4. Cliquez sur **Créer** pour enregistrer le modèle, ou cliquez sur **Créer et déployer** pour enregistrer et déployer immédiatement le modèle sur un ou plusieurs commutateurs d'armoire gérés.

Pour plus d'informations sur le déploiement d'un modèle, voir Déployer des modèles de configuration de commutateur sur un commutateur cible.

Suppression de canaux de port

Vous pouvez supprimer des canaux de port du commutateur à l'aide du modèle de suppression de canal de port.

Procédure

Procédez comme suit pour créer un modèle de suppression de canal de port.

Etape 1. Depuis la barre de menus XClarity Administrator, cliquez sur **Distribution → Modèles de configuration de commutateur**. La page Modèles de configuration de commutateur s'affiche.

Etape 2. Cliquez sur **Canal de port → Supprimer un canal de port** dans la navigation de gauche, puis cliquez sur l'icône **Créer** ( )

Etape 3. Dans la boîte de dialogue Nouveau modèle, indiquez les informations suivantes.

- Entrez un nom et une description de modèle.
- Indiquez un ou plusieurs ID de canal de port (interfaces d'agrégation de port) à supprimer. Vous pouvez spécifier une liste de nombres séparés par une virgule, une plage de nombres séparés par une virgule, ou une combinaison des deux. Les valeurs et les plages peuvent être des nombres de 1 à 4096, par exemple :
  - 10
  - 3,5,7,9
  - 5-10,21-32
  - 2-5,7,9,11-13

Etape 4. Cliquez sur **Créer** pour enregistrer le modèle, ou cliquez sur **Créer et déployer** pour enregistrer et déployer immédiatement le modèle sur un ou plusieurs commutateurs d'armoire gérés.

Pour plus d'informations sur le déploiement d'un modèle, voir Déployer des modèles de configuration de commutateur sur un commutateur cible.

Configuration de paramètres de commutateur généraux

Vous pouvez configurer les propriétés de commutateurs générales à l'aide du modèle de configuration générique global.

Procédure

Procédez comme suit pour créer un modèle de configuration générique global de commutateur.

Etape 1. Depuis la barre de menus XClarity Administrator, cliquez sur **Distribution → Modèles de configuration de commutateur**. La page Modèles de configuration de commutateur s'affiche.

Etape 2. Cliquez sur **Global → Configuration générique** dans la navigation de gauche, puis cliquez sur l'icône **Créer** ( ).

Etape 3. Dans la boîte de dialogue Nouveau modèle, indiquez les informations suivantes.

- Entrez un nom et une description de modèle.
- Indiquez la priorité système LACP qui est utilisée pour générer l'ID système LACP. Il peut s'agir d'un nombre compris entre 1 et 65535.
- Choisissez si le marquage VLAN natif doit être activé. Les valeurs possibles sont les suivantes.
  - **Entrée et sortie**
  - **Sortie uniquement**

  Remarque : Cette propriété est prise en charge par CNOS 10.10.1 et versions ultérieures.

Etape 4. Cliquez sur **Créer** pour enregistrer le modèle, ou cliquez sur **Créer et déployer** pour enregistrer et déployer immédiatement le modèle sur un ou plusieurs commutateurs d'armoire gérés.

Pour plus d'informations sur le déploiement d'un modèle, voir Déployer des modèles de configuration de commutateur sur un commutateur cible.

Configuration de paramètres d'interface L2 globaux

Vous pouvez configurer les propriétés de marquage VLAN sur les interfaces L2 à l'aide du modèle de configuration d'interface L2.

Procédure

Procédez comme suit pour créer un modèle de configuration d'interface L2.

Etape 1. Depuis la barre de menus XClarity Administrator, cliquez sur **Distribution → Modèles de configuration de commutateur**. La page Modèles de configuration de commutateur s'affiche.

Etape 2. Cliquez sur **Global → Configuration d'interface L2** dans le volet de gauche, puis cliquez sur l'icône **Créer** ( ).

Etape 3. Dans la boîte de dialogue Nouveau modèle, indiquez les informations suivantes.

- Entrez un nom et une description de modèle.
- Indiquez une ou plusieurs interfaces L2 physiques valides. Vous pouvez spécifier une liste d'interfaces séparées par une virgule, une place d'identifiants séparés par un tiret ou une combinaison des deux, par exemple :
  - Ethernet1/10
  - Ethernet1/3,5,7,9
  - Ethernet1/5-10,21-32
  - Ethernet2/2-5,7,9,11-13
- Choisissez si le marquage VLAN natif doit être activé. Les valeurs possibles sont les suivantes.
  - **Entrée et sortie**
  - **Sortie uniquement**

  Remarque : Cette propriété est prise en charge par CNOS 10.10.1 et versions ultérieures.
- Choisissez d'activer ou de désactiver la prise en charge de la tunnellisation (QinQ).

  Remarque : Cette propriété est prise en charge par CNOS 10.10.1 et versions ultérieures.

Etape 4. Cliquez sur **Créer** pour enregistrer le modèle, ou cliquez sur **Créer et déployer** pour enregistrer et déployer immédiatement le modèle sur un ou plusieurs commutateurs d'armoire gérés.

Pour plus d'informations sur le déploiement d'un modèle, voir Déployer des modèles de configuration de commutateur sur un commutateur cible.

Définition de paramètres de pair VLAG

Vous pouvez configurer des homologues VLAG à l'aide du modèle de configuration d'homologues VLAG.

Procédure

Procédez comme suit pour créer un modèle de configuration d'homologues VLAG.

Etape 1. Depuis la barre de menus XClarity Administrator, cliquez sur **Distribution → Modèles de configuration de commutateur**. La page Modèles de configuration de commutateur s'affiche.

Etape 2. Cliquez sur **VLAG → Configuration des homologues** dans la navigation de gauche, puis cliquez sur l'icône **Créer** ( ).

Etape 3. Dans la boîte de dialogue Nouveau modèle, indiquez les informations suivantes.

- Entrez un nom et une description de modèle.
- Choisissez d'activer ou de désactiver le VLAG.
- Pour Homologue 1 et Homologue 2, renseignez les zones ci-après. Les zones des deux homologues doivent être remplies.
  - Indiquez l'adresse IIPv4 ou IPv6 de l'homologue VLAG à utiliser pour la vérification de la santé.
  - Indiquez l'ID du canal de port qui est utilisé entre les deux homologues. Il peut s'agir d'un nombre compris entre 1 et 4095.
  - Indiquez le VRF utilisé pour le contrôle de santé (par exemple, management, default ou customVRF).

Etape 4. Cliquez sur **Créer** pour enregistrer le modèle, ou cliquez sur **Créer et déployer** pour enregistrer et déployer immédiatement le modèle sur un ou plusieurs commutateurs d'armoire gérés.

Pour plus d'informations sur le déploiement d'un modèle, voir Déployer des modèles de configuration de commutateur sur un commutateur cible.

Définition des paramètres d'instance VLAG

Vous pouvez créer ou mettre à jour une instance VLAG à l'aide du modèle de configuration d'instance VLAG. Une instance VLAG est un appareil qui est connecté aux deux commutateurs (généralement via une agrégation de port) sur lesquels la VLAG s'affiche sous la forme d'un appareil unique.

Procédure

Procédez comme suit pour créer un modèle de configuration d'instance VLAG.

Etape 1. Depuis la barre de menus XClarity Administrator, cliquez sur **Distribution → Modèles de configuration de commutateur**. La page Modèles de configuration de commutateur s'affiche.

Etape 2. Cliquez sur **VLAG → Configuration d'instance** dans la navigation de gauche, puis cliquez sur l'icône **Créer** ( ).

Etape 3. Dans la boîte de dialogue Nouveau modèle, indiquez les informations suivantes.

- Entrez un nom et une description de modèle.
- Spécifiez l'identifiant VLAG. Il peut s'agir d'un nombre compris entre 1 et 64.
- Indiquez l'ID du canal de port qui est connecté à homologue 1 et à l'homologue 2. Il peut s'agir d'un nombre compris entre 1 et 4095.

- Choisissez d'activer ou de désactiver l'instance VLAG.

Etape 4. Cliquez sur **Créer** pour enregistrer le modèle, ou cliquez sur **Créer et déployer** pour enregistrer et déployer immédiatement le modèle sur un ou plusieurs commutateurs d'armoire gérés.

Pour plus d'informations sur le déploiement d'un modèle, voir Déployer des modèles de configuration de commutateur sur un commutateur cible.

Définition des paramètres VLAG avancés

Vous pouvez configurer des propriétés VLAG avancées à l'aide du modèle de configuration avancé de VLAG.

Procédure

Procédez comme suit pour créer un modèle de configuration avancé de VLAG.

Etape 1. Depuis la barre de menus XClarity Administrator, cliquez sur **Distribution → Modèles de configuration de commutateur**. La page Modèles de configuration de commutateur s'affiche.

Etape 2. Cliquez sur **VLAG → Configuration avancée** dans la navigation de gauche, puis cliquez sur l'icône **Créer** ( ).

Etape 3. Dans la boîte de dialogue Nouveau modèle, indiquez les informations suivantes.

- Entrez un nom et une description de modèle.
- Spécifiez la priorité utilisée pour contrôler l'homologue qui est principal. Il peut s'agir d'un nombre compris entre 1 et 65535.

  Si aucun intervalle n'est spécifié, la priorité par défaut du commutateur est utilisé. Pour CNOS, la valeur par défaut est 0.
- Spécifiez le délai autorisé, en secondes, pour le VLAG à mettre en ligne après un redémarrage simultané. Il peut s'agir d'un nombre compris entre 240 et 3600.

  Si aucun intervalle n'est spécifié, l'intervalle par défaut du commutateur est utilisé. Pour CNOS, la valeur par défaut est 300.
- Indiquez l'ID de niveau qui est utilisé pour différencier les paramètres VLAG dans le même réseau. Il peut s'agir d'un nombre compris entre 1 et 512.
- Indiquez l'intervalle de retard de démarrage du vLAG, en secondes, qui est utilisé pour différer l'acheminement des ports après des rechargements d'homologue. Il peut s'agir d'un nombre compris entre 0 et 3600.

  Si aucun intervalle n'est spécifié, l'intervalle par défaut du commutateur est utilisé. Pour CNOS, la valeur par défaut est 120.
- Indiquez le nombre de tentatives de maintien opérationnel du VLAG (messages de salutation sans réponse) avant l'échec du VLAG. Il peut s'agir d'un nombre compris entre 1 et 24.

  Si aucun intervalle n'est spécifié, l'intervalle par défaut du commutateur est utilisé. Pour CNOS, la valeur par défaut est 3.
- Spécifiez l'intervalle, en secondes, entre les tentatives de maintien opérationnel du vLAG. Il peut s'agir d'un nombre compris entre 2 et 300.

  Si aucun intervalle n'est spécifié, l'intervalle par défaut du commutateur est utilisé. Pour CNOS, la valeur par défaut est 5.
- Spécifiez l'intervalle, en secondes, entre les nouvelles tentatives de maintien opérationnel du vLAG. Il peut s'agir d'un nombre compris entre 1 et 300.

  Si aucun intervalle n'est spécifié, l'intervalle par défaut du commutateur est utilisé. Pour CNOS, la valeur par défaut est 30.

Etape 4. Cliquez sur **Créer** pour enregistrer le modèle, ou cliquez sur **Créer et déployer** pour enregistrer et déployer immédiatement le modèle sur un ou plusieurs commutateurs d'armoire gérés.

Pour plus d'informations sur le déploiement d'un modèle, voir Déployer des modèles de configuration de commutateur sur un commutateur cible.

Suppression d'une instance de VLAG

Vous pouvez supprimer une instance VLAG à l'aide du modèle Supprimer une instance de VLAG.

Procédure

Procédez comme suit pour créer un modèle Supprimer une instance de VLAG.

Etape 1. Depuis la barre de menus XClarity Administrator, cliquez sur **Distribution → Modèles de configuration de commutateur**. La page Modèles de configuration de commutateur s'affiche.

Etape 2. Cliquez sur **VLAG → Suppression de l'instance** dans la navigation de gauche, puis cliquez sur l'icône **Créer** ( ).

Etape 3. Dans la boîte de dialogue Nouveau modèle, indiquez les informations suivantes.

- Entrez un nom et une description de modèle.
- Indiquez l'ID unique de l'instance de VLAG. Il peut s'agir d'un nombre compris entre 1 et 64.

Etape 4. Cliquez sur **Créer** pour enregistrer le modèle, ou cliquez sur **Créer et déployer** pour enregistrer et déployer immédiatement le modèle sur un ou plusieurs commutateurs d'armoire gérés.

Pour plus d'informations sur le déploiement d'un modèle, voir Déployer des modèles de configuration de commutateur sur un commutateur cible.

Définition une topologie feuille et tronc

Vous pouvez vérifier la topologie physique et déployer une configuration SpineLeaf (L3 fabric) sur les commutateurs gérés à l'aide du modèle d'Assistant topologie feuille et tronc.

Procédure

Procédez comme suit pour créer un modèle d'Assistant topologie feuille et tronc.

Etape 1. Depuis la barre de menus XClarity Administrator, cliquez sur **Distribution → Modèles de configuration de commutateur**. La page Modèles de configuration de commutateur s'affiche.

Etape 2. Cliquez sur **Feuille et tronc → Assistant de topologie** dans la navigation de gauche, puis cliquez sur l'icône **Créer** ( ).

Etape 3. Dans la boîte de dialogue Nouveau modèle, indiquez les informations suivantes.

- Entrez un nom et une description de modèle.
- Indiquez le numéro de système autonome (AS) pour le protocole BGP (Border Gateway) qui s'exécute sur le commutateur. Il peut s'agir d'un nombre compris entre 1 et 4294967295.

  Remarque : Cette configuration est prise en charge par CNOS 10.9.3 et versions ultérieures.
- Indiquez si vous souhaitez autoriser les liaisons uniques entre les commutateurs.

  Généralement, le déploiement échoue s'il n'y a pas au moins deux liaisons entre les commutateurs feuille et tronc.

Etape 4. Cliquez sur **Créer** pour enregistrer le modèle, ou cliquez sur **Créer et déployer** pour enregistrer et déployer immédiatement le modèle sur un ou plusieurs commutateurs d'armoire gérés.

Pour plus d'informations sur le déploiement d'un modèle, voir Déployer des modèles de configuration de commutateur sur un commutateur cible.

Déployer des modèles de configuration de commutateur sur un commutateur cible

Vous pouvez définir des paramètres de port VLAN en créant un modèle de configuration de port VLAN.

À propos de cette tâche

Il existe trois types de déploiements :

- **Normal**. Déploie les paramètres de configuration de commutateur sur un ou plusieurs commutateurs d'armoire dans une architecture à couches basique.
- **VLAG**. Déploie les paramètres de configuration de commutateur sur deux commutateurs exactement, qui prennent en charge une architecture VLAG. Les commutateurs doivent disposer du même modèle et de la même version de logiciel.
- **Feuille et tronc (spine-leaf)**. Des modèles de déploiement sur un ou plusieurs commutateurs de feuille et tronc.

Procédure

Pour déployer un modèle de configuration de commutateur sur un ou plusieurs commutateurs gérés, procédez comme suit.

Etape 1. Depuis la barre de menus XClarity Administrator, cliquez sur **Distribution → Modèles de configuration de commutateur**. La page Modèles de configuration de commutateur s'affiche.

Etape 2. Sélectionnez un ou plusieurs modèles de configuration de commutateur à déployer.

Etape 3. Cliquez sur l'icône **Déployer** ( ) pour afficher la boîte de dialogue Modèle de déploiement.

Etape 4. Sélectionnez un ou plusieurs commutateurs sur lesquels vous souhaitez déployer les modèles.

Seuls les commutateurs compatibles avec les modèles sélectionnés sont répertoriés.

Etape 5. Cliquez sur **Déployer**. Une boîte de dialogue répertoriant l'état de déploiement de chaque commutateur sélectionné s'affiche.

Etape 6. Cliquez à nouveau sur **Déployer** pour démarrer le processus de déploiement.

Remarque : Le déploiement peut prendre plusieurs minutes.

Après avoir terminé

Vous pouvez afficher l'historique de déploiement (voir Afficher l'historique de déploiement de la configuration de commutateur).

Afficher l'historique de déploiement de la configuration de commutateur

Vous pouvez afficher les informations sur les modèles de configuration du commutateur qui ont été déployées sur les commutateurs gérés, y compris le nom du modèle, le type du modèle, l'horodatage et les commutateurs sur lesquels elles ont été déployées. Chaque déploiement contient un instantané du modèle tel qu'il était au moment de son déploiement.

Procédure

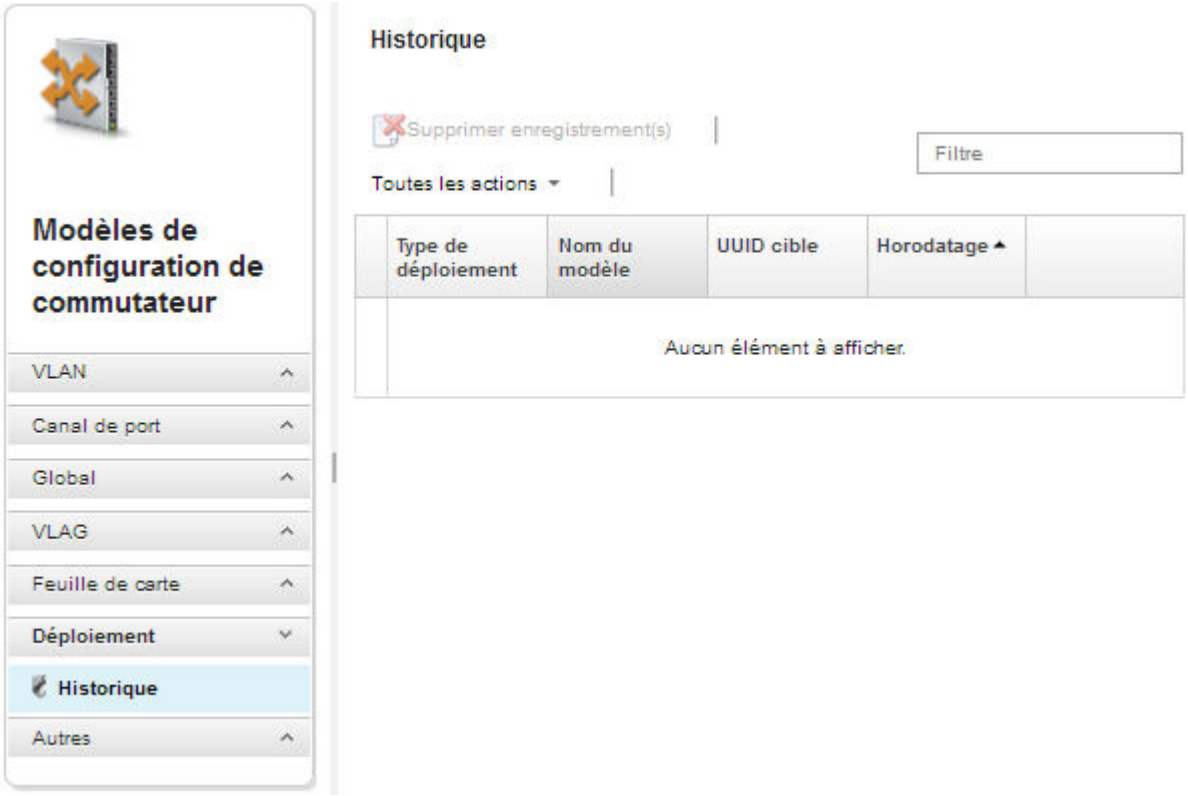
Procédez comme suit pour afficher l'historique de déploiement de configuration de commutateur.

Etape 1. Depuis la barre de menus XClarity Administrator, cliquez sur **Distribution → Modèles de configuration de commutateur**. La page Modèles de configuration de commutateur s'affiche.

Etape 2. Développez **Déploiement**, puis cliquez sur **Historique** dans la navigation de gauche pour afficher un tableau des modèles déployés.

La colonne **État** indique si le déploiement de la configuration a abouti. Les états possibles sont les suivants :

- **Succès**. Le déploiement de la configuration sur tous les commutateurs cible a abouti.
- **Avertissement**. Le déploiement de la configuration sur un ou plusieurs commutateurs cible s'est terminé avec des avertissements.
- **Échec**. Le déploiement de la configuration sur un ou plusieurs commutateurs cible a échoué.



Après avoir terminé

- Pour afficher des informations sur chaque modèle déployé, notamment ce qui a été déployé et ce qui a abouti ou échoué, cliquez sur le nom de modèle dans le tableau.
- Effacez l'historique de déploiement en sélectionnant un déploiement et en cliquant sur l'icône **Supprimer** ( ).

Chapitre 13. Mise à jour du microprogramme sur les appareils gérés

À partir de l'interface Web de Lenovo XClarity Administrator, vous pouvez télécharger, installer et gérer des mises à jour de microprogramme pour les appareils gérés, y compris les châssis, les serveurs, les systèmes de stockage et les commutateurs. Vous pouvez affecter des stratégies de conformité de microprogramme aux appareils gérés pour garantir la conformité du microprogramme figurant sur ces appareils. Vous pouvez également créer et éditer des stratégies de conformité de microprogramme lorsque les niveaux de microprogramme validés ne correspondent pas aux stratégies prédéfinies suggérées.

En savoir plus :

- XClarity Administrator : amélioration de l'efficacité lors de la mise à jour du microprogramme
- Meilleures pratiques concernant la mise à jour du microprogrammes et des pilotes Lenovo ThinkSystem
- XClarity Administrator : du serveur au cluster
- XClarity Administrator : mises à jour de microprogramme
- XClarity Administrator : Distribution des mises à jour de sécurité du microprogramme

Avant de commencer

La mise à jour du microprogramme et la mise à jour des pilotes de périphérique sont des processus distincts dans XClarity Administrator ; il n'y a pas de connexion entre ces processus. XClarity Administrator ne conserve pas la conformité entre les microprogrammes et les pilotes d'appareils sur les appareils gérés, même s'il est recommandé de mettre à jour les pilotes de périphérique en même temps que le microprogramme.

À propos de cette tâche

Remarque : Un système d'exploitation n'est pas requis pour mettre à jour un microprogramme. Pour les serveurs nus, assurez-vous que le serveur est mis hors tension avant de procéder à la mise à jour du microprogramme.

Vous pouvez gérer et appliquer un des mises à jour de microprogramme pour les appareils gérés suivants.

- **Chassis**. Mises à jour de module CMM
- **Serveurs ThinkAgile, ThinkSystem, System x, Converged, Flex System et NeXtScale**. Contrôleur de gestion de la carte mère, UEFI, DSA, mezzanine et mises à jour d'adaptateur
- **Commutateurs RackSwitch et Flex System**
- **Dispositifs de stockage Lenovo Storage et ThinkSystem DM**
- **Périphériques de bandothèque IBM TS4300**

Le microprogramme des appareils suivants ne peut pas être mis à jour via XClarity Administrator.

- **Serveurs ThinkServer**. Pour plus d'informations sur la mise à jour du microprogramme, voir la documentation fournie avec le serveur.
- **Nœuds de traitement Flex Power Systems**. Plusieurs méthodes vous permettent de mettre à jour le microprogramme des nœuds de traitement Flex Power Systems. Pour plus d'informations, voir Documentation en ligne Nœuds de traitement p260/p460 IBM Flex System. Le processus pour les autres nœuds de traitement Flex Power Systems est similaire.
- **Commutateurs Flex en mode empilé ou en mode protégé**. Vous *ne pouvez pas* mettre à jour le microprogramme des commutateurs empilés. La mise à jour de microprogramme est désactivée pour tous les commutateurs qui sont empilés.

- **Commutateurs Flex**. Si vous utilisez le commutateur suivant, voir la documentation fournie avec celui-ci pour plus d'informations sur la mise à jour du microprogramme.
  - Module d'extension de matrice Cisco Nexus B22

Procédure

La figure suivante illustre le flux de travaux relatif à la mise à jour de microprogramme sur des appareils gérés.

Etape 1. **Gérer le référentiel des mises à jour de microprogramme**

Le *référentiel des mises à jour de microprogramme* contient un catalogue de mises à jour disponibles, ainsi que les modules de mise à jour qui peuvent être appliqués aux appareils gérés.

Le *catalogue* contient des informations sur les mises à jour de microprogramme actuellement disponibles pour tous les appareils pris en charge par XClarity Administrator. Le catalogue organise les mises à jour du microprogramme par type de dispositif. Lorsque vous actualisez le catalogue, XClarity Administrator extrait des informations sur les dernières mises à jour de microprogramme disponibles à partir du site Web de Lenovo (y compris les fichiers de métadonnées .xml ou .json et Readme .txt) et stocke ces informations dans le référentiel des mises à jour de microprogramme. Le fichier de contenu (.exe) n'est pas téléchargé. Pour plus d'informations sur l'actualisation du catalogue, voir Actualisation du catalogue produit.

Si de nouvelles mises à jour de microprogramme sont disponibles, vous devez d'abord télécharger les modules de mise à jour avant de pouvoir mettre à jour ce microprogramme sur les appareils gérés. L'actualisation du catalogue n'entraîne pas le téléchargement automatique des modules de mise à jour. Le tableau **Catalogue produit** sur la page Référentiel des mises à jour de microprogramme identifie les modules de mise à jour qui ont été téléchargés et ceux qui sont disponibles pour téléchargement.

Vous pouvez télécharger les mises à jour du microprogramme de plusieurs manières différentes :

- **Modules de référentiel des mises à jour de microprogramme**

  Les modules de référentiel de mise à jour de microprogramme sont des collections des microprogrammes les plus récents et disponibles au moment de la publication de XClarity Administrator pour les appareils principaux pris en charge, ainsi qu'une stratégie de conformité de microprogramme actualisée par défaut. Ces modules de référentiel sont importés, puis appliqués à partir de la page Mettre à jour le serveur de gestion. Lorsque vous appliquez un module de référentiel de mises à jour de microprogramme, chaque module de mise à jour présent dans ce module est ajouté au référentiel de mises à jour de microprogramme, et une stratégie de conformité de microprogramme est automatiquement créée pour tous les appareils gérables. Vous pouvez copier cette stratégie prédéfinie, mais vous ne pouvez pas la modifier.

  Les modules de référentiel suivants sont disponibles.

  - **lnvgy_sw_lxca_cmmswitchrepo***x-x.x.x*_**anyos_noarch**. Contient des mises à jour de microprogramme pour tous les modules CMM et les commutateurs Flex System.
  - **lnvgy_sw_lxca_storagerackswitchrepo***x-x.x.x*_**anyos_noarch**. Contient des mises à jour de microprogramme pour tous les commutateurs RackSwitch et les dispositifs Lenovo Storage.

- **lnvgy_sw_lxca_systemxrepo***x-x.x.x*_**anyos_noarch**. Contient des mises à jour de microprogramme pour tous les serveurs des séries Converged HX, Flex System, NeXtScale et System x.
- **lnvgy_sw_thinksystemrepo***x-x.x.x*_**anyos_noarch**. Contient des mises à jour de microprogramme pour tous les serveurs ThinkSystem et ThinkAgile.
- **lnvgy_sw_lxca_thinksystemv2repo***x-x.x.x*_**anyos_noarch**. Contient des mises à jour de microprogramme pour tous les serveurs ThinkSystem V2 et ThinkAgile.
- **lnvgy_sw_lxca_thinksystemv3repo***x-x.x.x*_**anyos_noarch**. Contient des mises à jour de microprogramme pour tous les serveurs ThinkSystem V3 et ThinkAgile.

Vous pouvez déterminer si des modules de référentiel des mises à jour de microprogramme sont stockés dans le référentiel dans la colonne **État du téléchargement** sur la page Mettre à jour le serveur de gestion. Cette colonne contient les valeurs suivantes :

- **Téléchargé**. Le module de référentiel des mises à jour de microprogramme est stocké dans le référentiel.
- **Non téléchargé**. Le module de référentiel des mises à jour de microprogramme est disponible, mais pas stocké dans le référentiel.

- **UpdateXpress System Packs (UXSPs)**

  Remarque : Pour les serveurs équipés de XCC2, ces packages sont appelés modules (bundles) de microprogramme. *Bundle* est utilisé dans les noms de package et les noms de stratégie prédéfinis.

  Les modules UXSP contiennent les mises à jour de microprogramme et de pilote de périphérique disponibles les plus récentes, organisées par système d'exploitation. Lorsque vous téléchargez des modules UXSP, XClarity Administrator télécharge l'UXSP applicable à la version indiquée dans le catalogue et stocke les modules de mise à jour dans le référentiel des mises à jour de microprogramme. Lorsque vous téléchargez un UXSP, chaque mise à jour de microprogramme dans le UXSP est ajoutée au référentiel des mises à jour de microprogramme et est répertoriée sous l'onglet **Mises à jour individuelles**, et une stratégie de conformité du microprogramme par défaut est automatiquement créée pour tous les appareils gérables à l'aide des noms suivants. Vous pouvez copier cette stratégie prédéfinie, mais vous ne pouvez pas la modifier.
  - *{uxsp-version}-{date}-{nom-serveur-abrégé}***-UXSP** (par exemple, `v1.50-2017-11-22- SD530-UXSP`)
  - *{uxsp-version}-{numérodebuild}-{nom-serveur-abrégé}***-bundle** (par exemple, `22a.0-kaj92va-SR650V3-bundle`)

  Remarque : Lorsque vous téléchargez ou importez des UXSP depuis la page Mises à jour de microprogramme : référentiel, seules les mises à jour de microprogramme sont téléchargées et stockées dans le référentiel. Les mises à jour de pilote de périphérique sont supprimées. Pour plus d'informations sur le téléchargement ou de l'importation des mises à jour de pilote de périphérique Windows à l'aide de UXSP, voir Gestion du référentiel des pilotes de périphérique SE.

  Vous pouvez déterminer si les UXSP sont stockés dans le référentiel des mises à jour de microprogramme à partir de la colonne **État du téléchargement** sous l'onglet **Mises à jour individuelles** de la page Mises à jour de microprogramme : référentiel. Cette colonne contient les valeurs suivantes :

  - **Téléchargé**. L'ensemble du contenu du module de mise à jour ou la mise à jour de microprogramme individuelle est stocké dans le référentiel.
  - *x* **sur** *y* **téléchargés**. Une partie seulement des mises à jour de microprogramme présentes dans le module de mise à jour est stockée dans le référentiel. Les nombres entre

parenthèses indiquent le nombre de mises à jour disponibles et le nombre de mises à jour stockées, ou bien il n'existe aucune mise à jour pour le type d'appareil spécifique.

– **Non téléchargé**. La totalité du contenu du module de mise à jour ou la mise à jour de microprogramme individuelle est disponible, mais pas stockée dans le référentiel.

- **Mises à jour individuelles du microprogramme**

  Vous pouvez télécharger des modules de mise à jour de microprogramme individuels. Lorsque vous téléchargez des modules de mise à jour de microprogramme, XClarity Administrator télécharge la mise à jour applicable à la version indiquée dans le catalogue et stocke les modules de mise à jour dans le référentiel des mises à jour de microprogramme. Vous pouvez ensuite créer des stratégies de conformité de microprogramme à l'aide de ces modules de mise à jour pour chacun des appareils gérés.

  Remarque : Les mises à jour de microprogramme principales (telles que celles de type contrôleur de gestion, UEFI et pDSA) sont indépendantes du système d'exploitation. Les modules de mise à jour de microprogramme pour les systèmes d'exploitation RHEL 6 ou SLES 11 sont utilisés pour mettre à jour les nœuds de traitement et les serveurs rack. Pour plus d'informations sur les modules de mise à jour de microprogramme qui doivent être utilisés pour vos serveurs gérés, voir Téléchargement des mises à jour de microprogramme.

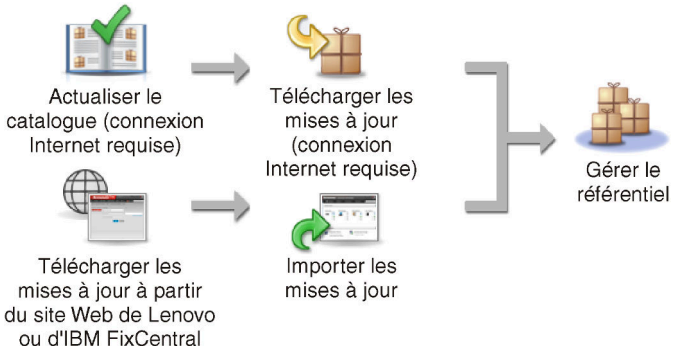
  Vous pouvez déterminer si des *mises à jour de microprogramme* spécifiques sont stockées dans le référentiel des mises à jour de microprogramme à partir de la colonne **État du téléchargement** sous l'onglet **Mises à jour individuelles** de la page Mises à jour de microprogramme : référentiel. Cette colonne contient les valeurs suivantes.

  – **Téléchargé**. L'ensemble du contenu du module de mise à jour ou la mise à jour de microprogramme individuelle est stocké dans le référentiel.

  – *x* **sur** *y* **téléchargés**. Une partie seulement des mises à jour de microprogramme présentes dans le module de mise à jour est stockée dans le référentiel. Les nombres entre parenthèses indiquent le nombre de mises à jour disponibles et le nombre de mises à jour stockées, ou bien il n'existe aucune mise à jour pour le type d'appareil spécifique.

  – **Non téléchargé**. La totalité du contenu du module de mise à jour ou la mise à jour de microprogramme individuelle est disponible, mais pas stockée dans le référentiel.

XClarity Administrator doit être connecté à Internet pour actualiser le catalogue et télécharger les mises à jour de microprogramme. S'il n'est pas connecté à Internet, vous pouvez télécharger manuellement les fichiers sur un poste de travail disposant d'un accès réseau à l'hôte XClarity Administrator à l'aide d'un navigateur Web, puis importer les fichiers dans le référentiel des mises à jour de microprogramme.



Lorsque vous importez manuellement des mises à jour du microprogramme dans XClarity Administrator, vous devez inclure les fichiers requis suivants : contenu (image et MIB), métadonnées, historique des modifications et Readme. Par exemple :

- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.tgz
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.xml
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.chg
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.txt

Attention :

- Importez uniquement ces fichiers requis. N'importez pas d'autres fichiers susceptibles de se trouver sur les sites Web de téléchargement du microprogramme.
- Si vous n'incluez pas le fichier XML dans le module de mise à jour, la mise à jour n'est pas importée.
- Si vous n'incluez pas tous les fichiers requis associés à la mise à jour, le référentiel indique que la mise à jour n'a pas été téléchargée, ce qui signifie qu'elle a été partiellement importée. Vous pouvez alors importer les fichiers manquants en les sélectionnant et en les important.
- Les mises à jour de microprogramme principales (telles que celles de type contrôleur de gestion, UEFI et pDSA) sont indépendantes du système d'exploitation. Les modules de mise à jour de microprogramme pour les systèmes d'exploitation RHEL 6 ou SLES 11 sont utilisés pour mettre à jour les nœuds de traitement et les serveurs rack. Pour plus d'informations sur les modules de mise à jour de microprogramme qui doivent être utilisés pour vos serveurs gérés, voir Téléchargement des mises à jour de microprogramme.

Pour plus d'informations sur la mise à jour de microprogramme, voir Gestion du référentiel des mises à jour de microprogramme.

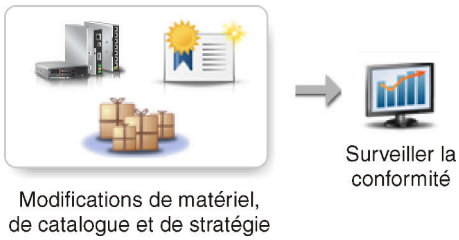
Etape 2. **(Facultatif) Créer et affecter des stratégies de conformité de microprogramme**

Les stratégies de conformité de microprogramme permettent de garantir que le microprogramme présent sur certains appareils gérés est au niveau en cours ou à un niveau spécifique en marquant les appareils qui nécessitent une attention. Chaque stratégie de conformité du microprogramme identifie les appareils surveillés et le niveau de microprogramme qui doit être installé pour assurer la bonne conformité de ces appareils. Vous pouvez définir la conformité au niveau du composant du microprogramme ou de l'appareil. XClarity Administrator va ensuite se servir de ces stratégies pour vérifier l'état des appareils gérés, mais aussi pour identifier ceux qui ne sont plus conformes.

Lorsque vous créez une stratégie de conformité de microprogramme, vous pouvez déclencher le marquage d'un appareil par XClarity Administrator lorsque :
- Le microprogramme de l'appareil est à un niveau inférieur
- Le microprogramme de l'appareil ne correspond pas à la version cible de conformité

XClarity Administrator est fourni avec une stratégie de conformité du microprogramme prédéfinie, appelée **Microprogramme le plus récent dans le référentiel**. Lorsque le nouveau microprogramme est téléchargé ou importé dans le référentiel, cette stratégie est mise à jour pour y inclure les dernières versions disponibles du microprogramme.

Une fois qu'une stratégie de conformité de microprogramme a été assignée à un appareil, XClarity Administrator vérifie l'état de conformité de chaque appareil lorsque des modifications ont été apportées à l'inventaire de l'appareil ou au référentiel des mises à jour de microprogramme. Lorsque le microprogramme d'un appareil est non compatible avec la stratégie affectée, XClarity Administrator indique que l'appareil n'est pas compatible sur la page Mises à jour de microprogramme : appliquer/activer, selon la règle que vous avez spécifiée dans la stratégie de conformité de microprogramme



Par exemple, vous pouvez créer une stratégie de conformité de microprogramme qui définit le niveau de référence du microprogramme qui est installé dans tous les appareils ThinkSystem SR850 et affecter ensuite la stratégie de conformité de microprogramme à tous les appareils ThinkSystem SR850 gérés. Lorsque le référentiel des mises à jour de microprogramme est actualisé et qu'une nouvelle mise à jour de microprogramme est ajoutée, il se peut que ces nœuds de traitement ne soient plus conformes. Lorsque cela se produit, XClarity Administrator met à jour la page Mises à jour de microprogramme : Appliquer/Activer pour indiquer que les appareils ne sont pas conformes et génère une alerte.

Remarque : Vous pouvez choisir d'afficher ou masquer les alertes pour les dispositifs qui ne répondent pas aux exigences de leurs des stratégies de conformité du microprogramme affectée (voir Configuration des paramètres globaux à jour de microprogramme). Les alertes sont masqués par défaut.

Pour plus d'informations sur les stratégies de conformité de microprogramme, voir Création et affectation de stratégies de conformité de microprogramme.

Etape 3. **Application et activation des mises à jour**

XClarity Administrator n'applique pas automatiquement des mises à jour de microprogramme à des appareils gérés. Pour mettre à jour le microprogramme, vous devez appliquer et activer manuellement la mise à jour sur des appareils sélectionnés. Vous pouvez appliquer le microprogramme de l'une des manières suivantes.

- **Appliquer les mises à jour du microprogramme en lot avec des stratégies de conformité**

  Vous pouvez appliquer les mises à jour du microprogramme à *tous* les composants des appareils sélectionnés, en fonction de la stratégie de conformité du microprogramme attribuée, à l'aide d'une image de lot contenant les modules de mise à jour applicables.

  Le processus de mise à jour en lot met tout d'abord à jour le contrôleur de gestion de la carte mère, puis l'UEFI hors bande. Une fois ces mises à jour terminées, en fonction du type de machine, le processus crée une image de lot du microprogramme restant dans la stratégie de conformité. Ensuite, le processus monte l'image sur l'appareil sélectionné, puis le redémarre afin d'amorcer l'image. L'image s'exécute automatiquement en vue d'effectuer les mises à jour restantes.

  Attention : Avant de démarrer le processus de mise à jour, les appareils sélectionnés sont mis hors tension. Assurez-vous que les charges de travail en cours d'exécution sont arrêtées ou, si vous travaillez dans un environnement virtualisé, vérifiez qu'elles ont été déplacées vers un autre serveur. Si des travaux sont en cours exécution, le travail de mise à jour est placé en file d'attente jusqu'à ce que tous les autres travaux soient terminés. Pour afficher la liste des travaux actifs, cliquez sur **Surveillance → Travaux**.

  Remarques :

  – L'application des mises à jour du microprogramme en lot n'est prise en charge que pour les serveurs ThinkSystem SR635 et SR655.

- L’application des mises à jour de microprogramme groupées n’est prise en charge que pour l’adresse IPv4. Les adresses IPv6 ne sont pas prises en charge.
- Vous devez vous assurer que chaque appareil cible a été amorcé sur le SE au moins une fois afin de récupérer toutes les informations de l’inventaire.
- Le microprogramme v2.94 ou ultérieure du contrôleur de gestion de la carte mère est requis pour utiliser la fonction de mise à jour en lot.
- Seules les mises à jour du microprogramme obtenues à partir de modules de référentiel ou les mises à jour du microprogramme individuelles sont utilisées. Les UpdateXpress System Packs (UXSP) ne sont pas pris en charge.
- Seules les mises à jour de microprogramme téléchargées sont appliquées. Actualisez le catalogue produit et téléchargez les mises à jour de microprogramme appropriées (voir Actualisation du catalogue produit et Téléchargement des mises à jour de microprogramme).

  Remarque : À l'origine, lorsque XClarity Administrator est installé, le catalogue produit et le référentiel sont vides.
- Pour les serveurs ThinkSystem SR635 et SR655, la vérification de conformité n’est prise en charge que pour le contrôleur de gestion de la carte mère et UEFI. Cependant, XClarity Administrator essaie d’appliquer des mises à jour du microprogramme à tous les composants matériels disponibles.
- Les mises à jour sont appliquées en fonction de la stratégie de conformité du microprogramme attribuée. Vous ne pouvez pas décider de mettre à jour un sous-ensemble de composants.
- XClarity Administrator v3.2 ou ultérieure est nécessaire pour appliquer des mises à jour du microprogramme pour Lenovo XClarity Provisioning Manager (LXPM), les pilotes Windows LXPM, ou bien les pilotes Linux LXPM aux serveurs ThinkSystem SR635 et SR655.
- Si la version installée est supérieure à la stratégie de conformité attribuée, alors les mises à jour du contrôleur de gestion de la carte mère et UEFI sont ignorées.
- Des stratégies de conformité de microprogramme doivent être créées et affectées aux appareils sur lesquels vous souhaitez appliquer des mises à jour de microprogramme. Pour plus d'informations, voir Création et affectation de stratégies de conformité de microprogramme.
- Avant de démarrer le processus de mise à jour, les appareils sélectionnés doivent être mis hors tension. Assurez-vous que les charges de travail en cours d’exécution sont arrêtées ou, si vous travaillez dans un environnement virtualisé, vérifiez qu’elles ont été déplacées vers un autre serveur.

- **Appliquer certaines mises à jour de microprogramme avec ou sans stratégies de conformité**

  Vous pouvez appliquer les mises à jour du microprogramme à certains composants et appareils, en fonction de la stratégie de conformité du microprogramme attribuée, à l’aide de modules de mise à jour du microprogramme applicables. Vous pouvez également décider d’appliquer des mises à jour du microprogramme postérieures au microprogramme actuellement installé sur certains composants et appareils, sans utiliser de stratégie de conformité.

  Vous pouvez décider d’appliquer les mises à jour à tous les composants d’un appareil spécifique. Vous pouvez aussi décider de ne mettre à jour qu’un sous-ensemble de composants des appareils sélectionnés, par exemple le contrôleur de gestion de la carte mère ou UEFI.

  Les appareils doivent être redémarrés pour que les mises à jour de microprogramme soient activées. (Notez que le redémarrage d'un appareil entraîne des interruptions.) Vous pouvez

décider de redémarrer les appareils dans le cadre du processus de mise à jour (*activation immédiate*) ou attendre qu'une fenêtre de maintenance soit disponible pour les redémarrer (*activation différée*). Dans ce cas, vous devez redémarrer manuellement l'appareil pour que la mise à jour prenne effet.

Lorsque vous choisissez de mettre à jour le microprogramme pour un appareil géré, les étapes requises sont les suivantes.

1. XClarity Administrator envoie les mises à jour de microprogramme (par exemple, pour le contrôleur de gestion, l'interface UEFI et DSA) à l'appareil.
2. Les mises à jour de microprogramme sont activées sur l'appareil lorsque celui-ci est redémarré.
3. Pour les serveurs, XClarity Administrator envoie des mises à jour pour les appareils en option, par exemple, des mises à jour de carte réseau et d'unité de disque dur. XClarity Administrator applique ces mises à jour et le serveur est redémarré.
4. Lorsque vous redémarrez l'appareil ou que vous choisissez l'activation immédiate, les mises à jour pour les appareils en option sont activées.

Remarques :

– Lorsque vous appliquez des mises à jour avec des stratégies de conformité, vous devez créer, puis attribuer une stratégie de conformité du microprogramme à chaque appareil cible. Pour plus d'informations, voir Création et affectation de stratégies de conformité de microprogramme.

– Si vous choisissez d'installer un module de mise à jour de microprogramme contenant les mises à jour de plusieurs composants, tous les composants auxquels le module de mise à jour s'applique sont mis à jour.

– Les mises à jour des modules CMM et des commutateurs Flex sont toujours activées immédiatement, même si vous sélectionnez l'activation différée.

Lorsque vous effectuez des mises à jour sur un ensemble d'appareils, XClarity Administrator effectue les mises à jour dans l'ordre suivant.

- Module CMM de châssis
- Commutateurs RackSwitch et Flex System
- Nœuds de traitement Flex et serveurs rack et au format tour
- Dispositifs Lenovo Storage

Attention : Avant de tenter d'appliquer des mises à jour du microprogramme aux appareils gérés, prenez soin d'effectuer les actions suivantes.

- Prenez connaissance des remarques relatives à la mise à jour de microprogramme avant de tenter de mettre à jour un microprogramme sur vos appareils gérés (voir Considérations relatives à la mise à jour du microprogramme).
- Initialement, les appareils qui ne sont pas pris en charge pour les mises à jour sont masqués dans la vue. Les appareils qui ne sont pas pris en charge ne peuvent pas être sélectionnés pour les mises à jour.
- Par défaut, tous les composants détectés sont répertoriés comme disponibles pour l'application des mises à jour ; toutefois, un microprogramme de niveau antérieur peut empêcher un composant d'apparaître dans l'inventaire ou d'afficher des informations de version complète. Pour répertorier tous les modules basés sur des stratégies vous permettant d'appliquer des mises à jour, cliquez sur **Toutes les actions → Paramètres globaux**, et sélectionnez **Support étendu pour les appareils de niveau précédent**. Lorsque cette option est sélectionnée, la mention « Autre logiciel disponible » apparaît dans la colonne Version installée pour les appareils non détectés. Pour plus d'informations, voir Configuration des paramètres globaux à jour de microprogramme.

Remarques :

- Les paramètres globaux ne peuvent pas être modifiés lorsque des mises à jour sont en cours sur des appareils gérés.
- La génération d'options supplémentaires peut nécessiter quelques minutes. Au bout de quelques instants, il vous faudra peut-être cliquer sur l'icône **Actualiser** () afin d'actualiser le tableau.

- Assurez-vous qu'aucun travail n'est en cours d'exécution sur le serveur cible. Si des travaux sont en cours exécution, le travail de mise à jour est placé en file d'attente jusqu'à ce que tous les autres travaux soient terminés. Pour afficher la liste des travaux actifs, cliquez sur **Surveillance → Travaux**.
- Assurez-vous que le référentiel des mises à jour de microprogramme contient les modules de microprogramme que vous souhaitez déployer. Si tel n'est pas le cas, actualisez le catalogue produit et téléchargez les mises à jour de microprogramme appropriées (voir Actualisation du catalogue produit et Téléchargement des mises à jour de microprogramme).

  Remarque : À l'origine, lorsque XClarity Administrator est installé, le catalogue produit et le référentiel sont vides.

  Si vous prévoyez d'installer un microprogramme prérequis, vérifiez que ce dernier a bien été téléchargé dans le référentiel.

  Dans certains cas, plusieurs versions peuvent être nécessaires afin de mettre à jour le microprogramme, et toutes devront être téléchargées vers le référentiel. Par exemple, pour effectuer la mise à niveau du commutateur évolutif IBM FC5022 SAN de la version v7.4.0a vers v8.2.0a, vous devez installer v8.0.1-pha, puis v8.1.1, et enfin v8.2.0a. Ces trois versions peuvent se trouver dans le référentiel afin de mettre à jour le commutateur vers v8.2.0a.
- En général, les appareils doivent être redémarrés pour que la mise à jour de microprogramme soit activée. Si vous décidez de redémarrer l'appareil lors du processus de mise à jour (*activation immédiate*), vérifiez que les charges de travail en cours d'exécution ont été arrêtées ou, si vous travaillez dans un environnement virtualisé, assurez-vous qu'elles ont été déplacées vers un autre serveur.

Pour plus d'informations sur l'installation des mises à jour, voir Application et activation des mises à jour de microprogramme.

Considérations relatives à la mise à jour du microprogramme

Avant de commencer à mettre à jour le microprogramme sur des appareils gérés à l'aide de Lenovo XClarity Administrator, prenez connaissance des remarques importantes présentées ci-après.

- Remarques générales
- Considérations CMM
- Remarques sur le contrôleur de gestion de la carte mère
- Remarques sur les appareils ThinkSystem
- Remarques sur les appareils Flex System
- Remarques sur le stockage

Remarques générales

- **Niveaux de microprogramme minimum requis**

  Vérifiez que le microprogramme installé sur chaque appareil géré correspond au niveau minimal requis avant d'utiliser XClarity Administrator pour mettre à jour le microprogramme sur ces appareils. Vous

pouvez rechercher les niveaux de microprogramme minimum requis par la Support de XClarity Administrator – Page Web de compatibilité en cliquant sur l'onglet **Compatibilité**, puis en cliquant sur le lien des types d'appareil appropriés.

Remarque : Pour plus d'informations sur le support des appareils d'E-S et les limitations connues, voir la Support de XClarity Administrator – Page Web de compatibilité.

- **Mettez à jour tous les composants vers le niveau qui est inclus dans le référentiel des mises à jour de microprogramme.**

  Etant donné que les mises à jour de microprogramme pour les composants Flex System sont testées et publiées ensemble, il est recommandé de conserver le même niveau de microprogramme sur tous les composants dans un châssis Flex System. Par conséquent, il est important d'utiliser une même fenêtre de maintenance pour mettre à jour le microprogramme sur tous les composants du châssis. Les mises à jour sélectionnées sont automatiquement appliquées selon la séquence appropriée par XClarity Administrator.

- **Les pilotes LXPM Linux et les pilotes LXPM Windows ne sont pas inclus lors du téléchargement des UXSP**

  Les pilotes Linux et Windows de Lenovo XClarity Provisioning Manager (LXPM) ne sont pas inclus dans UpdateXpress System Packs (UXSPs). Pour appliquer ces modules de mise à jour à vos appareils, téléchargez les derniers modules de référentiel des mises à jour du microprogramme ou téléchargez manuellement les modules individuels et créez une stratégie de conformité du microprogramme pour inclure ces modules.

- **Certaines mises à jour de microprogramme sont codépendantes d'un niveau de pilote de périphérique minimum.**

  Avant d'appliquer les mises à jour d'adaptateur et de microprogramme d'E-S sur un serveur, vous devrez peut-être mettre à jour le pilote de périphérique vers un niveau minimum. En général, les mises à jour de microprogramme ne dépendent pas de niveaux de pilote de périphérique spécifiques. Consultez la section relative à ce type de codépendances dans le fichier Readme traitant de la mise à jour de microprogramme, puis mettez à jour les pilotes de périphérique dans votre système d'exploitation avant de mettre à jour le microprogramme. XClarity Administrator ne met pas à jour les pilotes de périphérique dans votre système d'exploitation.

- **Réamorcez XClarity Administrator avant de mettre à jour le microprogramme**

  Si les tentatives de mise à jour précédentes échouent, réamorcez XClarity Administrator avant de mettre à jour le microprogramme. Le réamorçage du serveur de gestion garantit que le compte réservé au système utilisé pour mettre à jour le microprogramme est bien synchronisé sur les appareils gérés.

- **Les mises à jour de microprogramme entraînent des perturbations et nécessitent de mettre au repos les charges de travail sur les appareils.**

  L'exécution de mises à jour de microprogramme sur des appareils gérés entraîne des perturbations si vous choisissez d'activer immédiatement la mise à jour. Vous devez mettre les appareils au repos avant de procéder à la mise à jour du microprogramme à l'aide de l'option Activation immédiate.

  Lorsque vous mettez à jour un microprogramme sur des serveurs, ces derniers sont arrêtés et placés dans un système d'exploitation de maintenance afin de mettre à jour les pilotes de périphérique pour les adaptateurs, les unités de disque et les unités SSD.

  Les Commutateurs Flex dans un châssis donné sont mis à jour de manière séquentielle, puis redémarrés pendant le processus de mise à jour du microprogramme. L'implémentation de chemins de données redondants permet de réduire les perturbations, mais une brève interruption de la connectivité réseau peut tout de même se produire lors de la mise à jour du microprogramme.

- **N'utilisez pas XClarity Administrator pour mettre à jour le microprogramme du serveur sur lequel XClarity Administrator s'exécute.**

Si XClarity Administrator s'exécute sur un hôte de l'hyperviseur fonctionnant sur un serveur qu'il gère, vous ne devez pas mettre à jour le microprogramme sur ce serveur à l'aide de XClarity Administrator. Lorsque des mises à jour de microprogramme sont appliquées à l'aide de l'option Activation immédiate, XClarity Administrator force le redémarrage du serveur cible, ce qui entraîne le redémarrage de l'hôte de l'hyperviseur et de XClarity Administrator. Lorsque l'option Activation différée est utilisée pour l'application du microprogramme, seule une partie de celui-ci est appliquée tant que le système cible n'est pas redémarré

Considérations CMM

- **Réinstallez virtuellement les modules CMM avant de mettre à jour le microprogramme.**

  Si vous mettez à jour des modules CMM qui exécutent la pile version 1.3.2.1 2PET12K à 2PET12Q comme niveau de microprogramme, qui sont en cours d'exécution depuis plus de trois semaines et qui figurent dans une configuration à deux modules CMM, vous devez réinstaller virtuellement le module CMM principal et le module CMM de secours avant de mettre à jour le microprogramme (voir Réinstallation virtuelle d'un module CMM).

Remarques sur le contrôleur de gestion de la carte mère

- **Niveaux BMC requis pour l'état d'activation en attente**

  Pour afficher l'état d'activation en attente, la version de microprogramme suivante doit être installée sur le contrôleur de gestion de la carte mère principal dans le serveur.
  - **IMM2** : TCOO46F, TCOO46E ou version ultérieure (selon la plateforme)
  - **XCC** : CDI328M, PSI316N, TEI334I ou version ultérieure (selon la plateforme)
- **Mises à jour appliquées au contrôleur de gestion principal et aux partitions de microprogramme UEFI.**

  Les mises à jour du contrôleur de gestion de la carte mère et de l'interface UEFI peuvent être appliquées de façon indépendante aux partitions de microprogramme de sauvegarde et principales pour le contrôleur de gestion et l'interface UEFI.

  Vous pouvez également appliquer les mises à jour du contrôleur de gestion et de l'interface UEFI uniquement aux partitions de microprogramme principales sur le serveur. Par défaut, le contrôleur de gestion est configuré pour synchroniser la partition de contrôleur de gestion de sauvegarde avec la partition de contrôleur de gestion principale après que le contrôleur de gestion principal s'est exécuté de façon satisfaisante et que le nouveau niveau est prêt à être promu à la partition de sauvegarde. Cependant, le contrôleur de gestion n'est pas configuré pour synchroniser la partition de sauvegarde UEFI par défaut. Par conséquent, envisagez d'exécuter l'une des actions suivantes sur le contrôleur de gestion :

  - Activer la synchronisation automatique de la partition de sauvegarde UEFI.

    En agissant ainsi, vous vous assurez que la partition de sauvegarde et la partition principale s'exécutent toutes les deux au même niveau de microprogramme (et que le microprogramme UEFI de sauvegarde est compatible avec le microprogramme du contrôleur de gestion).
  - Désactiver la synchronisation automatique de la partition de sauvegarde du contrôleur de gestion.

    Bien que cette action ne soit pas recommandée, elle vous permet néanmoins d'avoir un contrôle total sur les niveaux de microprogramme du contrôleur de gestion et de l'interface UEFI. Toutefois, vous devez mettre à jour manuellement le microprogramme du contrôleur de gestion et de l'interface UEFI pour les deux partitions.

  Vous utilisez les stratégies de conformité de microprogramme pour identifier les mises à jour appliquées à chaque appareil. Pour plus d'informations sur les stratégies de conformité de microprogramme, voir Création et affectation de stratégies de conformité de microprogramme.

Remarque : Si le contrôleur de gestion et l'interface UEFI sont configurés pour synchroniser automatiquement le microprogramme de sauvegarde à partir du microprogramme principal, XClarity Administrator n'a pas besoin de mettre à jour les bancs de sauvegarde. Dans ce cas, vous pouvez effacer les mises à jour de banc de sauvegarde lors de l'application des mises à jour à un serveur ou retirer les bancs de sauvegarde de la stratégie de conformité de microprogramme.

- **Risque de défaillance du système VMware vSphere ESXi (écran de diagnostic mauve sur l'hôte) lorsqu'un contrôleur de gestion est réinitialisé.**

  Si vous exécutez VMware vSphere ESXi sur un serveur, assurez-vous que les niveaux VMware ESXi minimum suivants sont installés avant de mettre à jour le microprogramme sur le serveur :

  – Si vous exécutez VMware vSphere ESXi 5.0, installez le niveau minimum 5.0u2 (mise à jour 2)
  – Si vous exécutez VMware vSphere ESXi 5.1, installez le niveau minimum 5.1u1 (mise à jour 1)

  Si vous n'installez pas ces niveaux minimum, une défaillance du système VMware vSphere ESXi (écran de diagnostic mauve sur l'hôte) peut se produire à chaque fois que le contrôleur de gestion est réinitialisé, notamment lorsque le microprogramme du contrôleur de gestion est appliqué et activé.

  Remarque : Ce problème ne concerne pas ESXi v5.5.

Remarques sur les appareils ThinkSystem

- **Pour les serveurs ThinkSystem SE350 exécutant une version de microprogramme XCC antérieure à 20A, IPMI sur accès KCS doit être activé manuellement dans le contrôleur de gestion de la carte mère pour garantir que le contrôleur de gestion peut communiquer avec XClarity Administrator.**

  Pour les serveurs ThinkSystem SE350, IPMI sur KCS est désactivé par défaut. Pour les serveurs ThinkSystem SE350 exécutant une version de microprogramme XCC 20A ou ultérieure, XClarity Administrator active automatiquement IPMI sur KCS lors d'une mise à jour du microprogramme, puis le désactive une fois celle-ci terminée. Toutefois, pour les serveurs ThinkSystem SE350 qui exécutent une version de microprogramme XCC antérieure à 20A, vous devez activer cette option manuellement depuis l'interface utilisateur de Lenovo XClarity Controller en cliquant sur **Configuration BMC → Sécurité → IPMI sur accès KCS**.

- Pour les serveurs ThinkSystem SR635 et SR655, les limitations suivantes s'appliquent.

  – Seule l'activation immédiate est prise en charge. L'activation différée et l'activation par priorité ne sont pas prises en charge.
  – Concernant la version v3.1.1 ou ultérieure de XClarity Administrator, vous pouvez utiliser la fonction de mise à jour en lot afin de mettre à jour tous les composants des serveurs ThinkSystem SR635 et SR655, dont le contrôleur de gestion de la carte mère, UEFI, les unités de disque et les options d'E-S.

    Attention : Avant de démarrer le processus de mise à jour, les appareils sélectionnés sont mis hors tension. Assurez-vous que les charges de travail en cours d'exécution sont arrêtées ou, si vous travaillez dans un environnement virtualisé, vérifiez qu'elles ont été déplacées vers un autre serveur. Si des travaux sont en cours exécution, le travail de mise à jour est placé en file d'attente jusqu'à ce que tous les autres travaux soient terminés. Pour afficher la liste des travaux actifs, cliquez sur **Surveillance → Travaux**.

    Remarques :

    – L'application des mises à jour du microprogramme en lot n'est prise en charge que pour les serveurs ThinkSystem SR635 et SR655.
    – L'application des mises à jour de microprogramme groupées n'est prise en charge que pour l'adresse IPv4. Les adresses IPv6 ne sont pas prises en charge.
    – Vous devez vous assurer que chaque appareil cible a été amorcé sur le SE au moins une fois afin de récupérer toutes les informations de l'inventaire.

- Le microprogramme v2.94 ou ultérieure du contrôleur de gestion de la carte mère est requis pour utiliser la fonction de mise à jour en lot.
- Seules les mises à jour du microprogramme obtenues à partir de modules de référentiel ou les mises à jour du microprogramme individuelles sont utilisées. Les UpdateXpress System Packs (UXSP) ne sont pas pris en charge.
- Seules les mises à jour de microprogramme téléchargées sont appliquées. Actualisez le catalogue produit et téléchargez les mises à jour de microprogramme appropriées (voir Actualisation du catalogue produit et Téléchargement des mises à jour de microprogramme).

  Remarque : À l'origine, lorsque XClarity Administrator est installé, le catalogue produit et le référentiel sont vides.
- Pour les serveurs ThinkSystem SR635 et SR655, la vérification de conformité n'est prise en charge que pour le contrôleur de gestion de la carte mère et UEFI. Cependant, XClarity Administrator essaie d'appliquer des mises à jour du microprogramme à tous les composants matériels disponibles.
- Les mises à jour sont appliquées en fonction de la stratégie de conformité du microprogramme attribuée. Vous ne pouvez pas décider de mettre à jour un sous-ensemble de composants.
- XClarity Administrator v3.2 ou ultérieure est nécessaire pour appliquer des mises à jour du microprogramme pour Lenovo XClarity Provisioning Manager (LXPM), les pilotes Windows LXPM, ou bien les pilotes Linux LXPM aux serveurs ThinkSystem SR635 et SR655.
- Si la version installée est supérieure à la stratégie de conformité attribuée, alors les mises à jour du contrôleur de gestion de la carte mère et UEFI sont ignorées.
- Des stratégies de conformité de microprogramme doivent être créées et affectées aux appareils sur lesquels vous souhaitez appliquer des mises à jour de microprogramme. Pour plus d'informations, voir Création et affectation de stratégies de conformité de microprogramme.
- Avant de démarrer le processus de mise à jour, les appareils sélectionnés doivent être mis hors tension. Assurez-vous que les charges de travail en cours d'exécution sont arrêtées ou, si vous travaillez dans un environnement virtualisé, vérifiez qu'elles ont été déplacées vers un autre serveur.

  Vous pouvez également décider d'utiliser la fonction de mise à jour classique pour appliquer les mises à jour du microprogramme uniquement au contrôleur de gestion de la carte mère et UEFI.

- Pour XClarity Administrator v3.0 :
  - La gestion des données n'est pas correctement mise à jour lors de la mise à jour du microprogramme de 20A à 20B ou 20C. Pour résoudre ce problème, annulez la gestion de l'appareil, puis gérez-le à nouveau, ou redémarrez XClarity Administrator.
  - La rétromigration des mises à jour du microprogramme n'est pas prise en charge.

- **Les mises à jour de microprogramme ne sont pas prises en charge sur les serveurs ThinkSystem utilisant DHCPv6 ou des adresses IPv6 affectées statiquement**

  Lorsque vous utilisez l'adressage IPv6 sur les serveurs ThinkSystem, les mises à jour de microprogramme sont prises en charge uniquement sur les adresses IPv6 locales de liaison (LLA) et les adresses sans état.
- **Lors de la mise à jour du microprogramme vers la version 20D, vous devez mettre à jour à la fois UEFI et XCC.**

  UEFI et Lenovo XClarity Controller (XCC) doivent être mis à jour ensemble pour la version 20D. Si vous mettez seulement à jour XCC ou UEFI, cela peut provoquer des problèmes.

Remarques sur les appareils Flex System

- **Assurez-vous que les commutateurs Flex qui sont mis à jour sont sous tension,**
- **Sélectionnez l'option Activation immédiate lors de la mise à jour de nœuds de traitement qui sont à des niveaux de microprogramme de contrôleur de gestion antérieurs à Flex System 1.3.2.**

Lorsque vous appliquez l'édition de cycle de vie 2e trimestre Flex System 1.3.2 à un nœud de traitement, vous devez choisir l'option *Activation immédiate* pour mettre à jour celui-ci. L'activation immédiate force le nœud de traitement à redémarrer pendant le processus de mise à jour.

- Les **Commutateurs Flex doivent être configurés avec une adresse IP accessible à partir de XClarity Administrator.**

  Le Commutateur Flex cible doit se voir affecter une adresse IP pouvant communiquer avec XClarity Administrator de sorte que XClarity Administrator puisse télécharger et appliquer la mise à jour du microprogramme.

- **Support de mise à jour sur des environnements complexes évolutifs, tels que des nœuds x480 X6 et x880 X6.**

  Le support de mise à jour sur des nœuds évolutifs, tels que des nœuds Flex System x480 X6 et x880 X6 est limité aux configurations où le complexe est configuré en tant que *partition unique* qui inclut tous les nœuds de traitement faisant partie du complexe multinœud. Vous ne pouvez pas utiliser XClarity Administrator pour mettre à jour un complexe composé de plusieurs partitions.

  Si vous affectez une stratégie de conformité de microprogramme à une partition qui comprend plusieurs serveurs dans un environnement complexe évolutif (par exemple, des nœuds de traitement Flex System x480 X6 et x880 X6), par défaut, XClarity Administrator met à jour le microprogramme sur tous les contrôleurs de gestion et toutes les interfaces UEFI pour chaque serveur de la partition. Toutefois, si vous sélectionnez un sous-ensemble de composants de la partition, XClarity Administrator met à jour le microprogramme uniquement sur ces composants.

- **La mise à jour du module CMM2 vers v1.30 (1AON06C) ou une version ultérieure requiert que les commutateurs Flex exécutent la version de niveau 3 du protocole Enhanced Configuration and Management (EHCM L3)**

  Le module CMM2 et les commutateurs Flex communiquent via le protocole EHCM. Ce protocole est requis pour XClarity Administrator afin de mettre à jour les commutateurs Flex. Lorsque vous mettez à jour un module CMM2 vers v1.30 (1AON06C) ou une version ultérieure, XClarity Administrator vérifie que les commutateurs Flex exécutent EHCM L3 et, si tel n'est pas le cas, annule la mise à jour du module CMM avec un message d'avertissement indiquant que les commutateurs Flex doivent d'abord être mis à jour vers une version qui prend en charge EHCM L3. Vous pouvez outrepasser cette vérification en sélectionnant **Essayer de mettre à jour les composants déjà en conformité** lorsque vous mettez à jour le microprogramme du module CMM.

  Attention : Il n'existe actuellement aucune version de microprogramme pour les commutateurs Flex System EN6131 Ethernet et les commutateurs IB6131 InfiniBand qui prennent en charge EHCM L3. Cela signifie qu'après la mise à jour du modèle CMM2 vers le microprogramme v1.30 (1AON06C) ou une version ultérieure, vous ne pouvez plus utiliser XClarity Administrator pour mettre à jour ces commutateurs. La solution de contournement consiste à utiliser l'interface Web du contrôleur de gestion ou l'interface de ligne de commande pour le châssis afin de mettre à jour le commutateur.

Commutateur Flex System	Version	Date de publication
CN4093	7.8.4.0	Juin 2014
EN4023	6.0.0	Avril 2015
EN4093	7.8.4.0	Juin 2014
EN4093R	7.8.4.0	Juin 2014
EN6132	Non disponible	Non disponible
FC3171	9.1.3.02.00	Juin 2014
FC5022	7.4.0b1	Mars 2016
IB6132	Non disponible	Non disponible

Commutateur Flex System	Version	Date de publication
SI4091	7.8.4.0	Juin 2014
SI4093	7.8.4.0	Juin 2014

Remarque : Le commutateur évolutif Ethernet 1 Gb EN2092 ne requiert pas EHCM L3 et n'est pas soumis à cette restriction.

Remarques sur le stockage

- **Remarques sur les dispositifs de stockage DM ThinkSystem**

  Pour mettre à jour le microprogramme sur les dispositifs de stockage ThinkSystem DM, les appareils doivent être en cours d'exécution v9.7 ou version ultérieure.

  La rétromigration est prise en charge pour les versions mineures uniquement. Par exemple, vous pouvez rétrograder de 9.7P11 à 9.7P9 ; toutefois, vous ne pouvez pas rétrograder de 9.8 vers 9.7.

  Télécharger le microprogramme pour dispositifs de stockage series ThinkSystem DM :

  - Un ou plusieurs dispositifs de stockage ThinkSystem DM Series doivent être gérés par XClarity Administrator.
  - Chaque dispositif de stockage series DM ThinkSystem doit être autorisé pour le service et la prise en charge du matériel.
  - Vous devez spécifier le pays dans lequel se trouvent les dispositifs de stockage ThinkSystem DM Series sur les mises à jour de microprogramme : page référentiel. Seul le microprogramme chiffré peut être téléchargé pour des appareils dans les pays suivants : L'Arménie, la Biélorussie, la Chine, Cuba, l'Iran, le Kazakhstan, le Kirghizistan, la Corée du nord, la Russie, le Soudan, la Syrie.
- **Les unités de disque doivent être à l'état JBOD, En ligne, Prêt ou Non configuré (correct).**

  Pour mettre à jour le microprogramme sur les unités de disque, l'état RAID doit être JBOD, En ligne, Prêt ou Non configuré (correct). Les autres états ne sont pas pris en charge. Pour déterminer l'état RAID d'une unité de disque, accédez à la page d'inventaire de l'appareil, développez la section **Unités**, puis vérifiez la colonne **État de RAID** de cette unité de disque (voir Affichage des détails d'un serveur géré).
- **La version de microprogramme ne détecte pas d'unité de disque ni d'unité SSD.**

  XClarity Administrator détecte uniquement la version de microprogramme installée et effectue une vérification de conformité pour les unités de disque et les unités SSD associées à une carte MegaRAID ou NVME. Il se peut que d'autres unités liées disposent d'un niveau de microprogramme non pris en charge ou qu'elles ne prennent pas en charge le signalement de version de microprogramme. Toutefois, les mises à jour de microprogramme sont appliquées à ces unités si elles sont sélectionnées.
- **Le microprogramme NVMe est appliqué même s'il n'est pas identifié avec un composant cible.**

  Sur la page Appliquer/Activer, la version de microprogramme NVMe est indiquée pour les unités SSD. Aucune mise à jour de microprogramme cible n'est identifiée pour les appareils NVMe reconnus, par conséquent, un message d'avertissement s'affiche lorsque vous tentez de mettre à jour le système cible. Toutefois, la mise à jour d'unité de disque dur/unité SSD est appliquée même si elle n'est pas identifiée avec un composant cible, par conséquent, le microprogramme NVMe est toujours mis à jour.
- **L'application du module de mise à jour de ServeRAID M5115 PSoC3 à partir de XClarity Administrator requiert que le niveau minimum 68 soit installé.**

  La mise à jour de ServeRAID M5115 PSoC3 (Programmable System-on-Chip) à partir d'une version antérieure au niveau 68 doit être effectuée de manière contrôlée.

  Astuce : Vous pouvez visualiser la version de code pour ServeRAID M5115 PSoC3 en vous connectant à l'interface Web CMM et en sélectionnant l'onglet **Microprogramme** pour le nœud de traitement cible.

Sélectionnez ensuite la carte d'extension pour l'adaptateur ServeRAID M5115. La version de code PSoc3 est le type de microprogramme GÉNÉRIQUE.

Pour les versions installées antérieures au niveau 68, vous ne pouvez pas effectuer de mise à jour à l'aide de XClarity Administrator. À la place, vous devez procéder comme suit à partir de l'interface Web ou de l'interface de ligne de commande du module Chassis Management Module (CMM) :

- **Utilisation de l'interface Web CMM :**
  1. Connectez-vous à l'interface Web Chassis Management Module (CMM).
  2. Dans la barre de menus, cliquez sur **Service et support → Avancé**.
  3. Cliquez sur l'onglet **Réinitialisation de maintenance**.
  4. Sélectionnez le nœud de traitement approprié en cliquant sur le bouton d'option correspondant.
  5. À partir du bouton de défilement vers le bas **Réinitialiser**, cliquez sur **Réinstallation virtuelle**.
  6. Cliquez sur **OK** pour confirmer.
- **Utilisation de l'interface de ligne de commande CMM :**
  - Connectez-vous à l'interface SSH (Secure Shell) CMM.
  - Entrez la commande suivante pour effectuer une réinstallation virtuelle :
    `'service -vr -T blade[x]`

    où *x* est le numéro de baie du nœud de traitement à réinstaller.

Une fois le système remis sous tension, effectuez un amorçage sur le système d'exploitation, puis procédez à la mise à jour de ServeRAID M5115 PSoC3 à l'aide du module de mise à jour imbriqué extrait. Procédez comme suit pour extraire le module imbriqué.

- **Utilisation de Microsoft Windows :**

  Ouvrez le module de mise à jour (lnvgy_fw_psoc3_m5115-70_windows_32-64.exe) et sélectionnez Extraire sur le disque dur. Sélectionnez ensuite le chemin où le module imbriqué doit être extrait.
- **Utilisation de Linux :**

  Exécutez la commande suivante :

  `lnvgy_fw_psoc3_m5115-70_linux_32-64.bin -x`

  où *x* représente l'emplacement où le module imbriqué doit être extrait.

Gestion du référentiel des mises à jour de microprogramme

Le *référentiel des mises à jour de microprogramme* contient un catalogue de mises à jour disponibles, ainsi que les modules de mise à jour qui peuvent être appliqués aux appareils gérés.

À propos de cette tâche

Le *catalogue* contient des informations sur les mises à jour de microprogramme actuellement disponibles pour tous les appareils pris en charge par XClarity Administrator. Le catalogue organise les mises à jour du microprogramme par type de dispositif. Lorsque vous actualisez le catalogue, XClarity Administrator extrait des informations sur les dernières mises à jour de microprogramme disponibles à partir du site Web de Lenovo (y compris les fichiers de métadonnées .xml ou .json et Readme .txt) et stocke ces informations dans le référentiel des mises à jour de microprogramme. Le fichier de contenu (.exe) n'est pas téléchargé. Pour plus d'informations sur l'actualisation du catalogue, voir Actualisation du catalogue produit.

Si de nouvelles mises à jour de microprogramme sont disponibles, vous devez d'abord télécharger les modules de mise à jour avant de pouvoir mettre à jour ce microprogramme sur les appareils gérés. L'actualisation du catalogue n'entraîne pas le téléchargement automatique des modules de mise à jour. Le

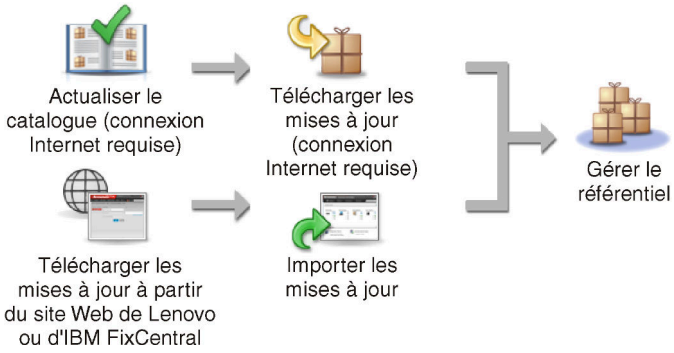
tableau **Catalogue produit** sur la page Référentiel des mises à jour de microprogramme identifie les modules de mise à jour qui ont été téléchargés et ceux qui sont disponibles pour téléchargement.

Vous pouvez télécharger les mises à jour du microprogramme de plusieurs manières différentes :

- **Modules de référentiel des mises à jour de microprogramme**. Les modules de référentiel contiennent les mises à jour de microprogramme les plus récentes pour tous les appareils pris en charge ainsi qu'une stratégie de conformité de microprogramme actualisée par défaut. Ces modules de référentiel sont importés, puis appliqués à partir de la page Mettre à jour le serveur de gestion.
- **UpdateXpress System Packs (UXSPs)**. Les modules UXSP contiennent les mises à jour de microprogramme et de pilote de périphérique disponibles les plus récentes, organisées par système d'exploitation. Lorsque vous téléchargez des modules UXSP depuis la page Mises à jour de microprogramme : référentiel, seules les mises à jour de microprogramme sont téléchargées et stockées dans le référentiel. Les mises à jour de pilote de périphérique sont exclues.

  Remarque : Pour les serveurs équipés de XCC2, ces packages sont appelés modules (*bundles*) de microprogramme.
- **Mises à jour individuelles du microprogramme**. Vous pouvez télécharger les modules de mise à jour du microprogramme individuel, en même temps, selon la version qui est répertoriée dans le catalogue.

XClarity Administrator doit être connecté à Internet pour actualiser le catalogue et télécharger les mises à jour de microprogramme. S'il n'est pas connecté à Internet, vous pouvez télécharger manuellement les fichiers sur un poste de travail disposant d'un accès réseau à l'hôte XClarity Administrator à l'aide d'un navigateur Web, puis importer les fichiers dans le référentiel des mises à jour de microprogramme.



Lorsque vous importez manuellement des mises à jour du microprogramme dans XClarity Administrator, vous devez inclure les fichiers requis suivants : contenu (image et MIB), métadonnées, historique des modifications et Readme. Par exemple :

- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.tgz
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.xml
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.chg
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.txt

Attention :

- Importez uniquement ces fichiers requis. N'importez pas d'autres fichiers susceptibles de se trouver sur les sites Web de téléchargement du microprogramme.
- Si vous n'incluez pas le fichier XML dans le module de mise à jour, la mise à jour n'est pas importée.
- Si vous n'incluez pas tous les fichiers requis associés à la mise à jour, le référentiel indique que la mise à jour n'a pas été téléchargée, ce qui signifie qu'elle a été partiellement importée. Vous pouvez alors importer les fichiers manquants en les sélectionnant et en les important.

- Les mises à jour de microprogramme principales (telles que celles de type contrôleur de gestion, UEFI et pDSA) sont indépendantes du système d'exploitation. Les modules de mise à jour de microprogramme pour les systèmes d'exploitation RHEL 6 ou SLES 11 sont utilisés pour mettre à jour les nœuds de traitement et les serveurs rack. Pour plus d'informations sur les modules de mise à jour de microprogramme qui doivent être utilisés pour vos serveurs gérés, voir Téléchargement des mises à jour de microprogramme.

Une fois les mises à jour de microprogramme téléchargées dans le référentiel, des informations sont fournies sur chacune des mises à jour contenues, y compris la date d'édition, la taille, l'utilisation de stratégie et le niveau de gravité. Le niveau de gravité indique l'impact et la nécessité d'appliquer la mise à jour pour vous aider à déterminer de quelle manière votre environnement peut être affecté.

- **Édition initiale**. Il s'agit de la première édition du microprogramme.
- **Critique**. L'édition de microprogramme contient des correctifs urgents destinés à résoudre des problèmes d'altération de données, de sécurité et de stabilité.
- **Suggérée**. L'édition de microprogramme contient des correctifs significatifs destinés à résoudre des problèmes potentiels.
- **Non critique**. L'édition de microprogramme contient des correctifs mineurs, des améliorations de performances et des modifications textuelles.

Remarques :

- Le niveau de gravité est relatif à la version précédente de la mise à jour. Par exemple, si la version 1.0.1 du microprogramme est installée, que la version 1.02 de mise à jour est de type Critique et que la version 1.03 de mise à jour est de type Recommandé, cela signifie que la mise à jour de la version 1.02 vers la version 1.03 est recommandée, mais que la mise à jour de la version 1.01 vers la version 1.03 est critique car elle est cumulative (la version 1.03 inclut les problèmes critiques résolus par la version 1.02).
- Des cas particuliers peuvent exister lorsqu'une mise à jour est uniquement critique ou recommandée pour un système d'exploitation ou un type de machine spécifique. Pour plus d'informations, voir le document Notes sur l'édition.

Procédure

Pour afficher les mises à jour de microprogramme disponibles dans le catalogue produit, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Référentiel**. La page Référentiel des mises à jour de microprogramme qui s'affiche présente une liste de modules de mise à jour de microprogramme disponibles, organisée par type d'appareil.

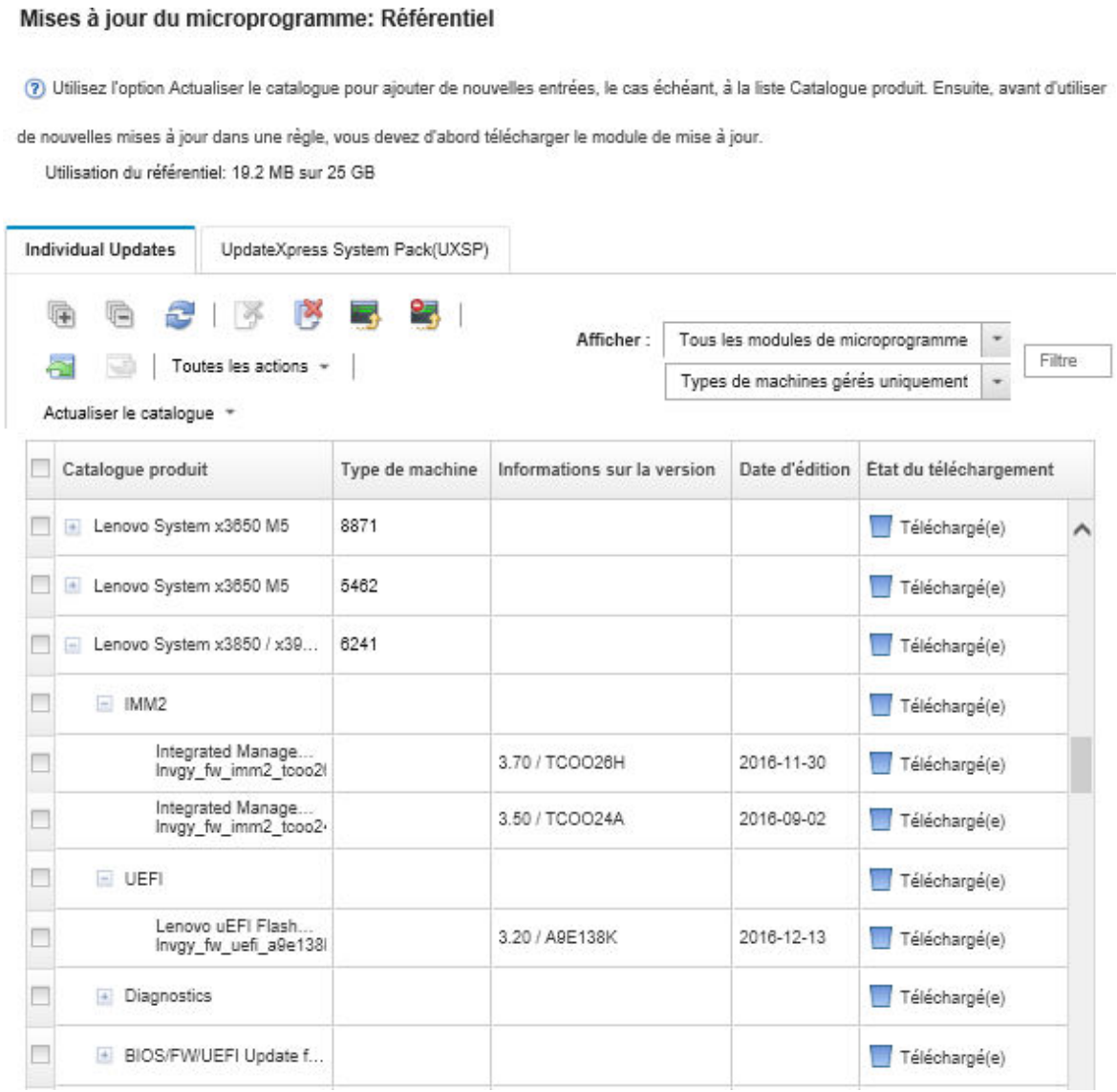
Etape 2. Cliquez sur le **Mises à jour individuelles** onglet pour afficher des informations sur les modules de mise à jour de microprogramme disponibles, ou cliquez sur le **UpdateXpress System Packs (UXSPs)** onglet pour afficher des informations sur les packs Uxsp disponible

Etape 3. Développez un appareil et les composants de ce dernier afin d'afficher la liste des modules de mise à jour et des mises à jour de microprogramme pour cet appareil.

Vous pouvez trier les colonnes du tableau et cliquer sur l'icône **Développer tout** ( ) et sur l'icône **Réduire tout** ( ) pour faciliter la recherche de mises à jour de microprogramme spécifiques. En outre, vous pouvez filtrer la liste des appareils affichés et des mises à jour de microprogramme en sélectionnant une option dans le menu **Afficher** pour afficher uniquement les mises à jour de microprogramme d'un âge donné, les mises à jour de microprogramme de tous les types de serveurs ou uniquement des types de serveurs gérés, ou en entrant du texte dans la zone **Filtre**. Notez que si vous recherchez des appareils spécifiques, seuls les appareils sont listés ; les mises à jour de microprogramme n'apparaissent pas sous le nom de l'appareil.

Remarque : Pour les serveurs, des modules de mise à jour spécifiques sont disponibles selon le type de serveur. Par exemple, si vous développez un serveur, tel que Nœud de traitement x240

Flex System, les modules de mise à jour disponibles spécifiquement pour ce nœud de traitement s'affichent.



Résultats

Depuis cette page, vous pouvez effectuer les actions suivantes :

- Actualisez cette page avec les informations sur les mises à jour de microprogramme en cours dans le catalogue en cliquant sur l'icône **Actualiser** ( ).
- Procédez à l'extraction des dernières informations relatives aux mises à jour disponibles en cliquant sur l'icône **Actualiser le catalogue**.L'extraction de ces informations peut durer plusieurs minutes. Pour plus d'informations, voir Actualisation du catalogue produit.
- Ajoutez les mises à jour de microprogramme au référentiel en sélectionnant un ou plusieurs modules de mise à jour ou une ou plusieurs mises à jour dans le catalogue produit, puis en cliquant sur l'icône **Télécharger** ( ). Une fois les mises à jour de microprogramme téléchargées et ajoutées au référentiel, l'état prend la valeur « Téléchargé ».

Remarque : Si vous souhaitez utiliser l'interface utilisateur de XClarity Administrator pour acquérir des mises à jour, XClarity Administrator doit être connecté à Internet. Si tel n'est pas le cas, vous pouvez importer les mises à jour que vous avez précédemment téléchargées.

Pour plus d'informations sur le téléchargement des mises à jour, voir Téléchargement des mises à jour de microprogramme.

- Importez les mises à jour de microprogramme que vous avez téléchargées manuellement sur un poste de travail disposant d'un accès réseau à XClarity Administrator en sélectionnant une ou plusieurs mises à jour, puis en cliquant sur l'icône **Importer** ().Pour plus d'informations sur l'importation des mises à jour, voir Téléchargement des mises à jour de microprogramme.
- Arrêtez les téléchargements de microprogramme actuellement en cours en sélectionnant une ou plusieurs mises à jour, puis en cliquant sur l'icône **Annuler les téléchargements** ().L'annulation des téléchargements annule *tous* les téléchargements de microprogramme en cours. Vous pouvez surveiller la progression détaillée et arrêter un téléchargement de microprogramme spécifique depuis le journal des travaux (voir Surveillance des travaux).
- Supprimez des modules de mise à jour ou des mises à jour individuelles du référentiel (voir Suppression des mises à jour de microprogramme).
- Exportez des mises à jour du microprogramme qui existent dans le référentiel des mises à jour du microprogramme vers un système local (voir Exporter et importer des mises à jour de microprogramme).

Utilisation d'un référentiel distant pour les mises à jour de microprogramme

By default, Lenovo XClarity Administrator utilise un référentiel local (interne) pour le stockage des mises à jour de microprogramme. Vous pouvez libérer de l'espace disque disponible pour le référentiel local XClarity Administrator à l'aide d'un partage distant monté sur un système de fichier SSH (SSHFS) comme référentiel distant. Vous pouvez ensuite utiliser des fichiers de mise à jour de microprogramme directement depuis le référentiel distant pour maintenir la conformité du microprogramme sur vos appareils.

Avant de commencer

Seules les mises à jour de microprogramme peuvent être stockées sur le partage distant. Les pilotes de périphérique Windows et les mises à jour XClarity Administrator ne peuvent être stockés que dans le référentiel des mises à jour local.

Assurez-vous que le service SFTP sur le port 22 est ouvert sur le serveur de partage distant. Les contrôleurs de gestion de la carte mère doivent avoir accès à ce port.

Le partage distant est utilisé comme serveur SFTP lorsqu'il est utilisé comme référentiel de microprogramme. Assurez-vous de ne pas désactiver le SFTP lors de la mise à jour de la configuration SSHD.

À propos de cette tâche

Lorsque vous modifiez l'emplacement du référentiel des mises à jour de microprogramme, vous pouvez choisir de copier toutes les mises à jour de microprogramme depuis le référentiel d'origine vers le nouveau référentiel.

Les fichiers de mise à jour de microprogramme du référentiel d'origine *ne sont pas* automatiquement effacés après la modification d'emplacements.

Si XClarity Administrator dispose d'autorisations de lecture et d'écriture sur le référentiel distant, le comportement est identique à l'utilisation du référentiel local. Cependant, si XClarity Administrator ne

dispose que d'autorisations de lecture, vous ne pouvez pas actualiser le catalogue, télécharger ou importer des mises à jour vers le référentiel.

Le même référentiel distant peut être partagé par plusieurs instances XClarity Administrator ; toutefois, si une instance XClarity Administrator modifie le référentiel, les autres instances XClarity Administrator ne sont pas notifiées automatiquement. Vous devez actualiser le référentiel pour obtenir les détails les plus récents. Pour actualiser le référentiel, cliquez sur **Toutes les actions → Actualiser le référentiel** depuis la page Mises à jour de microprogramme : référentiel.

Remarque : Faites attention lors de la suppression des mises à jour de microprogramme et des UXSP, en particulier si le référentiel des mises à jour de microprogramme est situé sur un partage distant utilisé par plusieurs instances XClarity Administrator.

Procédure

Pour utiliser un référentiel des mises à jour de microprogramme distant, procédez comme suit.

Etape 1. Ajoutez un partage distant à XClarity Administrator (voir Gestion de partages distants).

Etape 2. Dans la barre de menus XClarity Administrator, cliquez sur **Distribution → Mises à jour de microprogramme : référentiel**. La page Référentiel des mises à jour de microprogramme s'affiche.

Etape 3. Cliquez sur **Toutes les actions → Changer l'emplacement du référentiel** pour afficher la boîte de dialogue Changer l'emplacement du référentiel.

Etape 4. Sélectionnez le partage distant nouvellement créé depuis la liste déroulante **Emplacement du référentiel**.

Etape 5. De manière facultative, sélectionnez **Effacer le référentiel actuel** pour supprimer les fichiers de mise à jour de microprogramme de l'emplacement de référentiel actuel.

Etape 6. De manière facultative, sélectionnez **Copier les modules de mise à jour du référentiel actuel vers le nouveau référentiel** pour copier les fichiers de mise à jour de microprogramme vers le nouvel emplacement du référentiel avant de modifier l'emplacement du référentiel.

Par défaut, les fichiers de mise à jour de microprogramme existants dans le nouvel emplacement ne sont pas copiés (ils sont ignorés). De manière facultative, vous pouvez choisir de remplacer n'importe quel fichier existant, ou de remplacer uniquement les fichiers existants dont la taille ou la date de modification diffère par rapport à la liste déroulante **Règles de remplacement**.

Etape 7. Cliquez sur **OK**.

Un travail est créé pour copier les modules de mise à jour de microprogramme vers le nouveau référentiel. Vous pouvez surveiller la progression du travail en cliquant sur **Surveillance → Travaux** dans la barre de menus XClarity Administrator.

Actualisation du catalogue produit

Le catalogue produit contient des informations sur toutes les mises à jour de microprogramme disponibles pour tous les appareils pris en charge par Lenovo XClarity Administrator, notamment les châssis, les serveurs et les Commutateurs Flex.

Avant de commencer

Une connexion Internet est requise pour l'actualisation du catalogue produit.

L'actualisation du catalogue peut durer plusieurs minutes.

À propos de cette tâche

Lorsque vous actualisez le catalogue, XClarity Administrator extrait des informations sur les dernières mises à jour de microprogramme disponibles à partir du Site Web de support Lenovo XClarity et stocke ces informations dans le référentiel des mises à jour de microprogramme.

L'actualisation du catalogue a pour seul effet d'ajouter des informations sur les mises à jour de microprogramme au référentiel. Les modules de mise à jour ne sont pas téléchargés. Vous devez télécharger les mises à jour de microprogramme afin de les rendre disponibles pour installation. Pour plus d'informations sur le téléchargement des mises à jour, voir Téléchargement des mises à jour de microprogramme.

Procédure

Pour actualiser le catalogue produit, procédez comme suit.

Etape 1. Dans la barre de menus XClarity Administrator, cliquez sur **Distribution → Mises à jour de microprogramme : référentiel**. La page Référentiel des mises à jour de microprogramme s'affiche.

Etape 2. Cliquez sur l'onglet **Mises à jour individuelles** pour extraire des informations sur les modules de mise à jour de microprogramme individuels, ou cliquez sur l'onglet **UpdateXpress System Pack (UXSP)** pour extraire des informations sur les modules UXSP disponibles.

Etape 3. Cliquez sur **Actualiser le catalogue**, puis cliquez sur l'une des options suivantes pour obtenir des informations sur les dernières mises à jour de microprogramme disponibles.

- **Actualiser les éléments sélectionnés - Les éléments les plus récents uniquement**. Extrait des informations sur la dernière version des mises à jour de microprogramme disponibles uniquement pour les appareils sélectionnés.
- **Actualiser tout - Les éléments les plus récents uniquement**. Extrait des informations sur la dernière version de toutes les mises à jour de microprogramme disponibles pour tous les appareils pris en charge.
- **Actualiser les éléments sélectionnés**. Extrait des informations sur toutes les versions des mises à jour de microprogramme disponibles uniquement pour les appareils sélectionnés.
- **Actualiser tout**. Extrait des informations sur toutes les versions de toutes les mises à jour de microprogramme disponibles pour tous les appareils pris en charge.

Astuce : vous pouvez actualiser le catalogue produit et télécharger la dernière version du microprogramme en une seule étape en cliquant sur **Toutes les actions → Actualiser et télécharger la dernière version pour tous les appareils gérés** ou **Toutes les actions → Actualiser et télécharger la dernière version pour tous les appareils gérés**.

Téléchargement des mises à jour de microprogramme

Vous pouvez télécharger ou importer des mises à jour de microprogramme dans le référentiel des mises à jour de microprogramme en fonction de votre accès à Internet. Des mises à jour de microprogramme doivent être disponibles dans le référentiel des mises à jour de microprogramme pour que vous puissiez effectuer une mise à jour de microprogramme sur des dispositifs de gestion.

Avant de commencer

Assurez-vous que tous les ports et toutes les adresses Internet requis par Lenovo XClarity Administrator sont disponibles avant de tenter de télécharger le microprogramme. Pour plus d'informations sur les ports, voir Disponibilité de port et Pare-feux et serveurs proxy dans la documentation en ligne de XClarity Administrator.

Si un type d'appareil n'est pas répertorié dans le référentiel des mises à jour de microprogramme, vous devez commencer par gérer un appareil de ce type avant de pouvoir télécharger ou importer des mises à jour de microprogramme individuelles pour ce type d'appareil.

Important :

- Pour XClarity Administrator v1.1.1 et versions antérieures, vous devez télécharger et importer manuellement les modules de mise à jour de microprogramme pour le matériel Lenovo à partir de Site Web Assistance centre de données Lenovo.
- XClarity Administrator ne peut pas télécharger les mises à jour des commutateurs RackSwitch et des dispositifs de stockage Lenovo série DE, DX et SS à partir du site Web Lenovo sur le référentiel des mises à jour de microprogramme. Par conséquent, vous devez télécharger et importer manuellement ces mises à jour à partir du site Web Lenovo sur un poste de travail disposant d'un accès réseau à l'hôte XClarity Administrator, ou vous devez télécharger et appliquer les *modules de référentiel des mises à jour du microprogramme* contenant toutes les mises à jour de microprogramme disponibles.
- Internet Explorer et les navigateurs web Microsoft Edge ont une limite de téléchargement de 4 Go. Si le fichier que vous importez est supérieur à 4 Go, envisagez d'utiliser un autre navigateur web (par exemple, Chrome ou Firefox).
- Télécharger le microprogramme pour dispositifs de stockage series ThinkSystem DM :
  - Un ou plusieurs dispositifs de stockage ThinkSystem DM Series doivent être gérés par XClarity Administrator.
  - Chaque dispositif de stockage series DM ThinkSystem doit être autorisé pour le service et la prise en charge du matériel.
  - Vous devez spécifier le pays dans lequel se trouvent les dispositifs de stockage ThinkSystem DM Series sur les mises à jour de microprogramme : page référentiel. Seul le microprogramme chiffré peut être téléchargé pour des appareils dans les pays suivants : L'Arménie, la Biélorussie, la Chine, Cuba, l'Iran, le Kazakhstan, le Kirghizistan, la Corée du nord, la Russie, le Soudan, la Syrie.

À propos de cette tâche

Vous pouvez télécharger les mises à jour du microprogramme de plusieurs manières différentes :

- **Modules de référentiel des mises à jour de microprogramme**

  Les modules de référentiel de mise à jour de microprogramme sont des collections des microprogrammes les plus récents et disponibles au moment de la publication de XClarity Administrator pour les appareils principaux pris en charge, ainsi qu'une stratégie de conformité de microprogramme actualisée par défaut. Ces modules de référentiel sont importés, puis appliqués à partir de la page Mettre à jour le serveur de gestion. Lorsque vous appliquez un module de référentiel de mises à jour de microprogramme, chaque module de mise à jour présent dans ce module est ajouté au référentiel de mises à jour de microprogramme, et une stratégie de conformité de microprogramme est automatiquement créée pour tous les appareils gérables. Vous pouvez copier cette stratégie prédéfinie, mais vous ne pouvez pas la modifier.

  Les modules de référentiel suivants sont disponibles.

  - **lnvgy_sw_lxca_cmmswitchrepo***x-x.x.x*_**anyos_noarch**. Contient des mises à jour de microprogramme pour tous les modules CMM et les commutateurs Flex System.
  - **lnvgy_sw_lxca_storagerackswitchrepo***x-x.x.x*_**anyos_noarch**. Contient des mises à jour de microprogramme pour tous les commutateurs RackSwitch et les dispositifs Lenovo Storage.
  - **lnvgy_sw_lxca_systemxrepo***x-x.x.x*_**anyos_noarch**. Contient des mises à jour de microprogramme pour tous les serveurs des séries Converged HX, Flex System, NeXtScale et System x.
  - **lnvgy_sw_thinksystemrepo***x-x.x.x*_**anyos_noarch**. Contient des mises à jour de microprogramme pour tous les serveurs ThinkSystem et ThinkAgile.
  - **lnvgy_sw_lxca_thinksystemv2repo***x-x.x.x*_**anyos_noarch**. Contient des mises à jour de microprogramme pour tous les serveurs ThinkSystem V2 et ThinkAgile.

– **lnvgy_sw_lxca_thinksystemv3repo***x-x.x.x*_**anyos_noarch**. Contient des mises à jour de microprogramme pour tous les serveurs ThinkSystem V3 et ThinkAgile.

Vous pouvez déterminer si des modules de référentiel des mises à jour de microprogramme sont stockés dans le référentiel dans la colonne **État du téléchargement** sur la page Mettre à jour le serveur de gestion. Cette colonne contient les valeurs suivantes :

– **Téléchargé**. Le module de référentiel des mises à jour de microprogramme est stocké dans le référentiel.
– **Non téléchargé**. Le module de référentiel des mises à jour de microprogramme est disponible, mais pas stocké dans le référentiel.

- **UpdateXpress System Packs (UXSPs)**

  Remarque : Pour les serveurs équipés de XCC2, ces packages sont appelés modules (bundles) de microprogramme. *Bundle* est utilisé dans les noms de package et les noms de stratégie prédéfinis.

  Les modules UXSP contiennent les mises à jour de microprogramme et de pilote de périphérique disponibles les plus récentes, organisées par système d'exploitation. Lorsque vous téléchargez des modules UXSP, XClarity Administrator télécharge l'UXSP applicable à la version indiquée dans le catalogue et stocke les modules de mise à jour dans le référentiel des mises à jour de microprogramme. Lorsque vous téléchargez un UXSP, chaque mise à jour de microprogramme dans le UXSP est ajoutée au référentiel des mises à jour de microprogramme et est répertoriée sous l'onglet **Mises à jour individuelles**, et une stratégie de conformité du microprogramme par défaut est automatiquement créée pour tous les appareils gérables à l'aide des noms suivants. Vous pouvez copier cette stratégie prédéfinie, mais vous ne pouvez pas la modifier.
  – *{uxsp-version}-{date}-{nom-serveur-abrégé}***-UXSP** (par exemple, `v1.50-2017-11-22- SD530-UXSP`)
  – *{uxsp-version}-{numérodebuild}-{nom-serveur-abrégé}***-bundle** (par exemple, `22a.0-kaj92va-SR650V3-bundle`)

  Remarque : Lorsque vous téléchargez ou importez des UXSP depuis la page Mises à jour de microprogramme : référentiel, seules les mises à jour de microprogramme sont téléchargées et stockées dans le référentiel. Les mises à jour de pilote de périphérique sont supprimées. Pour plus d'informations sur le téléchargement ou de l'importation des mises à jour de pilote de périphérique Windows à l'aide de UXSP, voir Gestion du référentiel des pilotes de périphérique SE.

  Vous pouvez déterminer si les UXSP sont stockés dans le référentiel des mises à jour de microprogramme à partir de la colonne **État du téléchargement** sous l'onglet **Mises à jour individuelles** de la page Mises à jour de microprogramme : référentiel. Cette colonne contient les valeurs suivantes :

  – **Téléchargé**. L'ensemble du contenu du module de mise à jour ou la mise à jour de microprogramme individuelle est stocké dans le référentiel.
  – *x* **sur** *y* **téléchargés**. Une partie seulement des mises à jour de microprogramme présentes dans le module de mise à jour est stockée dans le référentiel. Les nombres entre parenthèses indiquent le nombre de mises à jour disponibles et le nombre de mises à jour stockées, ou bien il n'existe aucune mise à jour pour le type d'appareil spécifique.
  – **Non téléchargé**. La totalité du contenu du module de mise à jour ou la mise à jour de microprogramme individuelle est disponible, mais pas stockée dans le référentiel.

- **Mises à jour individuelles du microprogramme**

  Vous pouvez télécharger des modules de mise à jour de microprogramme individuels. Lorsque vous téléchargez des modules de mise à jour de microprogramme, XClarity Administrator télécharge la mise à jour applicable à la version indiquée dans le catalogue et stocke les modules de mise à jour dans le référentiel des mises à jour de microprogramme. Vous pouvez ensuite créer des stratégies de conformité de microprogramme à l'aide de ces modules de mise à jour pour chacun des appareils gérés.

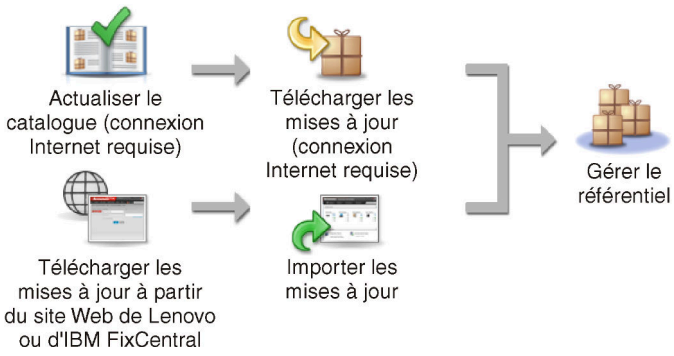
Remarque : Les mises à jour de microprogramme principales (telles que celles de type contrôleur de gestion, UEFI et pDSA) sont indépendantes du système d'exploitation. Les modules de mise à jour de microprogramme pour les systèmes d'exploitation RHEL 6 ou SLES 11 sont utilisés pour mettre à jour les nœuds de traitement et les serveurs rack. Pour plus d'informations sur les modules de mise à jour de microprogramme qui doivent être utilisés pour vos serveurs gérés, voir Téléchargement des mises à jour de microprogramme.

Vous pouvez déterminer si des *mises à jour de microprogramme* spécifiques sont stockées dans le référentiel des mises à jour de microprogramme à partir de la colonne **État du téléchargement** sous l'onglet **Mises à jour individuelles** de la page Mises à jour de microprogramme : référentiel. Cette colonne contient les valeurs suivantes.

- **Téléchargé**. L'ensemble du contenu du module de mise à jour ou la mise à jour de microprogramme individuelle est stocké dans le référentiel.
- *x* **sur** *y* **téléchargés**. Une partie seulement des mises à jour de microprogramme présentes dans le module de mise à jour est stockée dans le référentiel. Les nombres entre parenthèses indiquent le nombre de mises à jour disponibles et le nombre de mises à jour stockées, ou bien il n'existe aucune mise à jour pour le type d'appareil spécifique.
- **Non téléchargé**. La totalité du contenu du module de mise à jour ou la mise à jour de microprogramme individuelle est disponible, mais pas stockée dans le référentiel.

Lorsque vous installez XClarity Administrator ou effectuez une mise à jour vers une nouvelle version, il est recommandé de télécharger le module de référentiel le plus récent afin de vous assurer que vous disposez des dernières mises à jour de microprogramme. Ensuite, vous pouvez planifier un travail périodique pour actualiser le catalogue afin de rechercher des mises à jour individuelles qui ont été publiées sur le Web depuis le dernier référentiel, puis télécharger ces mises à jour par voie électronique, une par une.

XClarity Administrator doit être connecté à Internet pour actualiser le catalogue et télécharger les mises à jour de microprogramme. S'il n'est pas connecté à Internet, vous pouvez télécharger manuellement les fichiers sur un poste de travail disposant d'un accès réseau à l'hôte XClarity Administrator à l'aide d'un navigateur Web, puis importer les fichiers dans le référentiel des mises à jour de microprogramme.



Lorsque vous importez manuellement des mises à jour du microprogramme dans XClarity Administrator, vous devez inclure les fichiers requis suivants : contenu (image et MIB), métadonnées, historique des modifications et Readme. Par exemple :

- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.tgz
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.xml
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.chg
- lnvgy_sw_lxca_thinksystemrepo*_anyos_noarch.txt

Remarque : Les mises à jour de microprogramme principales (telles que celles de type contrôleur de gestion, UEFI et pDSA) sont indépendantes du système d'exploitation. Les modules de mise à jour de

microprogramme pour les systèmes d'exploitation RHEL 6 ou SLES 11 sont utilisés pour mettre à jour les nœuds de traitement et les serveurs rack.

Un message s'affiche sur la page lorsque le niveau de remplissage du référentiel est supérieur à 50 %. Un autre message s'affiche sur la page lorsque le niveau de remplissage du référentiel est supérieur à 85 %. Pour réduire l'espace utilisé dans le référentiel, vous pouvez retirer les fichiers image et les stratégies inutilisés. Vous pouvez retirer des stratégies de conformité de microprogramme inutilisées et les modules de microprogramme qui leur sont associés en cliquant sur **Distribution → Stratégies de conformité**, en sélectionnant une ou plusieurs stratégies à supprimer, puis en cliquant sur **Actions → Supprimer tous les modules de microprogramme et toutes les stratégies**.

Le tableau suivant répertorie les différences relatives à l'acquisition des packs de référentiel des mises à jour de microprogramme, des modules UXSPs et des modules de mise à jour de microprogramme individuel.

Module de mise à jour	**Page d'interface utilisateur de téléchargement et d'importation des fichiers**	**Page Web de téléchargement manuel des fichiers**	**Le référentiel des mises à jour de microprogramme est-il actualisé ?**	**La stratégie de conformité du microprogramme est-elle actualisée automatiquement ?**
Modules de référentiel des mises à jour de microprogramme	Page Mettre à jour le serveur de gestion **Remarque :** Vous devez importer, puis appliquer le module de référentiel.	Page Web de téléchargements XClarity Administrator	Oui	Oui
UpdateXpress System Packs	Mises à jour du microprogramme : page Référentiel, onglet **UpdateXpress System Packs (UXSPs)**	Page Web Lenovo XClarity Essentials UpdateXpress	Oui	Oui
Mises à jour du microprogramme	Mises à jour du microprogramme : page Référentiel, onglet **Mises à jour individuelles**	Site Web Assistance centre de données Lenovo **Remarques :** Utilisez le Site Web Fix Central pour les appareils suivants : • Flex System x220 Type 2585, 7906 • Flex System x222 Compute Nod Type 2589, 7916 • Flex System x240 Type 7863, 8737, 8738, 8956 • Flex System x280 / x480 / x880 X6 Type 4259, 7903 • Flex System x440 Type 2584, 7917	Oui	Non

Procédure

Pour télécharger une ou plusieurs mises à jour de microprogramme, procédez comme suit.

- Pour importer un ou plusieurs *modules de référentiel des mises à jour de microprogramme* :

1. Dans la barre de menus de XClarity Administrator, cliquez sur **Administration → Mettre à jour le serveur de gestion** pour afficher la page Mise à jour du serveur de gestion.
2. Téléchargez les modules de référentiel les plus récents :
   - Si XClarity Administrator est connecté à Internet :
     a. Procédez à l'extraction des informations relatives aux dernières mises à jour en cliquant sur **Actualiser le catalogue → .Actualiser tous les éléments gérés - Uniquement les plus récents**). Les nouvelles mises à jour du serveur de gestion et les nouveaux modules de référentiel des mises à jour de microprogramme sont répertoriés dans le tableau figurant sur la page « Mise à jour du serveur de gestion ».

        L'actualisation du référentiel peut durer plusieurs minutes.

        Remarque : L'actualisation du référentiel n'entraîne pas le téléchargement automatique des fichiers de contenu. Seuls les fichiers de métadonnées et Readme sont téléchargés.

     b. Sélectionnez les modules de référentiel des mises à jour de microprogramme que vous voulez télécharger.

        Astuce : Prenez soin de sélectionner des modules pour lesquels « Pack supplémentaire » est indiqué dans la colonne **Type**.

     c. Cliquez sur l'icône **Télécharger la sélection** ( ). Une fois le téléchargement terminé, la colonne **État du téléchargement** pour cette mise à jour de logiciel contient la valeur « Téléchargé ».
   - Si XClarity Administrator n'est pas connecté à Internet :
     a. Téléchargez les modules de référentiel des mises à jour de microprogramme à partir de la Page Web de téléchargements XClarity Administrator sur un poste de travail disposant d'une connexion réseau à l'hôte XClarity Administrator.
     b. Sur la page Mise à jour du serveur de gestion, cliquez sur l'icône **Importer** ( ).
     c. Cliquez sur **Sélectionner des fichiers** et recherchez l'emplacement des modules de référentiel des mises à jour de microprogramme sur le poste de travail.
     d. Sélectionnez tous les fichiers de module, puis cliquez sur **Ouvrir**.

        Vous devez importer le fichier de métadonnées (.xml ou .json), ainsi que le fichier image ou de contenu (.zip, .bin, .uxz, ou .tgz), le fichier historique des modifications (.chg) et le fichier Readme (.txt) pour la mise à jour. Tout fichier sélectionné qui n'est pas spécifié dans le fichier de métadonnées est ignoré. Si vous n'incluez pas le fichier de métadonnées, la mise à jour n'est pas importée.

     e. Cliquez sur **Importer**.

        Une fois l'importation terminée, les modules de référentiel des mises à jour de microprogramme sont répertoriés dans le tableau figurant sur la page Mise à jour du serveur de gestion et la colonne **État du téléchargement** pour chaque mise à jour contient la valeur « Téléchargé ».
3. Sélectionnez les modules de référentiel de mises à jour de microprogramme que vous souhaitez installer sur le référentiel des mises à jour de microprogramme.

   Remarque : Assurez-vous que la colonne **État du téléchargement** contient la valeur « Téléchargé » et que la colonne **Type** contient la valeur « Correctif ».
4. Cliquez sur l'icône **Effectuer la mise à jour** ( ) pour ajouter les modules de mise à jour de microprogramme au référentiel.
5. Patientez quelques minutes jusqu'à ce que la mise à jour soit terminée et que XClarity Administrator soit redémarré.

6. Déterminez si la mise à jour est terminée en actualisant le navigateur Web.

   Une fois la mise à jour terminée, la page Mise à jour du serveur de gestion s'affiche et la colonne **État appliqué** contient la valeur « Appliqué ».

7. Effacez le cache du navigateur Web.

- Pour télécharger un ou plusieurs modules *UXSPs*.
  1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Mises à jour de microprogramme : référentiel** pour afficher la page Référentiel des mises à jour de microprogramme.
  2. Cliquez sur l'onglet **UpdateXpress System Packs (UXSPs)**.
  3. Téléchargez les derniers modules UXSPs :
     - Si XClarity Administrator est connecté à Internet :

       Pour actualiser le catalogue et télécharger les derniers modules UXSP pour tous les appareils gérés, cliquez sur **Toutes les actions → Actualiser et télécharger la version la plus récente pour tous les appareils gérés**.

       Pour actualiser le catalogue et télécharger les derniers modules UXSP uniquement pour les appareils sélectionnés :

       a. Développez l'appareil pour afficher la liste des modules UXSPs disponibles.
       b. Sélectionnez un ou plusieurs modules UXSP à télécharger.
       c. Cliquez sur **Toutes les actions → Actualiser et télécharger la version la plus récente pour les appareils sélectionnés**.

          Une fois le téléchargement terminé, la colonne **État du téléchargement** des modules UXSP sélectionnés affiche « Téléchargé »

     - Si XClarity Administrator n'est pas connecté à Internet :

       a. Téléchargez les modules UXSPs de Page Web Lenovo XClarity Essentials UpdateXpress sur un poste de travail disposant d'une connexion réseau à l'hôte XClarity Administrator
       b. Depuis XClarity Administrator, cliquez sur l'icône **Importer** ().
       c. Cliquez sur **Sélectionner des fichiers** et recherchez l'emplacement des modules UXSPs sur le poste de travail.
       d. Sélectionnez tous les fichiers de module, puis cliquez sur **Ouvrir**.

          Vous devez importer le fichier de métadonnées (.xml ou .json), ainsi que le fichier image ou de contenu (.zip, .bin, .uxz, ou .tgz), le fichier historique des modifications (.chg) et le fichier Readme (.txt) pour la mise à jour. Tout fichier sélectionné qui n'est pas spécifié dans le fichier de métadonnées est ignoré. Si vous n'incluez pas le fichier de métadonnées, la mise à jour n'est pas importée.

       e. Cliquez sur **Importer**.

          Une fois l'importation terminée, les modules de référentiel des mises à jour de microprogramme sont répertoriés dans le tableau figurant sur la page Mise à jour du serveur de gestion et la colonne État du téléchargement pour chaque mise à jour contient la valeur « Téléchargé ».

- Pour télécharger un ou plusieurs *modules de mise à jour de microprogramme* individuels.
  1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Mises à jour de microprogramme : référentiel** pour afficher la page Référentiel des mises à jour de microprogramme.

2. Si vous téléchargez le microprogramme pour des dispositifs de stockage ThinkSystem DM Series, sélectionnez le pays où se trouvent ces dispositifs.
3. Cliquez sur l'onglet **Mises à jour individuelles**.
4. Téléchargez les dernières mises à jour du microprogramme individuelles.
   - Si XClarity Administrator est connecté à Internet :

     Pour actualiser le catalogue et télécharger le dernier microprogramme pour tous les appareils gérés, cliquez sur **Toutes les actions → Actualiser et télécharger la version la plus récente pour tous les appareils gérés**.

     Pour actualiser le catalogue et télécharger le dernier microprogramme uniquement pour les appareils sélectionnés :

     a. Développez l'appareil pour afficher la liste des mises à jour de microprogramme disponibles.
     b. Sélectionnez une ou plusieurs mise à jour de microprogramme à télécharger.

        Astuce : Un module de mise à jour peut comporter plusieurs mises à jour de microprogramme. Lorsque vous téléchargez une mise à jour de microprogramme, vous pouvez choisir de télécharger la totalité du module de mise à jour ou certaines mises à jour. Vous pouvez également choisir de télécharger plusieurs modules en même temps.
     c. Cliquez sur **Toutes les actions → Actualiser et télécharger la version la plus récente pour les appareils sélectionnés**.

        Une fois le téléchargement terminé, la colonne **État du téléchargement** pour cette mise à jour de microprogramme contient la valeur « Téléchargé ».
   - Si XClarity Administrator n'est pas connecté à Internet :

     a. Téléchargez les modules de mise à jour de microprogramme depuis les Site Web Assistance centre de données Lenovo sur un poste de travail disposant d'une connexion réseau à l'hôte XClarity Administrator.

        Pour les serveurs suivants, téléchargez les mises à jour de microprogramme applicables au système d'exploitation SLES 11 à partir du Site Web Fix Central :

        - Flex System x220 Type 2585, 7906
        - Flex System x222 Compute Nod Type 2589, 7916
        - Flex System x240 Type 7863, 8737, 8738, 8956
        - Flex System x280 / x480 / x880 X6 Type 4259, 7903
        - Flex System x440 Type 2584, 7917

        Pour les autres serveurs, téléchargez les mises à jour de microprogramme applicables au système d'exploitation RHEL 6 à partir du Site Web de support Lenovo XClarity :

     b. Depuis XClarity Administrator, cliquez sur l'icône **Importer** ( ).
     c. Cliquez sur **Sélectionner des fichiers** et recherchez l'emplacement des mises à jour de microprogramme sur le poste de travail.
     d. Sélectionnez tous les fichiers de module, puis cliquez sur **Ouvrir**.

        Vous devez importer le fichier de métadonnées (.xml ou .json), ainsi que le fichier image ou de contenu (.zip, .bin, .uxz, ou .tgz), le fichier historique des modifications (.chg) et le fichier Readme (.txt) pour la mise à jour. Tout fichier sélectionné qui n'est pas spécifié dans le fichier de métadonnées est ignoré.

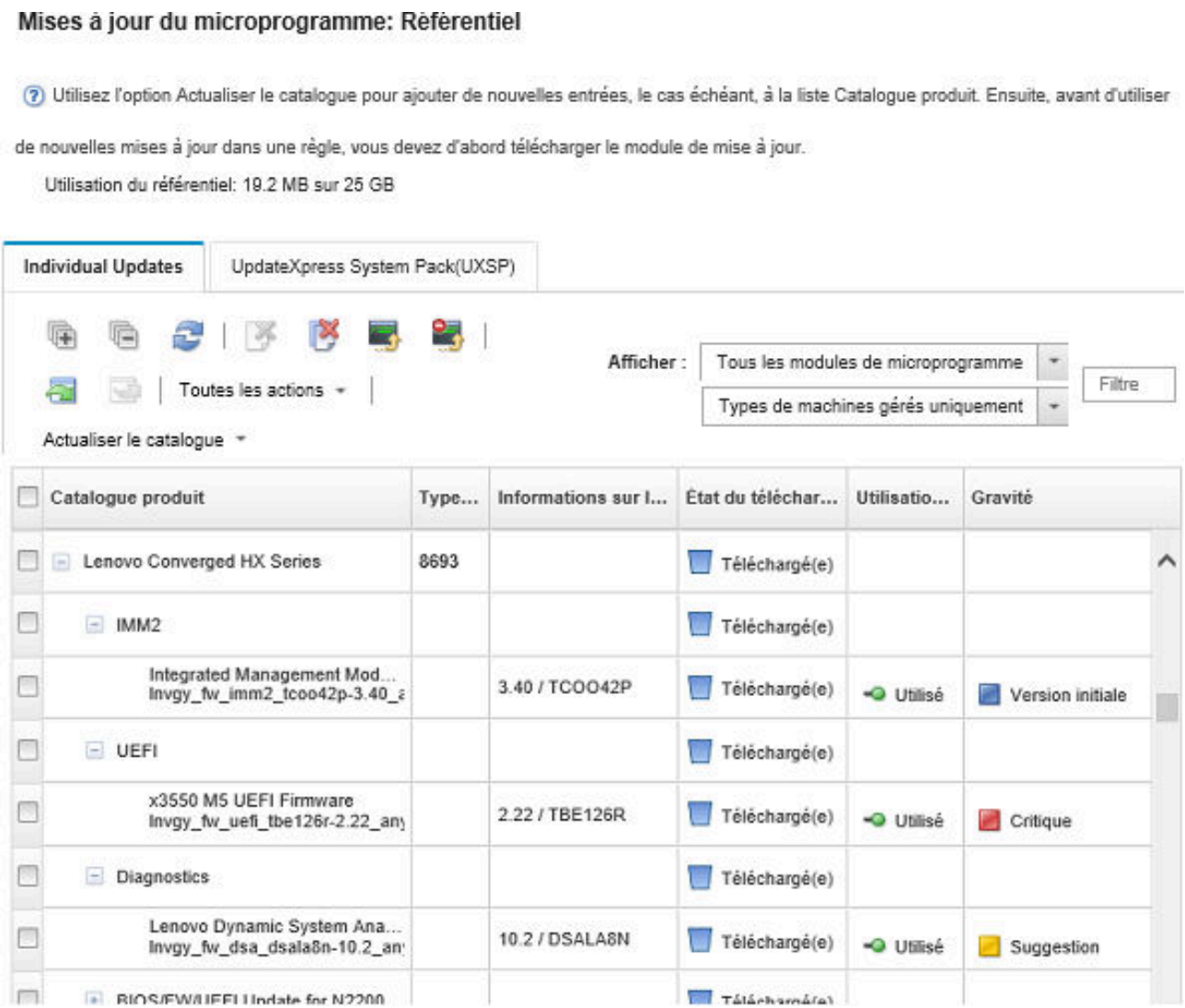
        Attention :

- Importez uniquement ces fichiers requis. N’importez pas d’autres fichiers susceptibles de se trouver sur les sites Web de téléchargement du microprogramme.
- Si vous n'incluez pas le fichier XML dans le module de mise à jour, la mise à jour n'est pas importée.
- Si vous n'incluez pas tous les fichiers requis associés à la mise à jour, le référentiel indique que la mise à jour n'a pas été téléchargée, ce qui signifie qu'elle a été partiellement importée. Vous pouvez alors importer les fichiers manquants en les sélectionnant et en les important.
- Les mises à jour de microprogramme principales (telles que celles de type contrôleur de gestion, UEFI et pDSA) sont indépendantes du système d'exploitation. Les modules de mise à jour de microprogramme pour les systèmes d'exploitation RHEL 6 ou SLES 11 sont utilisés pour mettre à jour les nœuds de traitement et les serveurs rack. Pour plus d'informations sur les modules de mise à jour de microprogramme qui doivent être utilisés pour vos serveurs gérés, voir Téléchargement des mises à jour de microprogramme.

e. Cliquez sur **Importer**.

L'actualisation du catalogue et le téléchargement des mises à jour du microprogramme peuvent durer plusieurs minutes. Une fois les mises à jour téléchargées et stockées dans le référentiel, la ligne du catalogue produit est mise en évidence et la colonne **État du téléchargement** contient la valeur « Téléchargé ».

Remarque : Le type de machine pour certains commutateurs peut apparaître sous la forme d'un nombre hexadécimal.



Après avoir terminé

Vous pouvez configurer la taille maximum du référentiel des mises à jour (dont le microprogramme, les pilotes de périphérique SE et les mises à jour du serveur de gestion) depuis la page Référentiel de microprogramme en cliquant sur **Toutes les actions → Paramètres globaux**. La taille minimale est de 50 Go. La taille maximum dépend de la quantité d'espace disque disponible sur le système local.

Exporter et importer des mises à jour de microprogramme

Vous pouvez exporter des mises à jour de microprogramme individuelles et des UpdateXpress System Packs (UXSPs) qui existent dans le référentiel vers le système local.

À propos de cette tâche

Seules les mises à jour de microprogramme qui existent dans le référentiel sont exportées. Assurez-vous que l'état de téléchargement des mises à jour du microprogramme sélectionnées indique « Téléchargé. »

Tous les fichiers associés à la mise à jour du microprogramme sont exportés, y compris l'image de mise à jour ou le fichier de charge utile (.zip, .bin, .uxz, ou .tgz), le fichier de métadonnées (.xml ou .json), le fichier de modification de l'historique (.chg) et le fichier readme (.txt).

Attention : Ne modifiez pas le nom des fichiers de mise à jour de microprogramme.

Procédure

- Pour exporter des mises à jour de microprogramme :
  1. Cliquez sur l'onglet **Mises à jour individuelles** ou sur l'onglet **UpdateXpress System Packs (UXSPs)**.
  2. Sélectionnez une ou plusieurs mises à jour du microprogramme.
  3. Cliquez sur l'icône **Exporter** ( ).
- Pour importer des mises à jour de microprogramme :

  Vous pouvez importer des fichiers que vous avez manuellement exportés depuis Lenovo XClarity Administrator et des fichiers que vous avez manuellement téléchargés à partir du Web. Pour plus d'informations, voir Téléchargement des mises à jour de microprogramme.

Suppression des mises à jour de microprogramme

Vous pouvez supprimer des mises à jour de microprogramme et des modules UXSPs (UpdateXpress System Packs) à partir du référentiel des mises à jour de microprogramme.

Avant de commencer

Assurez-vous que tous les travaux de mise à jour en cours d'exécution ou planifiés qui utilisent une stratégie de conformité de microprogramme contenant les mises à jour de microprogramme à supprimer sont terminés ou annulés (voir Surveillance des travaux).

Avant de supprimer la mise à jour, assurez-vous qu'elle n'est pas utilisée dans une stratégie de conformité de microprogramme. Vous ne pouvez pas supprimer les modules de mise à jour de microprogramme actuellement utilisés dans une ou plusieurs stratégies de conformité de microprogramme.

La suppression d'un module UXSP supprime également la stratégie de conformité de microprogramme qui a été automatiquement créée pour ce module UXSP.

Remarque : Faites attention lors de la suppression des mises à jour de microprogramme et des UXSP, en particulier si le référentiel des mises à jour de microprogramme est un partage distant utilisé par plusieurs instances XClarity Administrator.

Procédure

Pour supprimer une ou plusieurs mises à jour de microprogramme du référentiel, procédez comme suit.

Etape 1. Désaffectez toutes les stratégies de conformité du microprogramme contenant les mises à jour de microprogramme à supprimer de tous les appareils gérés.

a. Dans la barre de menus XClarity Administrator, cliquez sur **Distribution → Appliquer/Activer**. La page Mises à jour de microprogramme : Appliquer/Activer s'affiche.

b. Sélectionnez « Aucune affectation » ou choisissez une autre stratégie de conformité de microprogramme dans la colonne **Stratégie affectée** pour les appareils gérés qui utilisent la stratégie de conformité de microprogramme.

Etape 2. Supprimez toutes les stratégies de conformité du microprogramme définies par l'utilisateur et contenant les mises à jour de microprogramme à supprimer, ou éditez les stratégies de conformité du microprogramme afin de retirer les mises à jour de microprogramme à supprimer.

a. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Stratégies de conformité**. La page Stratégies de conformité des mises à jour de microprogramme s'affiche.

b. Sélectionnez la stratégie de conformité de microprogramme, puis sélectionnez l'icône **Supprimer** () pour supprimer la stratégie ou cliquez sur l'icône **Éditer** () pour retirer les mises à jour de microprogramme de la stratégie.

Etape 3. Supprimez les mise à jour du microprogramme.

- **Mises à jour individuelles du microprogramme**
  1. Dans la barre de menus XClarity Administrator, cliquez sur **Distribution → Mises à jour de microprogramme : référentiel**. La page Référentiel des mises à jour de microprogramme s'affiche.
  2. Cliquez sur l'onglet **Mises à jour individuelles**.
  3. Sélectionnez une ou plusieurs mises à jour de microprogramme à supprimer.
  4. Cliquez sur l'icône **Supprimer uniquement les images** () pour supprimer uniquement le fichier image ou le fichier de contenu (.zip, .bin, .uxz ou .tgz). Les informations sur la mise à jour sont conservées afin que vous puissiez aisément télécharger la mise à jour à nouveau. Vous pouvez également cliquer sur l'icône **Supprimer entièrement les modules de mise à jour** () pour supprimer entièrement les modules de mise à jour, y compris le fichier image ou de contenu, le fichier historique des modifications (.chg), le fichier Readme (.txt) et le fichier de métadonnées (.xml ou .json).

  Lorsque vous supprimez une mise à jour de microprogramme, les fichiers de contenu sont retirés ; en revanche, le fichier de métadonnées, qui contient des informations sur la mise à jour, est conservé, et vous pouvez facilement télécharger à nouveau la mise à jour si besoin est, ainsi que les modifications **État du téléchargement** sur « Non téléchargé ».
- **UXSPs**
  1. Dans la barre de menus XClarity Administrator, cliquez sur **Distribution → Mises à jour de microprogramme : référentiel**. La page Référentiel des mises à jour de microprogramme s'affiche.
  2. Cliquez sur l'onglet **UpdateXpress System Pack (UXSP)**.
  3. Sélectionnez un ou plusieurs modules UXSPs à supprimer.
  4. Cliquez sur l'icône **Supprimer le module UXSP et la stratégie associée** () pour supprimer entièrement les modules UXSP, y compris le fichier image ou de contenu, le fichier historique des modifications (.chg), le fichier Readme (.txt), le fichier de métadonnées (.xml ou .json) et toutes les stratégies de conformité du microprogramme.

  Si certains modules UXSPs sélectionnés sont associés à des stratégies qui sont en cours d'utilisation (affectées aux appareils), la boîte de dialogue de suppression des modules UXSP des stratégies et des modules de mise à jour s'affiche. Choisissez de supprimer les stratégies affectées en du module UXSP et les stratégies non affectées, puis cliquez sur **OK**.

Création et affectation de stratégies de conformité de microprogramme

Les stratégies de conformité de microprogramme permettent de garantir que le microprogramme présent sur certains appareils gérés est au niveau en cours ou à un niveau spécifique en marquant les appareils qui nécessitent une attention. Chaque stratégie de conformité du microprogramme identifie les appareils surveillés et le niveau de microprogramme qui doit être installé pour assurer la bonne conformité de ces appareils. Vous pouvez définir la conformité au niveau du composant du microprogramme ou de l'appareil. XClarity Administrator va ensuite se servir de ces stratégies pour vérifier l'état des appareils gérés, mais aussi pour identifier ceux qui ne sont plus conformes.

Avant de commencer

Lorsque vous créez une stratégie de conformité de microprogramme, vous sélectionnez la version de mise à jour cible à appliquer aux appareils qui seront affectés à ladite stratégie. Avant de créer la stratégie, assurez-vous que les mises à jour de microprogramme pour la version cible se trouvent dans le référentiel des mises à jour (voir Téléchargement des mises à jour de microprogramme).

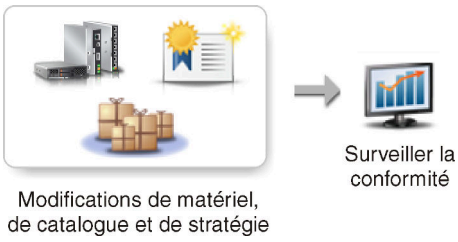
Si un type d'appareil n'est pas répertorié dans le référentiel des mises à jour de microprogramme, vous devez commencer par gérer un appareil de ce type, puis télécharger ou importer l'ensemble complet de mises à jour de microprogramme avant de créer des stratégies de conformité pour des appareils de ce type.

À propos de cette tâche

Lorsque vous créez une stratégie de conformité de microprogramme, vous pouvez déclencher le marquage d'un appareil par XClarity Administrator lorsque :
- Le microprogramme de l'appareil est à un niveau inférieur
- Le microprogramme de l'appareil ne correspond pas à la version cible de conformité

XClarity Administrator est fourni avec une stratégie de conformité du microprogramme prédéfinie, appelée **Microprogramme le plus récent dans le référentiel**. Lorsque le nouveau microprogramme est téléchargé ou importé dans le référentiel, cette stratégie est mise à jour pour y inclure les dernières versions disponibles du microprogramme.

Une fois qu'une stratégie de conformité de microprogramme a été assignée à un appareil, XClarity Administrator vérifie l'état de conformité de chaque appareil lorsque des modifications ont été apportées à l'inventaire de l'appareil ou au référentiel des mises à jour de microprogramme. Lorsque le microprogramme d'un appareil est non compatible avec la stratégie affectée, XClarity Administrator indique que l'appareil n'est pas compatible sur la page Mises à jour de microprogramme : appliquer/activer, selon la règle que vous avez spécifiée dans la stratégie de conformité de microprogramme



Par exemple, vous pouvez créer une stratégie de conformité de microprogramme qui définit le niveau de référence du microprogramme qui est installé dans tous les appareils ThinkSystem SR850 et affecter ensuite la stratégie de conformité de microprogramme à tous les appareils ThinkSystem SR850 gérés. Lorsque le référentiel des mises à jour de microprogramme est actualisé et qu'une nouvelle mise à jour de microprogramme est ajoutée, il se peut que ces nœuds de traitement ne soient plus conformes. Lorsque cela se produit, XClarity Administrator met à jour la page Mises à jour de microprogramme : Appliquer/Activer pour indiquer que les appareils ne sont pas conformes et génère une alerte.

Remarque : Vous pouvez choisir d'afficher ou masquer les alertes pour les dispositifs qui ne répondent pas aux exigences de leurs des stratégies de conformité du microprogramme affectée (voir Configuration des paramètres globaux à jour de microprogramme). Les alertes sont masqués par défaut.

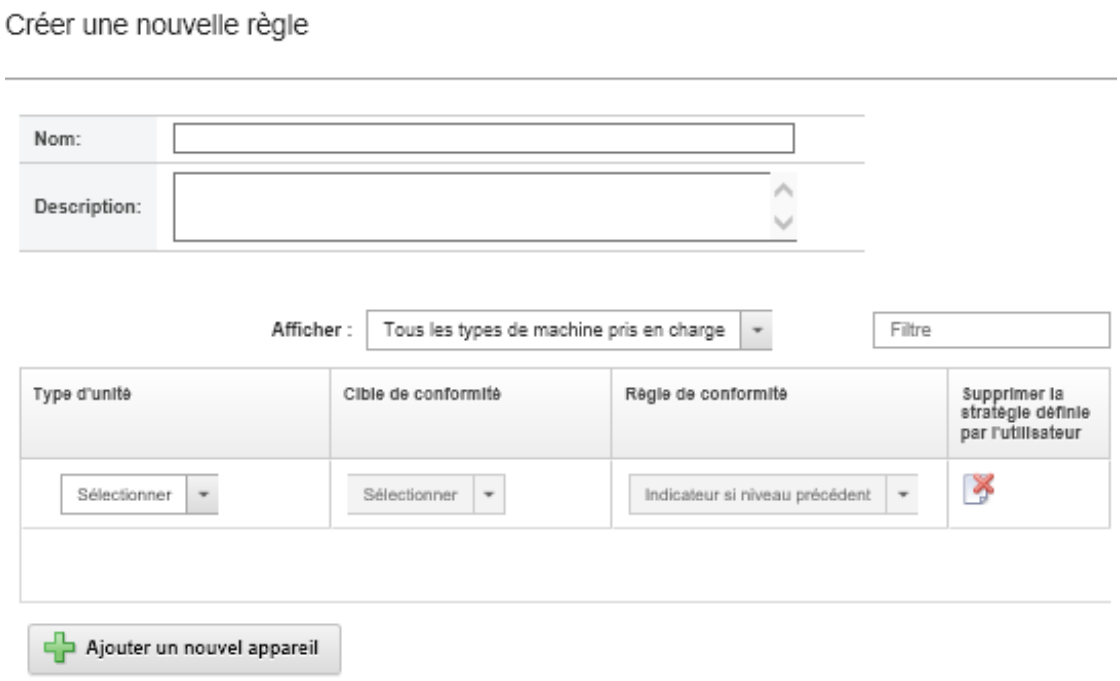
Procédure

Pour créer une stratégie de conformité de microprogramme et l'assigner , procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Mises à jour de microprogramme : Stratégies de conformité**. La page Stratégie de conformité s'affiche avec une liste répertoriant toutes les stratégies de conformité de microprogramme existantes.

Etape 2. Créer une stratégie de conformité-microprogramme.

1. Cliquez sur l'icône **Créer** ( ) pour afficher la boîte de dialogue Créer une stratégie.



2. Indiquez le nom et la description de la stratégie de conformité de microprogramme.
3. Renseignez le tableau en fonction des critères suivants pour chaque appareil.
   - **Type d'appareil**. Choisissez un type d'appareil ou un composant auquel cette stratégie doit s'appliquer.

     Astuce : Si vous choisissez un serveur, le niveau de conformité correspond au niveau UXSP. Cependant, vous pouvez aussi choisir de développer le serveur afin de spécifier des niveaux de microprogramme spécifiques pour chaque composant, tel que le contrôleur de gestion de la carte mère ou l'interface UEFI.
   - **Cible de conformité**. Indiquez la cible de conformité des appareils applicables et des sous-composants.

     Pour les serveurs, vous pouvez choisir l'une des valeurs suivantes.

- **Par défaut**. Définit la cible de conformité de chaque sous-composant sur la valeur par défaut (par exemple, l'ensemble de microprogramme le plus récent dans le référentiel pour cet appareil).
- **Ne pas mettre à jour**. Définit la cible de conformité de chaque sous-composant sur « Ne pas mettre à jour. »

Pour des appareils sans sous-composants (par exemple, les modules CMM, les commutateurs ou les dispositifs de stockage) ou les sous-composants d'un serveur, vous pouvez choisir l'une des valeurs suivantes.

- <*niveau_microprogramme*>. Indique le niveau de microprogramme de base.
- **Ne pas mettre à jour**. Indique que le microprogramme ne doit pas être mis à jour. Notez que le microprogramme du contrôleur de gestion de sauvegarde n'est pas mis à jour par défaut.

Remarque : Lorsque vous définissez les valeurs par défaut pour les sous-composants d'un serveur, la cible de conformité de ce serveur obtient le statut **Personnalisé**.

- **Règle de conformité**. Indiquez à quel moment un appareil est marqué comme non compatible dans la colonne **Version installée** sur la page Mises à jour de microprogramme : Appliquer/Activer.
  - **Marquer si niveau inférieur**. Si le niveau de microprogramme installé sur un appareil est antérieur au niveau spécifié dans la stratégie de conformité de microprogramme, l'appareil est marqué comme non compatible. Par exemple, si vous remplacez une carte réseau dans un nœud de traitement et que le microprogramme sur cette carte réseau est antérieur au niveau identifié dans la stratégie de conformité de microprogramme, le nœud de traitement est marqué comme non compatible.
  - **Marquer si pas de correspondance exacte**. Si le niveau de microprogramme installé sur un appareil ne correspond pas exactement à la stratégie de conformité de microprogramme, l'appareil est marqué comme non compatible. Par exemple, si vous remplacez une carte réseau dans un nœud de traitement et que le microprogramme sur cette carte réseau est différent du niveau identifié dans la stratégie de conformité de microprogramme, le nœud de traitement est marqué comme non compatible.
  - **Aucun indicateur**. Les appareils non compatibles ne sont pas marqués.

4. **Facultatif :** Développez le type de système pour afficher chaque mise à jour du module et sélectionnez le niveau de microprogramme à utiliser en tant que cible de conformité ou sélectionnez « Ne pas mettre à jour » pour empêcher la mise à jour du microprogramme sur cet appareil.
5. Cliquez sur **Créer**.

   La stratégie de conformité de microprogramme est indiquée dans le tableau sur la page Mises à jour de microprogramme : Stratégie de conformité. Le tableau affiche l'état d'utilisation, l'origine de la stratégie (définie par l'utilisateur ou prédéfinie) et la dernière date de modification.

Etape 3. Dans la barre de menus XClarity Administrator, cliquez sur **Distribution → Mises à jour de microprogramme : Appliquer/Activer**. La page Mises à jour de microprogramme : Appliquer/Activer présentant une liste d'appareils gérés s'affiche.

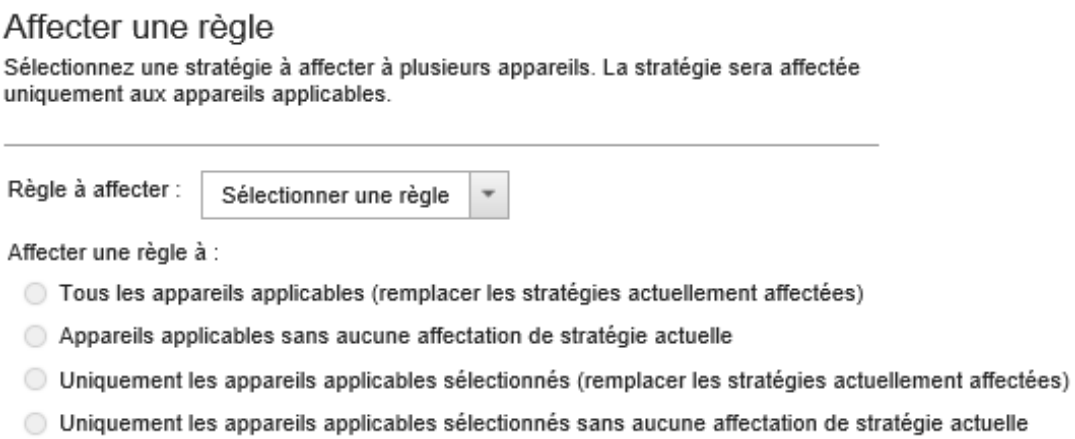
Etape 4. Affecter la stratégie de conformité-microprogramme aux appareils.

- **Pour un seul appareil**

  Pour chaque appareil, sélectionnez une stratégie dans le menu déroulant de la colonne **Stratégie de conformité affectée**.

Vous pouvez effectuer une sélection dans la liste des stratégies de conformité-microprogramme applicables à chaque appareil. Si aucune stratégie n'est affectée à l'appareil, la stratégie affectée est définie sur **Aucune affectation**. Si aucune stratégie ne s'applique à l'appareil, la stratégie affectée est définie sur **Aucune stratégie applicable**.

- **Pour plusieurs appareils**
  1. **Facultatif :** Sélectionnez un ou plusieurs appareils auxquels vous souhaitez affecter une stratégie de conformité de microprogramme.
  2. Cliquez sur l'icône **Affecter une stratégie** ( ) pour afficher la boîte de dialogue Affecter une stratégie.



  3. Sélectionnez une stratégie de conformité de microprogramme dans le menu déroulant **Stratégie à affecter**.

     Vous pouvez effectuer une sélection dans la liste des stratégies de conformité de microprogramme applicables à tous les appareils sélectionnés. Si les appareils n'ont pas été sélectionnés avant l'ouverture de la boîte de dialogue, toutes les stratégies sont répertoriées.

     Pour annuler l'affectation d'une stratégie, sélectionnez **Aucune affectation**.
  4. Sélectionnez l'une des portées suivantes pour l'affectation de stratégie.
     - **Tous les appareils applicables qui sont...**
     - **Uniquement les appareils appropriés sélectionnés qui sont...**
  5. Sélectionnez au moins un critère d'appareil.
     - **Sans stratégie affectée**
     - **Non conforme (remplacer la stratégie affectée actuelle)**
     - **Conforme (remplacer la stratégie affectée actuelle)**
     - **Non surveillé (remplacer la stratégie affectée actuelle)**
     - **Autre (remplacer la stratégie affectée actuelle)**. Cela s'applique aux appareils d'autres états, par exemple, En attente, avec des données manquantes ou non pris en charge en vue des mises à jour. Survolez l'icône d'aide ( ) pour afficher la liste des appareils applicables.

     Remarque : Les critères **Non surveillé** et **Autre** sont répertoriés uniquement lorsque des appareils sont dans ces états.
  6. Cliquez sur **OK**.

La stratégie indiquée dans la colonne **Stratégie affectée** sur la page Mises à jour de microprogramme : référentiel prend le nom de la stratégie de conformité de microprogramme sélectionnée.

Après avoir terminé

Après avoir créé une stratégie de conformité de microprogramme, vous effectuez les actions suivantes sur une stratégie de conformité de microprogramme sélectionnée :

- Afficher les détails de stratégie, y compris une liste des appareils affectés, en cliquant sur le nom de stratégie dans le tableau.
- Créer un doublon d'une stratégie de conformité sélectionnée en cliquant sur l'icône **Copier** ( ).
- Renommer ou Modifier une stratégie sélectionnée en cliquant sur l'icône **Éditer** ( ).Vous ne pouvez pas éditer une stratégie de conformité-microprogramme prédéfinie ou une stratégie qui est affectée à un appareil géré.

  Si vous modifiez une stratégie affectée de telle sorte qu'elle ne s'applique plus à certains appareils affectés, elle ne sera automatiquement plus assignée à ces appareils.

  Vous ne pouvez pas renommer ou modifier la stratégie **microprogramme la plus récente** prédéfinie.
- Supprimez une stratégie de conformité du microprogramme sélectionnée en cliquant sur l'icône **Supprimer la stratégie** ( ) ou supprimez la stratégie de conformité du microprogramme sélectionnée et toutes les mises à jour du microprogramme associées qui sont utilisées uniquement par cette stratégie en cliquant sur l'icône **Supprimer tous les modules de microprogramme et toutes les stratégies** ( ). Vous pouvez décider de supprimer la stratégie, et ce, même si elle est attribuée à un appareil.

  Si vous supprimez une stratégie qui est affectée à un appareil, elle est désaffectée avant d'être supprimée.

  Vous ne pouvez pas supprimer la **Dernière stratégie de microprogramme** prédéfinie ; toutefois, vous pouvez désactiver la stratégie en cliquant sur l'icône **Paramètres globaux** ( ), puis en sélectionnant **Désactiver la dernière stratégie de microprogramme**. Lorsque cette option est sélectionnée, la dernière stratégie de microprogramme est désaffectée des appareils gérés. La stratégie n'est plus mise à jour pour inclure les dernières versions de microprogramme disponibles dans le référentiel.
- Exporter une stratégie sélectionnée sur un système local en sélectionnant les stratégies et en cliquant sur **l'icône** Exporter . Vous pouvez ensuite importer la stratégie dans une autre instance de XClarity Administrator en cliquant sur l'icône **Importer** ( ).

Après avoir créé une stratégie de conformité de microprogramme, vous pouvez l'affecter à un appareil spécifique (voir Création et affectation de stratégies de conformité de microprogramme) et appliquer et activer les mises à jour pour cet appareil (voir Application et activation des mises à jour de microprogramme).

Identification des appareils non compatibles

Si une stratégie de conformité de microprogramme a été affectée à un appareil géré, vous pouvez déterminer si le microprogramme sur cet appareil est conforme à cette stratégie.

Procédure

Pour déterminer si le microprogramme d'un appareil est conforme à la stratégie de conformité de microprogramme qui lui a été affectée, cliquez sur **Distribution → Mises à jour de microprogramme : Appliquer/Activer** depuis la barre de menu Lenovo XClarity Administrator afin d'afficher la page Mise à jour

de microprogramme : stratégie de conformité, puis consultez la colonne **Versions installées** pour cet appareil.

La colonne **Versions installées** contient l'une des valeurs suivantes :

- **Version de microprogramme**. La version de microprogramme installée sur l'appareil est conforme à la stratégie affectée.
- **Compatible**. La version de microprogramme installée sur l'appareil est conforme à la stratégie affectée.
- **Non compatible**. La version de microprogramme installée sur l'appareil n'est pas conforme à la stratégie affectée.
- **Aucune stratégie de conformité définie**. Aucune stratégie de conformité de microprogramme n'est affectée à l'appareil.

Vous pouvez cliquer sur l'icône **Actualiser** ( ) pour actualiser le contenu de la colonne **Version installée**.

Configuration des paramètres globaux à jour de microprogramme

Les paramètres globaux sont utilisés en tant que paramètres de valeurs par défaut lorsque des mises à jour de microprogramme sont appliquées.

À propos de cette tâche

La page Paramètres globaux vous permet de configurer les paramètres suivants :
- Support étendu pour les appareils de niveau précédent
- Alertes pour les appareils qui ne sont pas compatibles avec les stratégies affectées
- L'affectation automatique d'une stratégie de conformité du microprogramme à un appareil auquel aucune stratégie n'est affectée.
- État de non-conformité pour les appareils avec un composant de microprogramme qui n'a pas de cible associée dans la stratégie de conformité de microprogramme

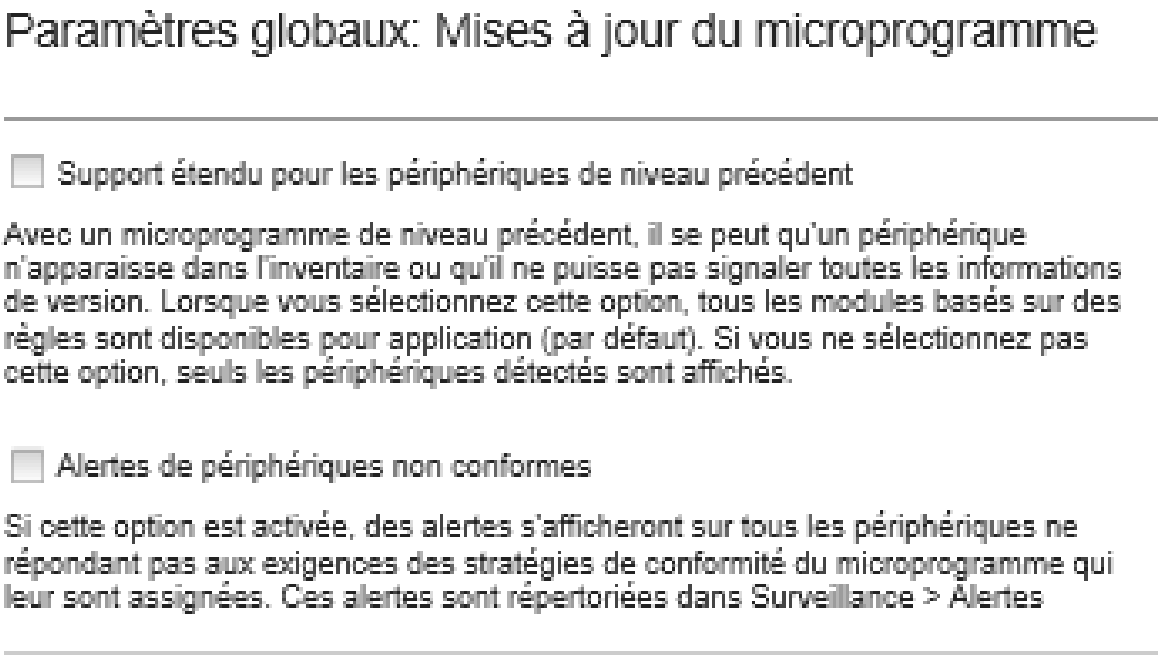
Procédure

Pour configurer les paramètres globaux à utiliser pour tous les serveurs, procédez comme suit.

Etape 1. Dans la barre de menus Lenovo XClarity Administrator, cliquez sur **Distribution → Mises à jour de microprogramme : Appliquer/Activer**. La page Mises à jour de microprogramme : Appliquer/Activer s'affiche.

Etape 2. Cliquez sur l'onglet **Mettre à jour avec stratégie** ou **Mettre à jour sans stratégie**.

Etape 3. Cliquez sur **Toutes les actions → Paramètres globaux** pour afficher la boîte de dialogue Paramètres globaux : Mises à jour du microprogramme.



Etape 4. Vous pouvez aussi sélectionner l'une des options suivantes.

- Sélectionnez **Support étendu pour les appareils de niveau précédent** pour afficher l'inventaire et les informations de version complète pour tous les appareils, même si le microprogramme est de niveau précédent ou qu'un appareil est absent de l'inventaire.
- Sélectionnez **Alertes pour les appareils non conformes** pour afficher les alertes sur la page Alertes des appareils qui ne répondent pas aux exigences des stratégies de conformité du microprogramme qui leur sont affectées. Par défaut, les alertes sont masquées sur la page Alertes. Pour plus d'informations, voir Affichage des alertes actives.
- Sélectionnez **Désactiver l'affectation de stratégie automatique** pour désactiver l'affectation automatique d'une stratégie de conformité du microprogramme à un appareil auquel aucune stratégie n'est affectée. Si cette option n'est pas sélectionnée, des stratégies de conformité de microprogramme sont affectées aux appareils sans stratégie lorsque XClarity Administrator est redémarré ou lorsque vous gérez un nouvel appareil.
- Sélectionnez **Rapporter une non conformité au microprogramme sans cible** pour marquer les appareils comme non compatibles lorsqu'un composant de microprogramme n'a pas de cible associée dans la stratégie de conformité du microprogramme. Si cette option n'est pas sélectionnée, les appareils sans cible sont marqués comme étant conformes.

Etape 5. Cliquez sur **OK** pour fermer la boîte de dialogue.

Application et activation des mises à jour de microprogramme

Lenovo XClarity Administrator n'applique pas automatiquement des mises à jour de microprogramme à des appareils gérés. Vous pouvez choisir d'appliquer des mises à jour de microprogramme avec ou sans stratégies de conformité.

Avant de commencer

Lorsque vous utilisez des stratégies de conformité, vous pouvez planifier des mises à jour sur plusieurs appareils en même temps. Les appareils sont automatiquement mis à jour selon la séquence appropriée par

XClarity Administrator. Le module CMM est mis à jour en premier, puis les commutateurs, les serveurs et les dispositifs de stockage.

Seules les mises à jour de microprogramme téléchargées peuvent être appliquées.

Lorsque vous effectuez une mise à jour de microprogramme, XClarity Administrator démarre un ou plusieurs travaux pour effectuer la mise à jour.

Pendant l'opération de mise à jour de microprogramme, l'appareil cible est verrouillé. Vous ne pouvez pas lancer d'autres tâches de gestion sur l'appareil cible tant que le processus de mise à jour n'est pas terminé.

Une fois qu'une mise à jour de microprogramme est appliquée à un appareil, un ou plusieurs redémarrages peuvent être requis pour activer complètement la mise à jour du microprogramme. Vous pouvez choisir de redémarrer l'appareil immédiatement, de différer l'activation ou hiérarchiser l'activation. Si vous choisissez de redémarrer l'appareil immédiatement, XClarity Administrator réduit le nombre de redémarrages requis. Si vous choisissez de différer l'activation, les mises à jour seront activées lorsque l'appareil sera redémarré. Si vous choisissez l'activation hiérarchisée, les mises à sont immédiatement activées sur le contrôleur de gestion de la carte mère et toutes les autres mises à jour de microprogramme sont activées au redémarrage suivant de l’appareil.

Vous pouvez mettre à jour certains microprogrammes sur un maximum de 50 appareils à la fois. Si vous choisissez de mettre à jour certains microprogrammes sur plus de 50 appareils, les autres appareils sont mis en file d’attente. Un appareil en file d’attente est retiré de la file d’attente « de mise à jour de certains microprogrammes » lorsque l’activation se termine sur un appareil mis à jour ou qu’un appareil mis à jour est placé dans le mode En attente de maintenance (si un redémarrage est requis sur cet appareil). Lorsqu’un appareil dans le mode En attente de maintenance est redémarré, l’appareil démarre en mode de maintenance et poursuit le processus de mise à jour, même si le nombre maximal de mises à jour de microprogramme est déjà en cours.

Vous pouvez mettre à jour le microprogramme en lot sur un maximum de 10 appareils à la fois. Si vous choisissez de mettre à jour le microprogramme en lot sur plus de 10 appareils, les autres appareils sont mis en file d’attente. Un appareil en file d’attente est retiré de la file d’attente de la « mise à jour du microprogramme en lot » lorsque l’activation se termine sur un appareil dont le microprogramme a été mis à jour en lot.

Attention : Pour Red Hat® Enterprise Linux (RHEL) versions 7 et suivantes, le redémarrage du système d'exploitation à partir d'un mode graphique interrompt le serveur par défaut. Avant d'effectuer les actions **Redémarrer normalement** ou **Redémarrer immédiatement** depuis XClarity Administrator, vous devez configurer manuellement le système d'exploitation afin de modifier le comportement du bouton d'alimentation pour la mise hors tension. Pour des instructions détaillées, voir Guide d'administration et de migration des données Red Hat : Modification du comportement lors de l'utilisation du bouton d'alimentation dans le mode cible graphique.

Remarque : XClarity Administrator active automatiquement l'interface LAN-over-USB.

Application des mises à jour du microprogramme en lot avec des stratégies de conformité

Dès que Lenovo XClarity Administrator identifie un appareil géré non conforme, vous pouvez appliquer une mise à jour du microprogramme manuelle à *tous* les composants de certains serveurs ThinkSystem SR635 et SR655 non conformes à la stratégie de conformité du microprogramme attribuée, avec une image de lot contenant les modules de mise à jour du microprogramme applicables. L’*image de lot* est créée lors du processus de mise à jour par collecte de tous les modules de mise à jour du microprogramme de la stratégie de conformité.

Avant de commencer

- Prenez connaissance des remarques relatives à la mise à jour de microprogramme avant de tenter de mettre à jour un microprogramme sur vos appareils gérés (voir Considérations relatives à la mise à jour du microprogramme).
- Initialement, les appareils qui ne sont pas pris en charge pour les mises à jour sont masqués dans la vue. Les appareils qui ne sont pas pris en charge ne peuvent pas être sélectionnés pour les mises à jour.
- Par défaut, tous les composants détectés sont répertoriés comme disponibles pour l'application des mises à jour ; toutefois, un microprogramme de niveau antérieur peut empêcher un composant d'apparaître dans l'inventaire ou d'afficher des informations de version complète. Pour répertorier tous les modules basés sur des stratégies vous permettant d'appliquer des mises à jour, cliquez sur **Toutes les actions → Paramètres globaux**, et sélectionnez **Support étendu pour les appareils de niveau précédent**. Lorsque cette option est sélectionnée, la mention « Autre logiciel disponible » apparaît dans la colonne Version installée pour les appareils non détectés. Pour plus d'informations, voir Configuration des paramètres globaux à jour de microprogramme.

  Remarques :

  – Les paramètres globaux ne peuvent pas être modifiés lorsque des mises à jour sont en cours sur des appareils gérés.

  – La génération d'options supplémentaires peut nécessiter quelques minutes. Au bout de quelques instants, il vous faudra peut-être cliquer sur l'icône **Actualiser** () afin d'actualiser le tableau.
- Assurez-vous qu'aucun travail n'est en cours d'exécution sur le serveur cible. Si des travaux sont en cours exécution, le travail de mise à jour est placé en file d'attente jusqu'à ce que tous les autres travaux soient terminés. Pour afficher la liste des travaux actifs, cliquez sur **Surveillance → Travaux**.
- L'application des mises à jour du microprogramme en lot n'est prise en charge que pour les serveurs ThinkSystem SR635 et SR655.
- L'application des mises à jour de microprogramme groupées n'est prise en charge que pour l'adresse IPv4. Les adresses IPv6 ne sont pas prises en charge.
- Vous devez vous assurer que chaque appareil cible a été amorcé sur le SE au moins une fois afin de récupérer toutes les informations de l'inventaire.
- Le microprogramme v2.94 ou ultérieure du contrôleur de gestion de la carte mère est requis pour utiliser la fonction de mise à jour en lot.
- Seules les mises à jour du microprogramme obtenues à partir de modules de référentiel ou les mises à jour du microprogramme individuelles sont utilisées. Les UpdateXpress System Packs (UXSP) ne sont pas pris en charge.
- Seules les mises à jour de microprogramme téléchargées sont appliquées. Actualisez le catalogue produit et téléchargez les mises à jour de microprogramme appropriées (voir Actualisation du catalogue produit et Téléchargement des mises à jour de microprogramme).

  Remarque : À l'origine, lorsque XClarity Administrator est installé, le catalogue produit et le référentiel sont vides.
- Pour les serveurs ThinkSystem SR635 et SR655, la vérification de conformité n'est prise en charge que pour le contrôleur de gestion de la carte mère et UEFI. Cependant, XClarity Administrator essaie d'appliquer des mises à jour du microprogramme à tous les composants matériels disponibles.
- Les mises à jour sont appliquées en fonction de la stratégie de conformité du microprogramme attribuée. Vous ne pouvez pas décider de mettre à jour un sous-ensemble de composants.
- XClarity Administrator v3.2 ou ultérieure est nécessaire pour appliquer des mises à jour du microprogramme pour Lenovo XClarity Provisioning Manager (LXPM), les pilotes Windows LXPM, ou bien les pilotes Linux LXPM aux serveurs ThinkSystem SR635 et SR655.
- Si la version installée est supérieure à la stratégie de conformité attribuée, alors les mises à jour du contrôleur de gestion de la carte mère et UEFI sont ignorées.

- Des stratégies de conformité de microprogramme doivent être créées et affectées aux appareils sur lesquels vous souhaitez appliquer des mises à jour de microprogramme. Pour plus d'informations, voir Création et affectation de stratégies de conformité de microprogramme.
- Avant de démarrer le processus de mise à jour, les appareils sélectionnés doivent être mis hors tension. Assurez-vous que les charges de travail en cours d'exécution sont arrêtées ou, si vous travaillez dans un environnement virtualisé, vérifiez qu'elles ont été déplacées vers un autre serveur.

Attention : Avant de démarrer le processus de mise à jour, les appareils sélectionnés sont mis hors tension. Assurez-vous que les charges de travail en cours d'exécution sont arrêtées ou, si vous travaillez dans un environnement virtualisé, vérifiez qu'elles ont été déplacées vers un autre serveur. Si des travaux sont en cours exécution, le travail de mise à jour est placé en file d'attente jusqu'à ce que tous les autres travaux soient terminés. Pour afficher la liste des travaux actifs, cliquez sur **Surveillance → Travaux**.

À propos de cette tâche

Le processus de mise à jour en lot met tout d'abord à jour le contrôleur de gestion de la carte mère, puis l'UEFI hors bande. Une fois ces mises à jour terminées, en fonction du type de machine, le processus crée une image de lot du microprogramme restant dans la stratégie de conformité. Ensuite, le processus monte l'image sur l'appareil sélectionné, puis le redémarre afin d'amorcer l'image. L'image s'exécute automatiquement en vue d'effectuer les mises à jour restantes.

Vous pouvez mettre à jour le microprogramme en lot sur un maximum de 10 appareils à la fois. Si vous choisissez de mettre à jour le microprogramme en lot sur plus de 10 appareils, les autres appareils sont mis en file d'attente. Un appareil en file d'attente est retiré de la file d'attente de la « mise à jour du microprogramme en lot » lorsque l'activation se termine sur un appareil dont le microprogramme a été mis à jour en lot.

Si une erreur se produit lors de la mise à jour d'un composant de l'appareil, le processus de mise à jour de microprogramme ne met pas à jour le microprogramme du composant concerné ; toutefois, le processus de mise à jour de microprogramme continue de mettre à jour les autres composants de l'appareil et de mettre à jour tous les autres appareils du travail de mise à jour de microprogramme en cours.

Procédure

Pour appliquer les mises à jour du microprogramme sous la forme d'une image de lot sur des appareils gérés, procédez comme suit.

Etape 1. Dans la barre de menus XClarity Administrator, cliquez sur **Distribution → Mises à jour de microprogramme : Appliquer/Activer**. La page Mises à jour de microprogramme : Appliquer/Activer s'affiche.

Etape 2. Cliquez sur l'onglet **Mettre à jour avec stratégie**.

Etape 3. Sélectionnez un ou plusieurs appareils et composants auxquels des mises à jour de microprogramme doivent être appliquées.

Vous pouvez trier les colonnes du tableau afin de faciliter la recherche de dispositifs spécifiques. En outre, vous pouvez filtrer la liste des appareils affichés en sélectionnant une option dans le menu **Afficher** pour afficher uniquement la liste des appareils dans un châssis, armoire ou groupe spécifique, en entrant du texte (par exemple, un nom ou une adresse IP) dans la zone **Filtre** ou en cliquant sur les icônes suivantes pour afficher uniquement les appareils avec un état spécifique.

- Icône **Masquer les appareils non conformes** ()
- Icône **Masquer les appareils non conformes** ()
- Icône **Masquer les appareils auxquels aucune stratégie de conformité n'est affectée** ()

- Icône **Masquer les appareils non surveillés** ( )
- Icône **Masquer les appareils avec activation en attente du microprogramme** ( )
- Icône **Masquer les appareils avec des erreurs de conformité** ( )
- Icône **Masquer les appareils non pris en charge pour les mises à jour** ( )
- Icône **Masquer les appareils avec des mises à jour de microprogramme en cours** ( )
- Icône **Masquer les appareils avec microprogramme non indexable** ( )

La colonne **Groupes** indique les groupes dont chaque appareil est membre. Vous pouvez survoler la colonne **Groupes** pour obtenir une liste complète des groupes, par type de groupe

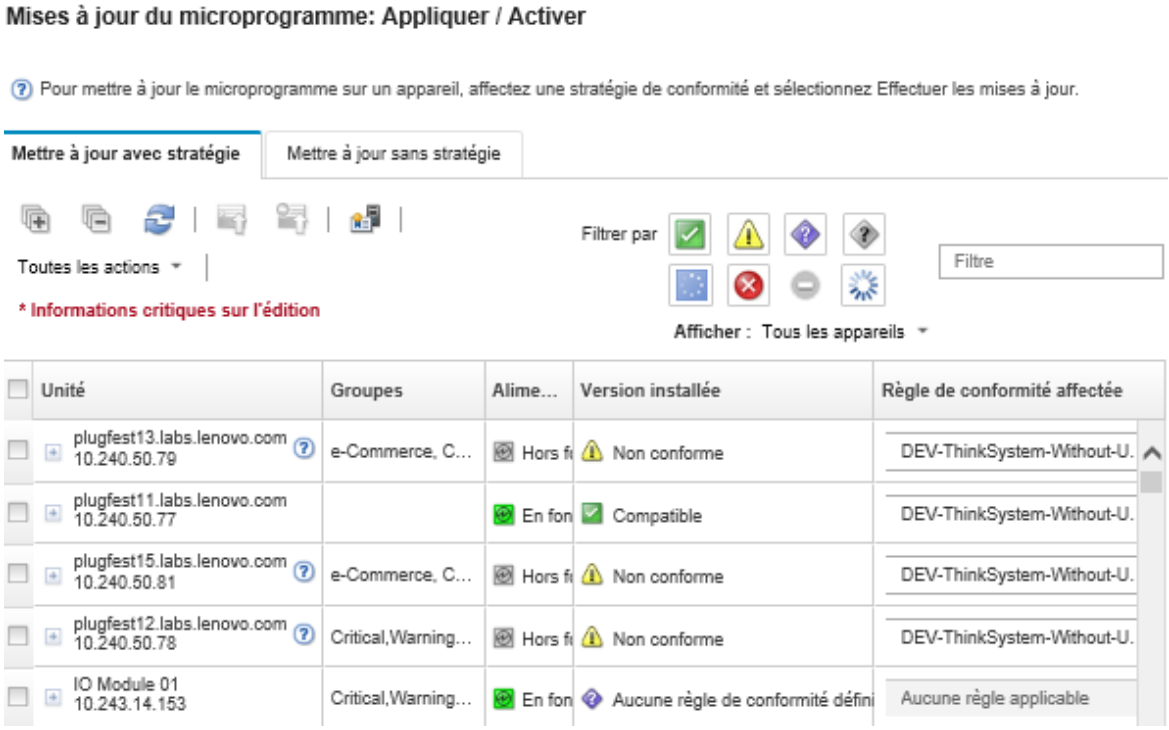
La colonne **Version installée** indique la version de microprogramme installée, l'état de conformité ou l'état de l'appareil.

L'état de conformité peut être l'un des suivants :

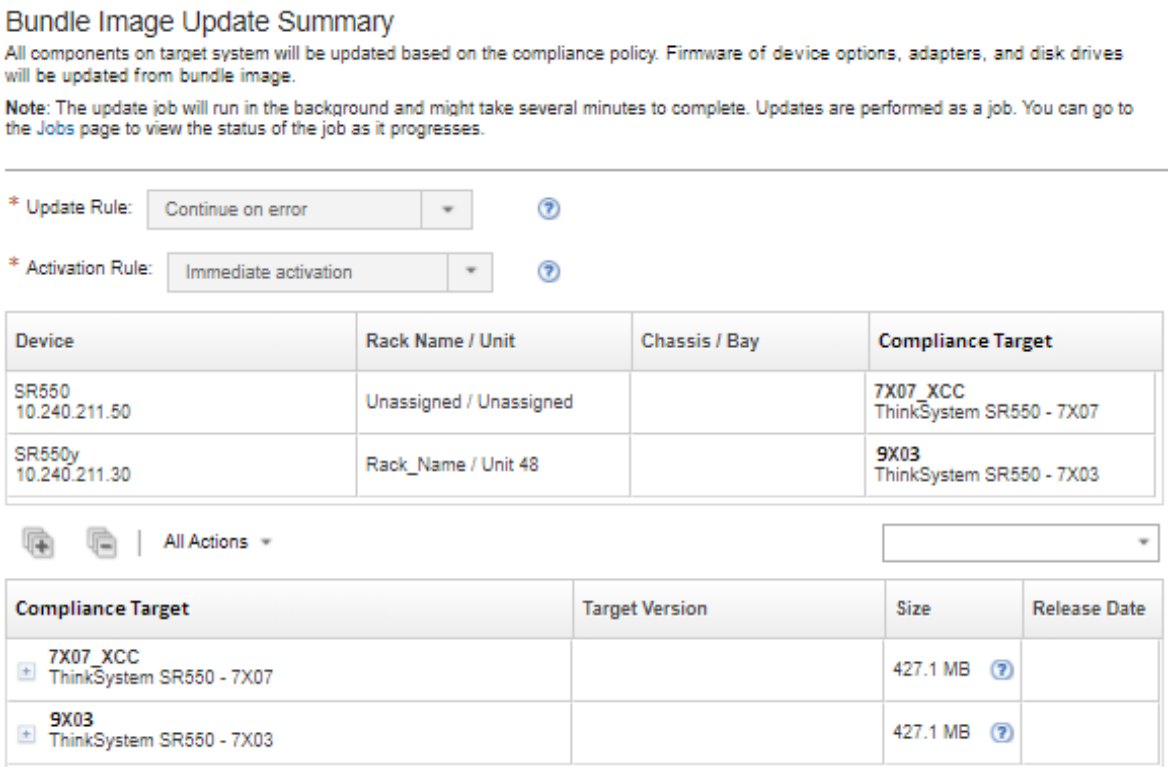
- **Conforme**
- **Erreur de conformité**
- **Non compatible**
- **Aucune stratégie de conformité définie**
- **Non surveillé**

L'état de l'appareil peut être l'un des suivants :

- **Mises à jour non prises en charge**
- **Mise à jour en cours**



Etape 4. Cliquez sur l'icône **Effectuer une mise à jour à partir d'une image de lot** ( ). La boîte de dialogue Récapitulatif des mises à jour d'image de lot s'affiche. Cette boîte de dialogue énumère les appareils concernés, ainsi que les mises à jour du microprogramme incluses dans l'image de lot.



Etape 5. Cliquez sur **Effectuer les mises à jour à partir d'une image de lot** pour mettre à jour immédiatement, ou cliquez sur **Planning** pour planifier cette mise à jour en vue d'une exécution ultérieure.

Après avoir terminé

Lors de l'application d'une mise à jour de microprogramme, si le serveur ne passe pas en mode de maintenance, essayez à nouveau d'appliquer la mise à jour.

Si des mises à jour n'ont pas abouti, voir Problème de mise à jour et de référentiel de microprogramme dans la documentation en ligne de XClarity Administrator pour savoir comment identifier et résoudre les problèmes.

Depuis la page Mises à jour de microprogramme : Appliquer/Activer, vous pouvez effectuer les actions suivantes.

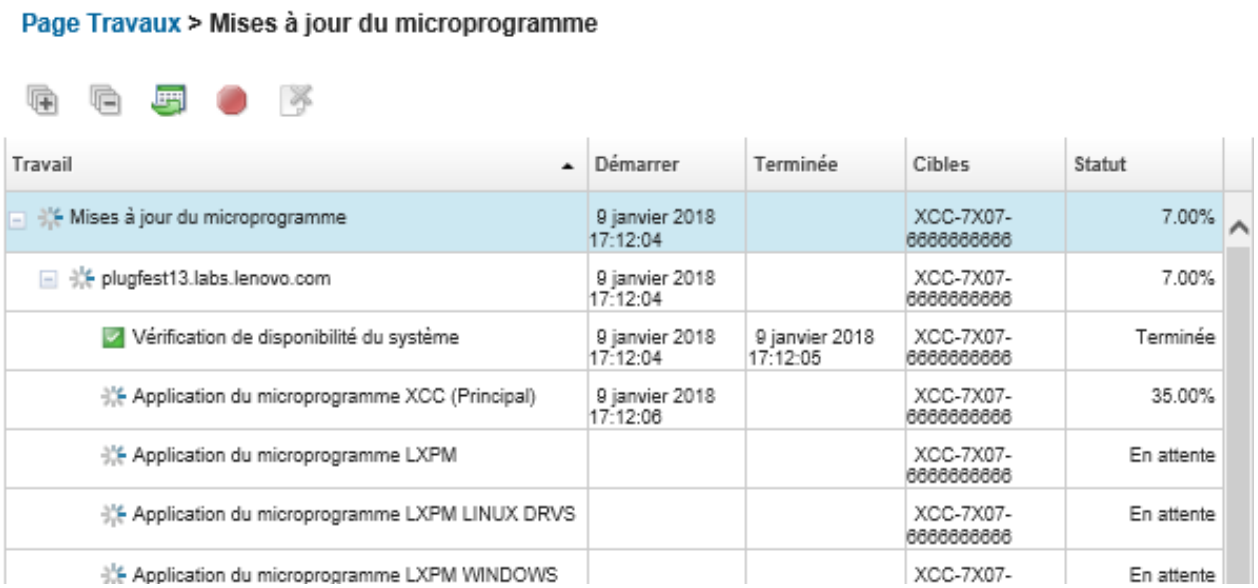
- Exporter les informations sur le microprogramme et la conformité pour chaque appareil géré en cliquant sur **Toutes les actions → Export View as CSV**.

  Remarque : Le fichier CSV contient uniquement les informations filtrées dans la vue en cours. Les informations qui sont filtrées en dehors de la vue et les information dans les colonnes masquées ne sont pas incluses.
- Annuler une mise à jour en cours d'application sur un appareil en sélectionnant celui-ci et en cliquant sur l'icône **Annuler la mise à jour** ( ).

Remarque : Vous pouvez annuler les mises à jour de microprogramme qui se trouvent dans la file d'attente de démarrage. Après le démarrage du processus de mise à jour, la mise à jour de microprogramme peut être annulée uniquement lorsque le processus de mise à jour exécute une tâche autre que l'application de la mise à jour, par exemple, le passage en mode de maintenance ou le redémarrage de l'appareil.

- Visualiser l'état de la mise à jour de microprogramme directement à partir de la page Appliquer/Activer dans la colonne **État**.
- Surveiller l'état du processus de mise à jour en consultant le journal des travaux. Dans le menu Lenovo XClarity Administrator, cliquez sur **Surveillance → Travaux**.

  Pour plus d'informations sur le journal des travaux, voir Surveillance des travaux.



Lorsque les travaux de mise à jour de microprogramme sont terminés, vous pouvez vérifier que les appareils sont conformes en cliquant sur **Distribution → Mises à jour de microprogramme : Appliquer/Activer** pour revenir à la page Mises à jour de microprogramme : Appliquer/Activer, puis en cliquant sur l'icône **Actualiser** ( ). La version de microprogramme active sur chaque appareil est répertoriée dans la colonne **Version installée**.

Application de certaines mises à jour de microprogramme avec des stratégies de conformité

Lorsque Lenovo XClarity Administrator identifie un appareil comme non compatible, vous pouvez appliquer et activer manuellement les mises à jour de microprogramme sur cet appareil géré. Vous pouvez choisir d'appliquer et activer toutes les mises à jour de microprogramme applicables à une stratégie de conformité de microprogramme ou uniquement certaines mises à jour de microprogramme d'une stratégie. Seules les mises à jour de microprogramme téléchargées sont appliquées.

En savoir plus :

- XClarity Administrator : amélioration de l'efficacité lors de la mise à jour du microprogramme
- Meilleures pratiques concernant la mise à jour du microprogrammes et des pilotes Lenovo ThinkSystem
- XClarity Administrator : du serveur au cluster
- XClarity Administrator : mises à jour de microprogramme
- XClarity Administrator : Distribution des mises à jour de sécurité du microprogramme

Avant de commencer

- Prenez connaissance des remarques relatives à la mise à jour de microprogramme avant de tenter de mettre à jour un microprogramme sur vos appareils gérés (voir Considérations relatives à la mise à jour du microprogramme).
- Initialement, les appareils qui ne sont pas pris en charge pour les mises à jour sont masqués dans la vue. Les appareils qui ne sont pas pris en charge ne peuvent pas être sélectionnés pour les mises à jour.
- Par défaut, tous les composants détectés sont répertoriés comme disponibles pour l'application des mises à jour ; toutefois, un microprogramme de niveau antérieur peut empêcher un composant d'apparaître dans l'inventaire ou d'afficher des informations de version complète. Pour répertorier tous les modules basés sur des stratégies vous permettant d'appliquer des mises à jour, cliquez sur **Toutes les actions → Paramètres globaux**, et sélectionnez **Support étendu pour les appareils de niveau précédent**. Lorsque cette option est sélectionnée, la mention « Autre logiciel disponible » apparaît dans la colonne Version installée pour les appareils non détectés. Pour plus d'informations, voir Configuration des paramètres globaux à jour de microprogramme.

  Remarques :

  – Les paramètres globaux ne peuvent pas être modifiés lorsque des mises à jour sont en cours sur des appareils gérés.

  – La génération d'options supplémentaires peut nécessiter quelques minutes. Au bout de quelques instants, il vous faudra peut-être cliquer sur l'icône **Actualiser** () afin d'actualiser le tableau.
- Assurez-vous qu'aucun travail n'est en cours d'exécution sur le serveur cible. Si des travaux sont en cours exécution, le travail de mise à jour est placé en file d'attente jusqu'à ce que tous les autres travaux soient terminés. Pour afficher la liste des travaux actifs, cliquez sur **Surveillance → Travaux**.
- Assurez-vous que le référentiel des mises à jour de microprogramme contient les modules de microprogramme que vous souhaitez déployer. Si tel n'est pas le cas, actualisez le catalogue produit et téléchargez les mises à jour de microprogramme appropriées (voir Actualisation du catalogue produit et Téléchargement des mises à jour de microprogramme).

  Remarque : À l'origine, lorsque XClarity Administrator est installé, le catalogue produit et le référentiel sont vides.

  Si vous prévoyez d'installer un microprogramme prérequis, vérifiez que ce dernier a bien été téléchargé dans le référentiel.

  Dans certains cas, plusieurs versions peuvent être nécessaires afin de mettre à jour le microprogramme, et toutes devront être téléchargées vers le référentiel. Par exemple, pour effectuer la mise à niveau du commutateur évolutif IBM FC5022 SAN de la version v7.4.0a vers v8.2.0a, vous devez installer v8.0.1-pha, puis v8.1.1, et enfin v8.2.0a. Ces trois versions peuvent se trouver dans le référentiel afin de mettre à jour le commutateur vers v8.2.0a.
- En général, les appareils doivent être redémarrés pour que la mise à jour de microprogramme soit activée. Si vous décidez de redémarrer l'appareil lors du processus de mise à jour (*activation immédiate*), vérifiez que les charges de travail en cours d'exécution ont été arrêtées ou, si vous travaillez dans un environnement virtualisé, assurez-vous qu'elles ont été déplacées vers un autre serveur.
- Pour les serveurs ThinkSystem SR635 et SR655, vous pouvez suivre la procédure de mise à jour classique afin d'appliquer uniquement les mises à jour du microprogramme UEFI et du contrôleur de gestion de la carte mère. La version AMBT10M ou ultérieure du microprogramme du contrôleur de gestion est requise, de même que la version CFE114L ou ultérieure du microprogramme UEFI. Utilisez la fonction de mise à jour en lot pour mettre à jour tous les composants (dont le contrôleur de gestion, UEFI, les unités de disque et les options d'E-S) (voir Application des mises à jour du microprogramme en lot avec des stratégies de conformité).

À propos de cette tâche

- Vous pouvez mettre à jour certains microprogrammes sur un maximum de 50 appareils à la fois. Si vous choisissez de mettre à jour certains microprogrammes sur plus de 50 appareils, les autres appareils sont mis en file d'attente. Un appareil en file d'attente est retiré de la file d'attente « de mise à jour de certains microprogrammes » lorsque l'activation se termine sur un appareil mis à jour ou qu'un appareil mis à jour est placé dans le mode En attente de maintenance (si un redémarrage est requis sur cet appareil). Lorsqu'un appareil dans le mode En attente de maintenance est redémarré, l'appareil démarre en mode de maintenance et poursuit le processus de mise à jour, même si le nombre maximal de mises à jour de microprogramme est déjà en cours.
- Vous pouvez appliquer et activer un microprogramme qui est postérieur au microprogramme actuellement installé.
- Vous pouvez choisir d'appliquer toutes les mises à jour pour un appareil spécifique. Cependant, vous pouvez aussi choisir de développer un appareil afin de spécifier des mises à jour pour un composant spécifique, par exemple, le contrôleur de gestion de la carte mère ou UEFI.
- Si vous choisissez d'installer un module de mise à jour de microprogramme contenant les mises à jour de plusieurs composants, tous les composants auxquels le module de mise à jour s'applique sont mis à jour.

Procédure

Pour appliquer et activer des mises à jour sur des appareils gérés, procédez comme suit.

Etape 1. Dans la barre de menus XClarity Administrator, cliquez sur **Distribution → Mises à jour de microprogramme : Appliquer/Activer**. La page Mises à jour de microprogramme : Appliquer/Activer s'affiche.

Etape 2. Cliquez sur l'onglet **Mettre à jour avec stratégie**.

Etape 3. Sélectionnez un ou plusieurs appareils et dispositifs auxquels des mises à jour de microprogramme doivent être appliquées.

Vous pouvez trier les colonnes du tableau afin de faciliter la recherche de serveurs spécifiques. En outre, vous pouvez filtrer la liste des appareils affichés en sélectionnant une option dans le menu **Afficher** pour afficher uniquement la liste des appareils dans un châssis, armoire ou groupe spécifique, en entrant du texte (par exemple, un nom ou une adresse IP) dans la zone **Filtre** ou en cliquant sur les icônes suivantes pour afficher uniquement les appareils avec un état spécifique.

- Icône **Masquer les appareils non conformes** ()
- Icône **Masquer les appareils non conformes** ()
- Icône **Masquer les appareils auxquels aucune stratégie de conformité n'est affectée** ()
- Icône **Masquer les appareils non surveillés** ()
- Icône **Masquer les appareils avec activation en attente du microprogramme** ()
- Icône **Masquer les appareils avec des erreurs de conformité** ()
- Icône **Masquer les appareils non pris en charge pour les mises à jour** ()
- Icône **Masquer les appareils avec des mises à jour de microprogramme en cours** ()
- Icône **Masquer les appareils avec microprogramme non indexable** ()

La colonne **Groupes** indique les groupes dont chaque appareil est membre. Vous pouvez survoler la colonne **Groupes** pour obtenir une liste complète des groupes, par type de groupe

La colonne **Version installée** indique la version de microprogramme installée, l'état de conformité ou l'état de l'appareil.

L'état de conformité peut être l'un des suivants :

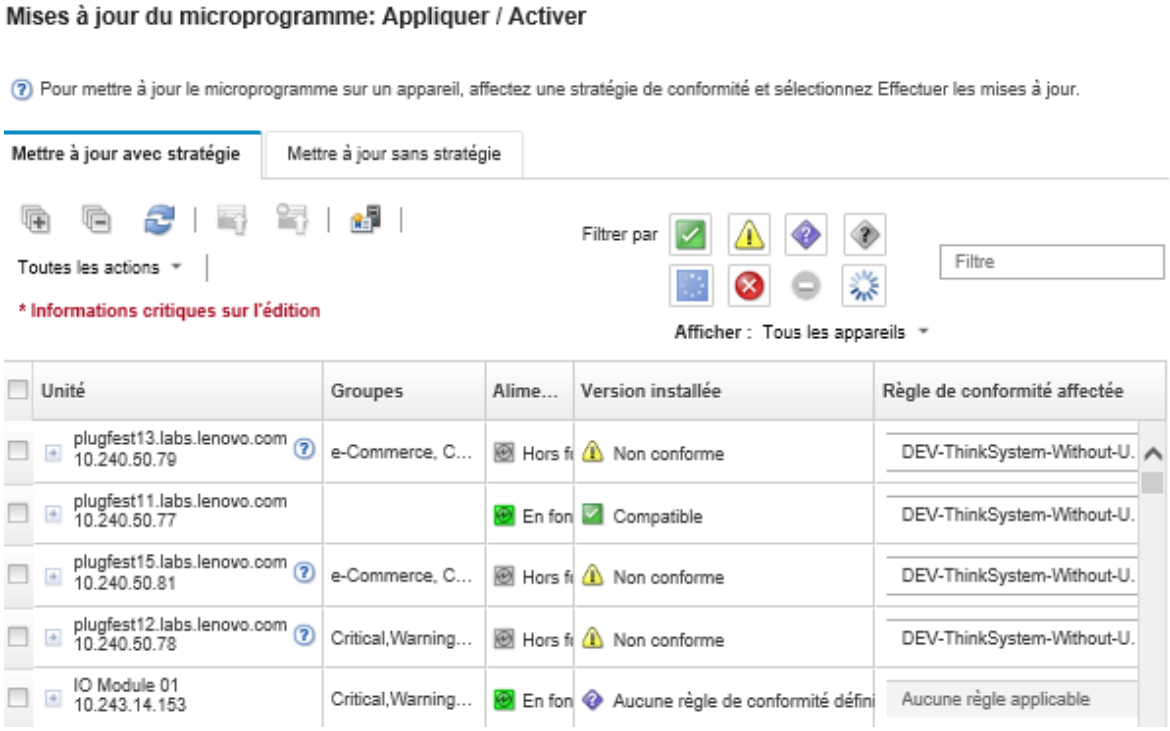
- **Conforme**
- **Erreur de conformité**
- **Non compatible**
- **Aucune stratégie de conformité définie**
- **Non surveillé**

L'état de l'appareil peut être l'un des suivants :

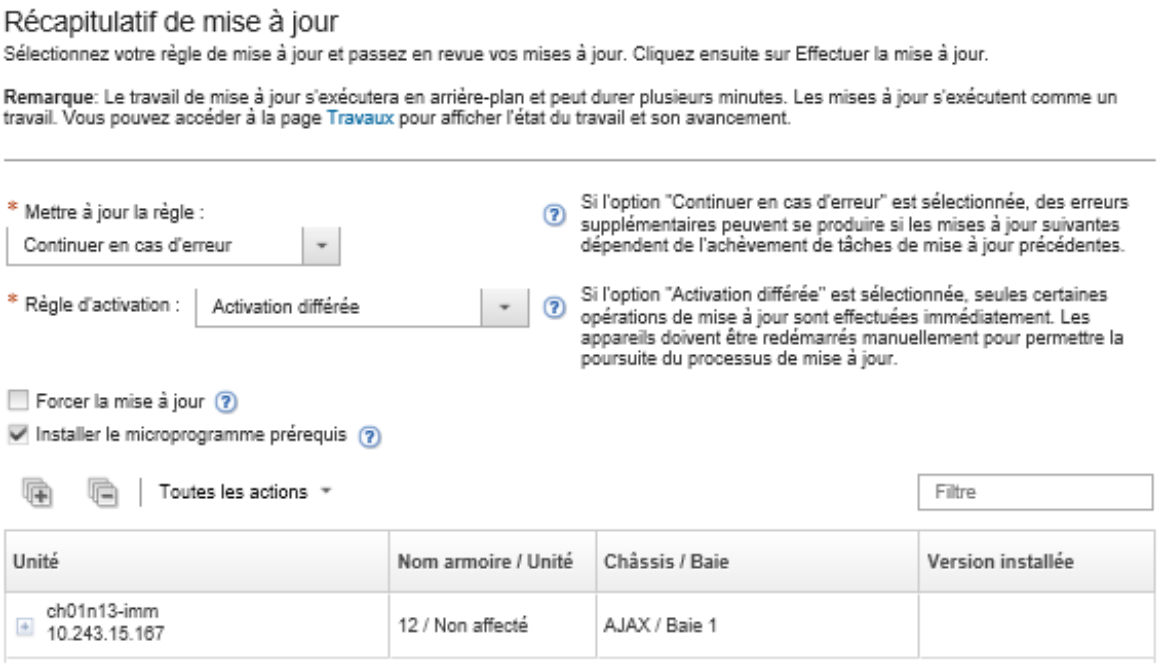
- **Mises à jour non prises en charge**
- **Mise à jour en cours**

Remarques : Si la version de microprogramme installée est en attente d'activation, « (Activation en attente) » est ajouté à la version de microprogramme installée et l'état de conformité de chaque appareil applicable, par exemple « 2.20 / A9E12EUS (Activation en attente). » Pour afficher l'état d'activation en attente, la version de microprogramme suivante doit être installée sur le contrôleur de gestion de la carte mère principal dans le serveur.

- **IMM2** : TCOO46F, TCOO46E ou version ultérieure (selon la plateforme)
- **XCC** : CDI328M, PSI316N, TEI334I ou version ultérieure (selon la plateforme)



Etape 4. Cliquez sur l'icône **Effectuer les mises à jour** ( ). La boîte de dialogue Récapitulatif des mises à jour s'affiche.



Etape 5. Sélectionnez l'une des règles de mise à jour

- **Arrêter toutes les mises à jour en cas d'erreur**. Si une erreur se produit lors de la mise à jour de l'un des composants (par exemple, un adaptateur ou un contrôleur de gestion) sur l'appareil cible, le processus de mise à jour de microprogramme s'arrête pour tous les appareils sélectionnés dans le travail de mise à jour de microprogramme en cours. Dans ce cas, aucune des mises à jour du module de mise à jour pour l'appareil n'est appliquée. Le microprogramme actuellement installé sur tous les systèmes sélectionnés reste en vigueur.
- **Continuer en cas d'erreur**. Si une erreur se produit lors de la mise à jour de l'un des dispositifs de l'appareil, le processus de mise à jour de microprogramme ne met pas à jour le microprogramme de l'appareil concerné ; toutefois, le processus de mise à jour de microprogramme continue de mettre à jour les autres dispositifs de l'appareil et de mettre à jour tous les autres appareils du travail de mise à jour de microprogramme en cours.
- **Passer au système suivant en cas d'erreur**. Si une erreur se produit lors de la mise à jour de l'un des dispositifs de l'appareil, le processus de mise à jour de microprogramme arrête toutes les tentatives de mise à jour de microprogramme pour cet appareil spécifique, de sorte que le microprogramme actuellement installé sur celui-ci reste en vigueur. Le processus de mise à jour de microprogramme continue de mettre à jour tous les autres appareils du travail de mise à jour de microprogramme en cours.

Etape 6. Sélectionnez l'une des règles d'activation :

- **Activation immédiate**. Au cours du processus de mise à jour, il est possible que l'appareil redémarre automatiquement plusieurs fois jusqu'à la fin du processus de mise à jour. Avant de continuer, prenez soin de mettre au repos toutes les applications sur l'appareil.
- **Activation différée**. Seules certaines opérations de mise à jour sont effectuées. Les appareils doivent être redémarrés pour permettre la poursuite du processus de mise à jour. Des redémarrages supplémentaires sont ensuite effectués jusqu'à l'achèvement de l'opération de mise à jour.

  Un événement est déclenché lorsque l'état passe en **mode de maintenance du microprogramme en attente** pour vous avertir du redémarrage du serveur.

  Si un appareil redémarre pour une raison quelconque, le processus de mise à jour différé se termine.

Cette règle d'activation est prise en charge uniquement pour les serveurs et les commutateurs de type armoire. Les modules CMM et les commutateurs Flex sont activés immédiatement, quelle que soit la valeur affectée à ce paramètre.

Un événement est déclenché lorsque l'état passe en **mode de maintenance du microprogramme en attente** pour vous avertir du redémarrage du serveur.

Le processus de mise à jour différée s'achève lorsque l'appareil est redémarré pour une raison quelconque (y compris un redémarrage manuel). Il n'y a pas de limite de temps imposée au redémarrage du serveur.

XClarity Administrator peut appliquer des mises à jour avec une activation différée sur 50 appareils simultanément au maximum. Si vous tentez d'appliquer des mises à jour avec une activation différée sur plus de 50 appareils, les appareils excédentaires seront mis en file d'attente. Un appareil sort de la file d'attente lorsqu'un appareil mis à jour passe à l'état **Mode de maintenance du microprogramme en attente.**

Important :

- Si XClarity Administrator est redémarré pendant la tâche de mise à jour, cette tâche s'arrêtera avec une erreur.
- Si un serveur se trouvant dans l'état **Mode de maintenance du microprogramme en attente** est redémarré alors que XClarity Administrator est à l'arrêt ou inaccessible, le serveur s'amorce sur la BMU, mais comme XClarity Administrator ne peut pas se connecter à la BMU et que le délai expire au bout de 60 secondes, le statut d'alimentation du système est rétabli par le contrôleur de gestion de la carte mère (arrête le système s'il était hors tension, le redémarre s'il était sous tension).

- **Activation hiérarchisée**. Les mises à jour du microprogramme sur le contrôleur de gestion de la carte mère sont activées immédiatement. toutes les autres mises à jour de microprogramme sont des mises à jour de microprogramme et sont activées au redémarrage suivant de l'appareil. Des redémarrages supplémentaires sont ensuite effectués jusqu'à l'achèvement de l'opération de mise à jour. Cette règle est prise en charge uniquement pour les serveurs.

  Un événement est déclenché lorsque l'état passe en mode de maintenance du microprogramme en attente pour vous avertir du redémarrage du serveur.

Remarque : Une fois activée, l'option d'amorçage Wake on LAN peut affecter les opérations XClarity Administrator qui mettent le serveur hors tension, notamment les mises à jour du microprogramme si votre réseau comprend un client Wake on LAN qui émet des commandes « Wake on Magic Packet ».

Etape 7. **Facultatif :** Sélectionnez **Forcer la mise à jour** pour mettre à jour le microprogramme sur les composants sélectionnés même si le niveau de microprogramme est à jour, ou pour appliquer une mise à jour du microprogramme antérieure à celle actuellement installée sur le composant sélectionné.

Remarque : Vous pouvez appliquer une version antérieure du microprogramme aux options d'appareils, d'adaptateurs et d'unités qui sont compatibles avec la rétromigration. Référez-vous à la documentation sur le matériel afin de déterminer si la rétromigration est bien prise en charge.

Etape 8. **Facultatif :** Désélectionnez **Installer le microprogramme requis** si vous ne souhaitez pas installer le microprogramme requis. Le microprogramme requis est installé par défaut.

Remarque : Lorsque vous utilisez **Activation différée** ou **Activation hiérarchisée** pour les mises à jour de microprogramme prérequises, vous devez redémarrer le serveur pour activer le microprogramme prérequis. Après le redémarrage initial, les mises à jour de microprogramme restantes sont installées à l'aide de **Activation immédiate**.

Etape 9. **Facultatif :** si vous avez sélectionné **Activation immédiate**, sélectionnez **Test mémoire** pour exécuter un test mémoire une fois la mise à jour du microprogramme terminée et si le serveur redémarre au cours de la mise à jour.

Cette option est prise en charge pour les serveurs ThinkSystem v1 et v2 (à l'exclusion des serveurs ThinkSystem SR635, SR645, SR655, SR665).

Etape 10. Cliquez sur **Effectuer la mise à jour** pour mettre à jour immédiatement, ou cliquez sur **Planning** pour planifier cette mise à jour pour une exécution ultérieure.

Le cas échéant, vous pouvez effectuer des actions d'alimentation sur les appareils gérés. Les actions d'alimentation sont utiles lorsque l'option **Activation différée** est sélectionnée et que vous souhaitez poursuivre les mises à jour lorsque l'appareil est à l'état « En attente de maintenance ». Pour effectuer une action d'alimentation sur un appareil géré à partir de cette page, cliquez sur **Toutes les actions → Actions d'alimentation**, puis cliquez sur l'une des actions d'alimentation suivantes.

- **Mettre sous tension**
- **Arrêter le système d'exploitation et mettre hors tension**
- **Mettre hors tension**
- **Arrêter le système d'exploitation et redémarrer**
- **Redémarrer**

Après avoir terminé

Lors de l'application d'une mise à jour de microprogramme, si le serveur ne passe pas en mode de maintenance, essayez à nouveau d'appliquer la mise à jour.

Si des mises à jour n'ont pas abouti, voir Problème de mise à jour et de référentiel de microprogramme dans la documentation en ligne de XClarity Administrator pour savoir comment identifier et résoudre les problèmes.

Depuis la page Mises à jour de microprogramme : Appliquer/Activer, vous pouvez effectuer les actions suivantes :

- Exporter les informations sur le microprogramme et la conformité pour chaque appareil géré en cliquant sur **Toutes les actions → Export View as CSV**.

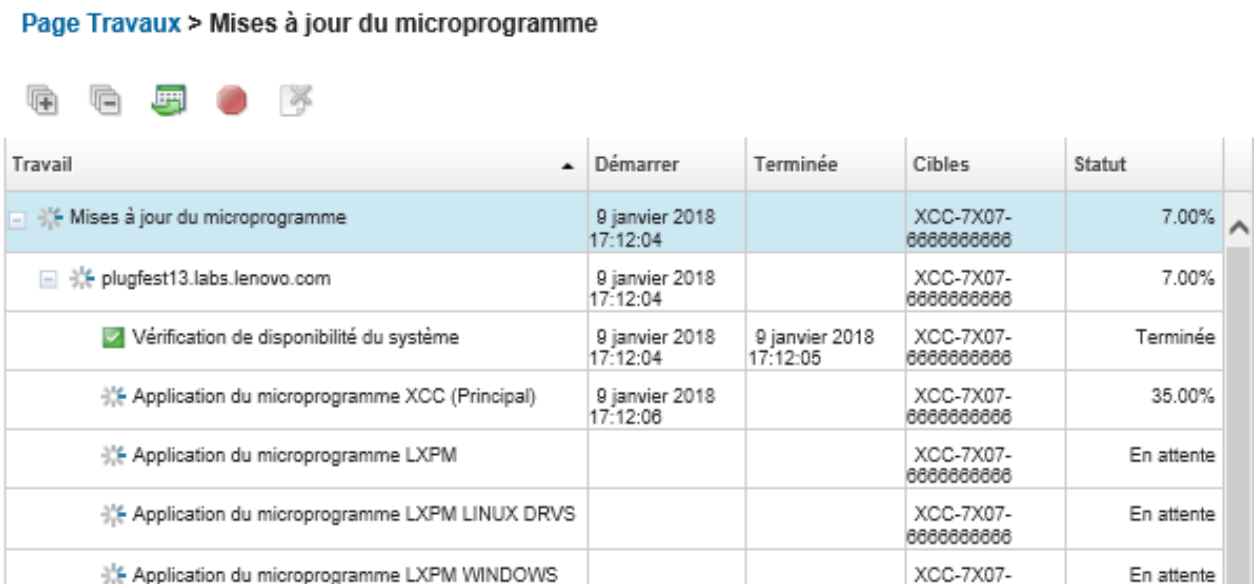
  Remarque : Le fichier CSV contient uniquement les informations filtrées dans la vue en cours. Les informations qui sont filtrées en dehors de la vue et les information dans les colonnes masquées ne sont pas incluses.

- Annuler une mise à jour en cours d'application sur un appareil en sélectionnant celui-ci et en cliquant sur l'icône **Annuler la mise à jour** ().

  Remarque : Vous pouvez annuler les mises à jour de microprogramme qui se trouvent dans la file d'attente de démarrage. Après le démarrage du processus de mise à jour, la mise à jour de microprogramme peut être annulée uniquement lorsque le processus de mise à jour exécute une tâche autre que l'application de la mise à jour, par exemple, le passage en mode de maintenance ou le redémarrage de l'appareil.

- Visualiser l'état de la mise à jour de microprogramme directement à partir de la page Appliquer/Activer dans la colonne **État**.
- Surveiller l'état du processus de mise à jour en consultant le journal des travaux. Dans le menu Lenovo XClarity Administrator, cliquez sur **Surveillance → Travaux**.

  Pour plus d'informations sur le journal des travaux, voir Surveillance des travaux.



Lorsque les travaux de mise à jour de microprogramme sont terminés, vous pouvez vérifier que les appareils sont conformes en cliquant sur **Distribution → Mises à jour de microprogramme : Appliquer/Activer** pour revenir à la page Mises à jour de microprogramme : Appliquer/Activer, puis en cliquant sur l'icône **Actualiser** ( ). La version de microprogramme active sur chaque appareil est répertoriée dans la colonne **Version installée**.

Application de certaines mises à jour de microprogramme sans utiliser de stratégie de conformité

Vous pouvez appliquer et activer rapidement un microprogramme qui est postérieur au microprogramme actuellement installé sur un appareil géré ou sur un groupe d'appareils sans utiliser de stratégies de conformité.

En savoir plus :

- XClarity Administrator : amélioration de l'efficacité lors de la mise à jour du microprogramme
- Meilleures pratiques concernant la mise à jour du microprogrammes et des pilotes Lenovo ThinkSystem
- XClarity Administrator : du serveur au cluster
- XClarity Administrator : mises à jour de microprogramme
- XClarity Administrator : Distribution des mises à jour de sécurité du microprogramme

Avant de commencer

- Prenez connaissance des remarques relatives à la mise à jour de microprogramme avant de tenter de mettre à jour un microprogramme sur vos appareils gérés (voir Considérations relatives à la mise à jour du microprogramme).
- Initialement, les appareils qui ne sont pas pris en charge pour les mises à jour sont masqués dans la vue. Les appareils qui ne sont pas pris en charge ne peuvent pas être sélectionnés pour les mises à jour.
- Par défaut, tous les composants détectés sont répertoriés comme disponibles pour l'application des mises à jour ; toutefois, un microprogramme de niveau antérieur peut empêcher un composant d'apparaître dans l'inventaire ou d'afficher des informations de version complète. Pour répertorier tous les modules basés sur des stratégies vous permettant d'appliquer des mises à jour, cliquez sur **Toutes les actions → Paramètres globaux**, et sélectionnez **Support étendu pour les appareils de niveau précédent**. Lorsque cette option est sélectionnée, la mention « Autre logiciel disponible » apparaît dans

la colonne Version installée pour les appareils non détectés. Pour plus d'informations, voir Configuration des paramètres globaux à jour de microprogramme.

Remarques :

- Les paramètres globaux ne peuvent pas être modifiés lorsque des mises à jour sont en cours sur des appareils gérés.
- La génération d'options supplémentaires peut nécessiter quelques minutes. Au bout de quelques instants, il vous faudra peut-être cliquer sur l'icône **Actualiser** () afin d'actualiser le tableau.

- Assurez-vous qu'aucun travail n'est en cours d'exécution sur le serveur cible. Si des travaux sont en cours exécution, le travail de mise à jour est placé en file d'attente jusqu'à ce que tous les autres travaux soient terminés. Pour afficher la liste des travaux actifs, cliquez sur **Surveillance → Travaux**.
- Assurez-vous que le référentiel des mises à jour de microprogramme contient les modules de microprogramme que vous souhaitez déployer. Si tel n'est pas le cas, actualisez le catalogue produit et téléchargez les mises à jour de microprogramme appropriées (voir Actualisation du catalogue produit et Téléchargement des mises à jour de microprogramme).

  Remarque : À l'origine, lorsque XClarity Administrator est installé, le catalogue produit et le référentiel sont vides.

  Si vous prévoyez d'installer un microprogramme prérequis, vérifiez que ce dernier a bien été téléchargé dans le référentiel.

  Dans certains cas, plusieurs versions peuvent être nécessaires afin de mettre à jour le microprogramme, et toutes devront être téléchargées vers le référentiel. Par exemple, pour effectuer la mise à niveau du commutateur évolutif IBM FC5022 SAN de la version v7.4.0a vers v8.2.0a, vous devez installer v8.0.1-pha, puis v8.1.1, et enfin v8.2.0a. Ces trois versions peuvent se trouver dans le référentiel afin de mettre à jour le commutateur vers v8.2.0a.
- En général, les appareils doivent être redémarrés pour que la mise à jour de microprogramme soit activée. Si vous décidez de redémarrer l'appareil lors du processus de mise à jour (*activation immédiate*), vérifiez que les charges de travail en cours d'exécution ont été arrêtées ou, si vous travaillez dans un environnement virtualisé, assurez-vous qu'elles ont été déplacées vers un autre serveur.

À propos de cette tâche

- Vous pouvez mettre à jour certains microprogrammes sur un maximum de 50 appareils à la fois. Si vous choisissez de mettre à jour certains microprogrammes sur plus de 50 appareils, les autres appareils sont mis en file d'attente. Un appareil en file d'attente est retiré de la file d'attente « de mise à jour de certains microprogrammes » lorsque l'activation se termine sur un appareil mis à jour ou qu'un appareil mis à jour est placé dans le mode En attente de maintenance (si un redémarrage est requis sur cet appareil). Lorsqu'un appareil dans le mode En attente de maintenance est redémarré, l'appareil démarre en mode de maintenance et poursuit le processus de mise à jour, même si le nombre maximal de mises à jour de microprogramme est déjà en cours.
- Vous pouvez appliquer et activer un microprogramme qui est postérieur au microprogramme actuellement installé.
- Vous pouvez choisir d'appliquer toutes les mises à jour pour un appareil spécifique. Cependant, vous pouvez aussi choisir de développer un appareil afin de spécifier des mises à jour pour un composant spécifique, par exemple, le contrôleur de gestion de la carte mère ou UEFI.
- Si vous choisissez d'installer un module de mise à jour de microprogramme contenant les mises à jour de plusieurs composants, tous les composants auxquels le module de mise à jour s'applique sont mis à jour.

Procédure

Pour appliquer et activer des mises à jour sur un appareil géré, procédez comme suit.

Etape 1. Dans la barre de menus XClarity Administrator, cliquez sur **Distribution → Mises à jour de microprogramme : Appliquer/Activer**. La page Mises à jour de microprogramme : Appliquer/Activer s'affiche.

Etape 2. Cliquez sur l'onglet **Mettre à jour sans stratégie**.

Etape 3. Sélectionnez le niveau de microprogramme dans la colonne **Versions ultérieures téléchargées** pour chaque appareil que vous souhaitez mettre à jour.

Etape 4. Sélectionnez l'un ou plusieurs des appareils que vous souhaitez mettre à jour.

Vous pouvez trier les colonnes du tableau afin de faciliter la recherche de serveurs spécifiques. En outre, vous pouvez filtrer la liste des appareils affichés en sélectionnant une option dans le menu **Afficher** pour afficher uniquement la liste des appareils dans un châssis, armoire ou groupe spécifique, en entrant du texte (par exemple, un nom ou une adresse IP) dans la zone **Filtre** ou en cliquant sur les icônes suivantes pour afficher uniquement les appareils avec un état spécifique.

- Icône **Masquer les composants avec des versions ultérieures** ( )
- Icône **Masquer les composants sans versions ultérieures** ( )
- Icône **Masquer les appareils non pris en charge pour les mises à jour** ( )
- Icône **Masquer les appareils avec des mises à jour de microprogramme en cours** ( )
- Icône **Masquer les appareils avec microprogramme non indexable** ( )

La colonne **Groupes** indique les groupes dont chaque appareil est membre. Vous pouvez survoler la colonne **Groupes** pour obtenir une liste complète des groupes, par type de groupe

La colonne **Version installée** indique la version de microprogramme installée, l'état de conformité ou l'état de l'appareil.

L'état de conformité peut être l'un des suivants :

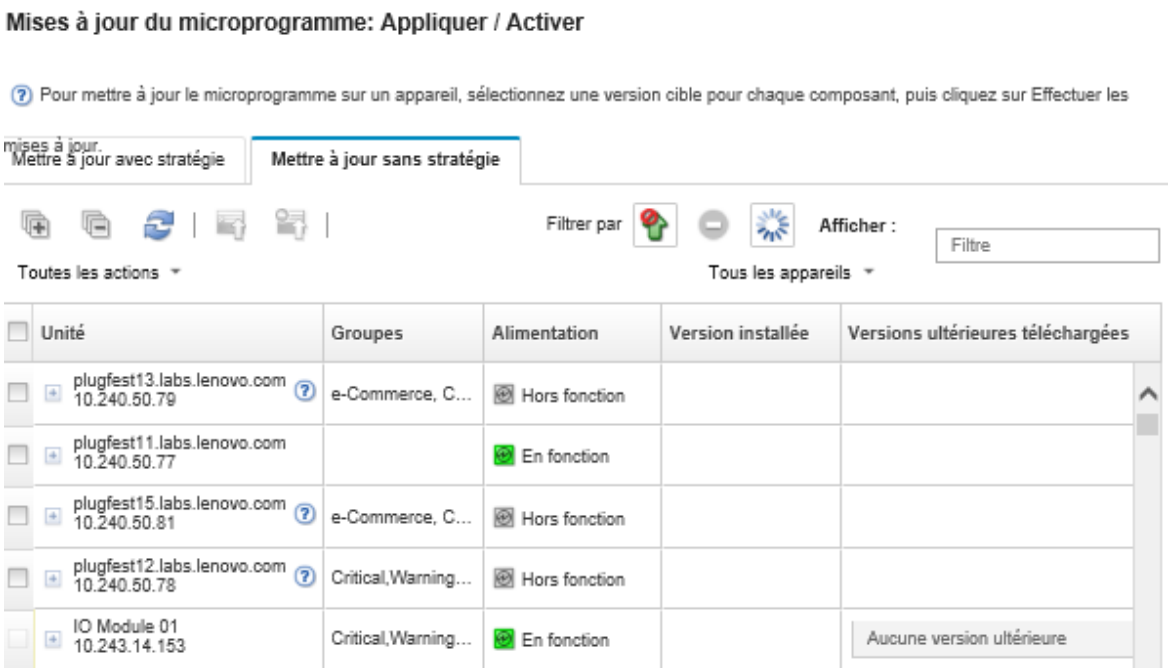
- **Conforme**
- **Erreur de conformité**
- **Non compatible**
- **Aucune stratégie de conformité définie**
- **Non surveillé**

L'état de l'appareil peut être l'un des suivants :

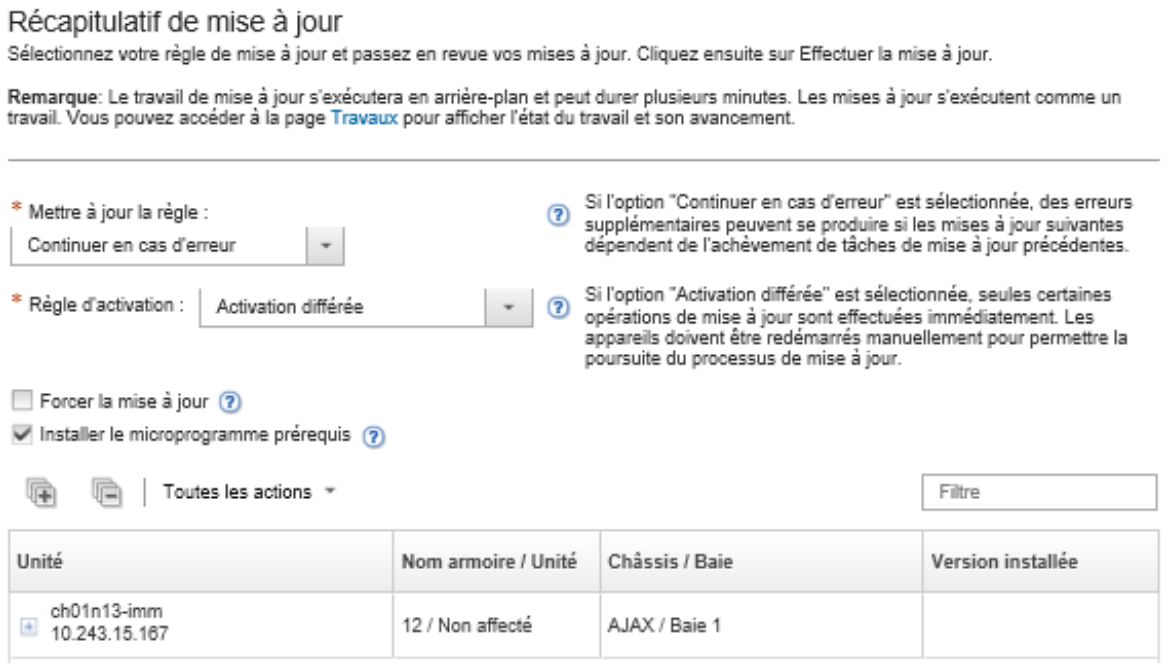
- **Mises à jour non prises en charge**
- **Mise à jour en cours**

Remarques : Si la version de microprogramme installée est en attente d'activation, « (Activation en attente) » est ajouté à la version de microprogramme installée et l'état de conformité de chaque appareil applicable, par exemple « 2.20 / A9E12EUS (Activation en attente). » Pour afficher l'état d'activation en attente, la version de microprogramme suivante doit être installée sur le contrôleur de gestion de la carte mère principal dans le serveur.

- **IMM2** : TCOO46F, TCOO46E ou version ultérieure (selon la plateforme)
- **XCC** : CDI328M, PSI316N, TEI334I ou version ultérieure (selon la plateforme)



Etape 5. Cliquez sur l'icône **Effectuer les mises à jour** ( ). La boîte de dialogue Récapitulatif des mises à jour s'affiche.



Etape 6. Sélectionnez l'une des règles de mise à jour

- **Arrêter toutes les mises à jour en cas d'erreur**. Si une erreur se produit lors de la mise à jour de l'un des composants (par exemple, un adaptateur ou un contrôleur de gestion) sur l'appareil cible, le processus de mise à jour de microprogramme s'arrête pour tous les appareils sélectionnés dans le travail de mise à jour de microprogramme en cours. Dans ce cas, aucune des mises à jour du module de mise à jour pour l'appareil n'est appliquée. Le microprogramme actuellement installé sur tous les systèmes sélectionnés reste en vigueur.

- **Continuer en cas d'erreur**. Si une erreur se produit lors de la mise à jour de l'un des dispositifs de l'appareil, le processus de mise à jour de microprogramme ne met pas à jour le microprogramme de l'appareil concerné ; toutefois, le processus de mise à jour de microprogramme continue de mettre à jour les autres dispositifs de l'appareil et de mettre à jour tous les autres appareils du travail de mise à jour de microprogramme en cours.
- **Passer au système suivant en cas d'erreur**. Si une erreur se produit lors de la mise à jour de l'un des dispositifs de l'appareil, le processus de mise à jour de microprogramme arrête toutes les tentatives de mise à jour de microprogramme pour cet appareil spécifique, de sorte que le microprogramme actuellement installé sur celui-ci reste en vigueur. Le processus de mise à jour de microprogramme continue de mettre à jour tous les autres appareils du travail de mise à jour de microprogramme en cours.

Remarque : Une fois activée, l'option d'amorçage Wake on LAN peut affecter les opérations XClarity Administrator qui mettent le serveur hors tension, notamment les mises à jour du microprogramme si votre réseau comprend un client Wake on LAN qui émet des commandes « Wake on Magic Packet ».

Etape 7. Sélectionnez l'une des règles d'activation :

- **Activation immédiate**. Au cours du processus de mise à jour, il est possible que l'appareil redémarre automatiquement plusieurs fois jusqu'à la fin du processus de mise à jour. Avant de continuer, prenez soin de mettre au repos toutes les applications sur l'appareil.
- **Activation différée**. Seules certaines opérations de mise à jour sont effectuées. Les appareils doivent être redémarrés pour permettre la poursuite du processus de mise à jour. Des redémarrages supplémentaires sont ensuite effectués jusqu'à l'achèvement de l'opération de mise à jour.

  Un événement est déclenché lorsque l'état passe en **mode de maintenance du microprogramme en attente** pour vous avertir du redémarrage du serveur.

  Si un appareil redémarre pour une raison quelconque, le processus de mise à jour différé se termine.

  Cette règle d'activation est prise en charge uniquement pour les serveurs et les commutateurs de type armoire. Les modules CMM et les commutateurs Flex sont activés immédiatement, quelle que soit la valeur affectée à ce paramètre.

  Un événement est déclenché lorsque l'état passe en **mode de maintenance du microprogramme en attente** pour vous avertir du redémarrage du serveur.

  Le processus de mise à jour différée s'achève lorsque l'appareil est redémarré pour une raison quelconque (y compris un redémarrage manuel). Il n'y a pas de limite de temps imposée au redémarrage du serveur.

  XClarity Administrator peut appliquer des mises à jour avec une activation différée sur 50 appareils simultanément au maximum. Si vous tentez d'appliquer des mises à jour avec une activation différée sur plus de 50 appareils, les appareils excédentaires seront mis en file d'attente. Un appareil sort de la file d'attente lorsqu'un appareil mis à jour passe à l'état **Mode de maintenance du microprogramme en attente.**

  Important :

  – Si XClarity Administrator est redémarré pendant la tâche de mise à jour, cette tâche s'arrêtera avec une erreur.

  – Si un serveur se trouvant dans l'état **Mode de maintenance du microprogramme en attente** est redémarré alors que XClarity Administrator est à l'arrêt ou inaccessible, le serveur s'amorce sur la BMU, mais comme XClarity Administrator ne peut pas se connecter à la BMU et que le délai expire au bout de 60 secondes, le statut d'alimentation du système est

rétabli par le contrôleur de gestion de la carte mère (arrête le système s'il était hors tension, le redémarre s'il était sous tension).

- **Activation hiérarchisée**. Les mises à jour du microprogramme sur le contrôleur de gestion de la carte mère sont activées immédiatement. toutes les autres mises à jour de microprogramme sont des mises à jour de microprogramme et sont activées au redémarrage suivant de l'appareil. Des redémarrages supplémentaires sont ensuite effectués jusqu'à l'achèvement de l'opération de mise à jour. Cette règle est prise en charge uniquement pour les serveurs.

  Un événement est déclenché lorsque l'état passe en mode de maintenance du microprogramme en attente pour vous avertir du redémarrage du serveur.

Remarque : Une fois activée, l'option d'amorçage Wake on LAN peut affecter les opérations XClarity Administrator qui mettent le serveur hors tension, notamment les mises à jour du microprogramme si votre réseau comprend un client Wake on LAN qui émet des commandes « Wake on Magic Packet ».

Etape 8. **Facultatif :** Sélectionnez **Forcer la mise à jour** pour mettre à jour le microprogramme sur les composants sélectionnés même si le niveau de microprogramme est à jour, ou pour appliquer une mise à jour du microprogramme antérieure à celle actuellement installée sur le composant sélectionné.

Remarque : Vous pouvez appliquer une version antérieure du microprogramme aux options d'appareils, d'adaptateurs et d'unités qui sont compatibles avec la rétromigration. Référez-vous à la documentation sur le matériel afin de déterminer si la rétromigration est bien prise en charge.

Etape 9. **Facultatif :** Désélectionnez **Installer le microprogramme requis** si vous ne souhaitez pas installer le microprogramme requis. Le microprogramme requis est installé par défaut.

Remarque : Lorsque vous utilisez **Activation différée** ou **Activation hiérarchisée** pour les mises à jour de microprogramme prérequises, vous devez redémarrer le serveur pour activer le microprogramme prérequis. Après le redémarrage initial, les mises à jour de microprogramme restantes sont installées à l'aide de **Activation immédiate**.

Etape 10. **Facultatif :** si vous avez sélectionné **Activation immédiate**, sélectionnez **Test mémoire** pour exécuter un test mémoire une fois la mise à jour du microprogramme terminée et si le serveur redémarre au cours de la mise à jour.

Cette option est prise en charge pour les serveurs ThinkSystem v1 et v2 (à l'exclusion des serveurs ThinkSystem SR635, SR645, SR655, SR665).

Etape 11. Cliquez sur **Effectuer la mise à jour** pour mettre à jour immédiatement, ou cliquez sur **Planning** pour planifier cette mise à jour pour une exécution ultérieure.

Le cas échéant, vous pouvez effectuer des actions d'alimentation sur les appareils gérés. Les actions d'alimentation sont utiles lorsque l'option **Activation différée** est sélectionnée et que vous souhaitez poursuivre les mises à jour lorsque l'appareil est à l'état « En attente de maintenance ». Pour effectuer une action d'alimentation sur un appareil géré à partir de cette page, cliquez sur **Toutes les actions → Actions d'alimentation**, puis cliquez sur l'une des actions d'alimentation suivantes.

- **Mettre sous tension**
- **Arrêter le système d'exploitation et mettre hors tension**
- **Mettre hors tension**
- **Arrêter le système d'exploitation et redémarrer**
- **Redémarrer**

Après avoir terminé

Lors de l'application d'une mise à jour de microprogramme, si le serveur ne passe pas en mode de maintenance, essayez à nouveau d'appliquer la mise à jour.

Si des mises à jour n'ont pas abouti, voir Problème de mise à jour et de référentiel de microprogramme dans la documentation en ligne de XClarity Administrator pour savoir comment identifier et résoudre les problèmes.

Depuis la page Mises à jour de microprogramme : Appliquer/Activer, vous pouvez effectuer les actions suivantes :

- Exporter les informations sur le microprogramme et la conformité pour chaque appareil géré en cliquant sur **Toutes les actions → Export View as CSV**.

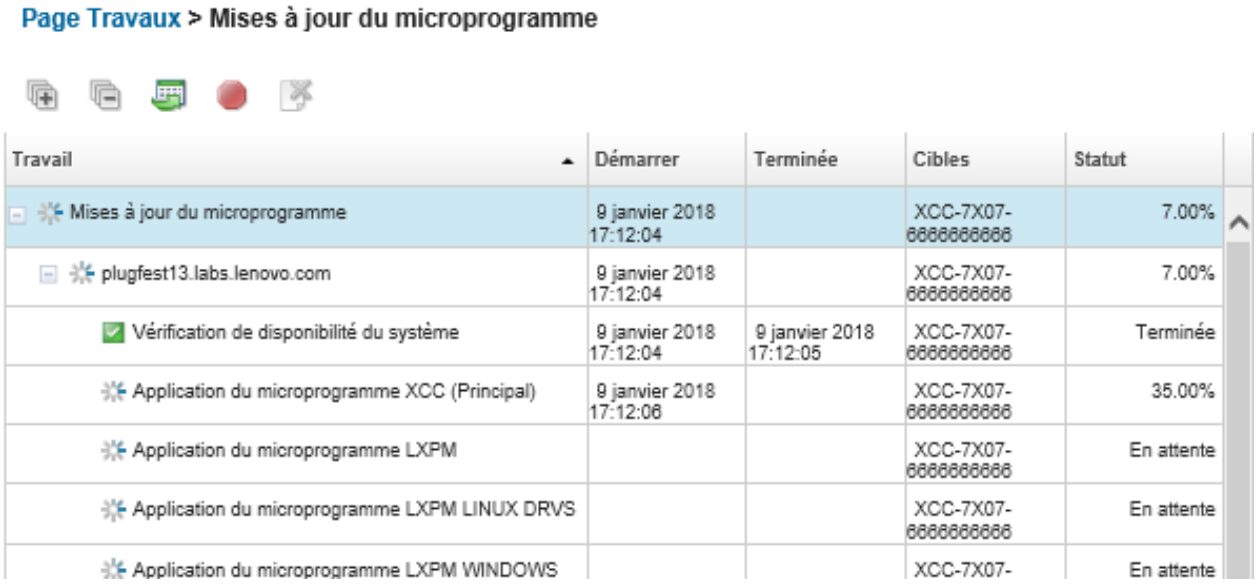
  Remarque : Le fichier CSV contient uniquement les informations filtrées dans la vue en cours. Les informations qui sont filtrées en dehors de la vue et les information dans les colonnes masquées ne sont pas incluses.

- Annuler une mise à jour en cours d'application sur un appareil en sélectionnant celui-ci et en cliquant sur l'icône **Annuler la mise à jour** ( ).

  Remarque : Vous pouvez annuler les mises à jour de microprogramme qui se trouvent dans la file d'attente de démarrage. Après le démarrage du processus de mise à jour, la mise à jour de microprogramme peut être annulée uniquement lorsque le processus de mise à jour exécute une tâche autre que l'application de la mise à jour, par exemple, le passage en mode de maintenance ou le redémarrage de l'appareil.

- Visualiser l'état de la mise à jour de microprogramme directement à partir de la page Appliquer/Activer dans la colonne **État**.
- Surveiller l'état du processus de mise à jour en consultant le journal des travaux. Dans le menu Lenovo XClarity Administrator, cliquez sur **Surveillance → Travaux**.

  Pour plus d'informations sur le journal des travaux, voir Surveillance des travaux.



Lorsque les travaux de mise à jour de microprogramme sont terminés, vous pouvez vérifier que les appareils sont conformes en cliquant sur **Distribution → Mises à jour de microprogramme : Appliquer/Activer** pour revenir à la page Mises à jour de microprogramme : Appliquer/Activer, puis en cliquant sur l'icône **Actualiser** ( ). La version de microprogramme active sur chaque appareil est répertoriée dans la colonne **Version installée**.

Chapitre 14. Mise à jour des pilotes de périphérique Windows sur des serveurs gérés

Avec Windows UpdateXpress System Packs (UXSPs), vous pouvez mettre à jour des pilotes de périphérique SE sur les systèmes d'exploitation Windows déployés.

Avant de commencer

Vous devez disposer de droits **lxc-os-admin**, **lxc-supervisor**, **lxc-admin** ou **lxc-matériel-admin** pour gérer et déployer des pilotes de périphérique SE et pour effectuer des actions d'alimentation sur des serveur gérés à partir de pages Mises à joue de pilote Windows.

La mise à jour du microprogramme et la mise à jour des pilotes de périphérique sont des processus distincts dans XClarity Administrator ; il n'y a pas de connexion entre ces processus. XClarity Administrator ne conserve pas la conformité entre les microprogrammes et les pilotes d'appareils sur les appareils gérés, même s'il est recommandé de mettre à jour les pilotes de périphérique en même temps que le microprogramme.

À propos de cette tâche

Les UpdateXpress System Packs (UXSPs) Windows contiennent des pilotes de périphérique Windows pour les versions Windows prises en charge et pour les serveurs Lenovo prenant en charge Windows.

Seuls les pilotes de périphérique pour Windows Server 2012 R2 et versions ultérieures sont pris en charge. XClarity Administrator ne prend pas en charge la mise à jour des pilotes de périphériques Linux ou VMware.

Pour plus d'informations sur l'installation de pilotes de périphérique lors du déploiement de systèmes d'exploitation, voir Installation de systèmes d'exploitation sur des serveurs nus.

Procédure

Etape 1. **Configuration de Windows Server pour les mises à jour de pilote de périphérique SE**

Module Lenovo XClarity Administrator utilise le service WinRM (Windows Remote Management) qui écoute via HTTPS ou HTTP pour exécuter des commandes de mise à jour du pilote de périphérique sur les systèmes Windows cibles. Ce service WinRM doit être configuré correctement sur les serveurs cible avant de tenter de mettre à jour les pilotes de périphérique SE (voir Configuration de Windows Server pour les mises à jour de pilote de périphérique SE).

Etape 2. **Gestion du référentiel de pilote de périphérique SE**

Le *référentiel de pilote de périphérique SE* présente un catalogue de pilotes de périphériques Windows disponibles et les modules de pilotes de périphériques applicables aux appareils gérés.

Le *catalogue* présente des informations sur tous les Windows UpdateXpress System Packs (UXSP) et les mises à jour de pilotes de périphériques disponibles pour tous les serveurs Lenovo prenant en charge Windows. Le catalogue organise les mises à jour de pilote de périphérique par type de dispositif. Lorsque vous actualisez le catalogue, XClarity Administrator extrait des informations sur les UXSPs disponibles à partir du Site Web Assistance centre de données Lenovo (y compris les métadonnées .xml et les fichiers .txt readme) et stocke ces informations dans le référentiel. Le fichier de contenu (.exe) n'est pas téléchargé. Pour plus d'informations sur l'actualisation du catalogue, voir Actualisation du catalogue de pilotes de périphérique SE.

Vous pouvez télécharger ou importer les UXSP Windows dans le référentiel. Les UXSP Windows contiennent des pilotes de périphérique Windows pour les versions Windows prises en charge et pour les serveurs Lenovo prenant en charge Windows. Les UXSP doivent être disponibles dans le référentiel afin que vous puissiez mettre à jour les pilotes de périphérique Windows sur les serveurs gérés. Pour plus d'informations sur le téléchargement des pilotes de périphérique, voir Téléchargement des pilotes de périphérique Windows .

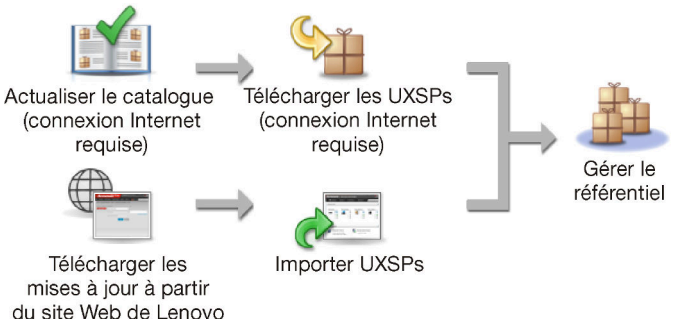
Vous pouvez déterminer si les modules UXSP sont stockés dans le référentiel des pilotes de périphérique SE à partir de la colonne État du téléchargement sous l'onglet Mises à jour individuelles, à la page Mises à jour de pilote Windows : référentiel. Cette colonne contient les valeurs suivantes.

- **Téléchargé**. L'ensemble du contenu du module ou la mise à jour individuelle est stocké(e) dans le référentiel.
- ***x* sur *y* téléchargé(s)**. Une partie seulement des mises à jour présentes dans le module est stockée dans le référentiel. Les nombres entre parenthèses indiquent le nombre de mises à jour disponibles et le nombre de mises à jour stockées, ou bien il n'existe aucune mise à jour pour le type d'appareil spécifique.
- **Non téléchargé**. La totalité du contenu du module ou la mise à jour individuelle est disponible, mais pas stocké(e) dans le référentiel.

Remarque : Lorsque vous téléchargez ou importez des UXSP depuis la page Référentiel des mises à jour de pilote Windows, seuls les pilotes de périphérique sont téléchargés et stockés dans le référentiel. Les mises à jour du microprogramme ont été supprimées. Pour plus d'informations sur le téléchargement ou l'importation de mises à jour de microprogramme, voir Gestion du référentiel des mises à jour de microprogramme.

XClarity Administrator doit être connecté à Internet pour actualiser le catalogue et télécharger les UXSPs. S'ils ne sont pas connecté à Internet, vous pouvez télécharger manuellement les UXSPs sur un poste de travail disposant d'un accès réseau à l'hôte XClarity Administrator à l'aide d'un navigateur web. Ce téléchargement UXSPs est au format zip et il contient tous les fichiers de pilote de périphérique requis pour UXSP, y compris le contenu (.exe), les métadonnées (.xml) et le fichier historique des modifications (.chg) ainsi que les fichiers readme (.txt).

Remarque : Vous pouvez voir des messages indiquant que des fichiers de microprogramme (fw) ne sont pas nécessaires et ont été supprimés. Ceci est normal, car seuls les pilotes de périphérique Windows sont mis à jour à l'aide de ce processus.



Attention :

- Ne décompressez pas UXSP avant de l'importer.
- Les UXSPs Windows incluent des pilotes de périphérique et des mises à jour de microprogramme. Les mises à jour de microprogramme dans les UXSPs Windows sont

supprimés lorsque les UXSPs sont importés dans le référentiel et un message d'avertissement s'affiche. Seuls les pilotes de périphérique sont importés.

Etape 3. **Application de pilotes de périphérique SE**

XClarity Administrator n'applique pas automatiquement les pilotes de périphérique aux serveurs gérés. Pour mettre à jour les pilotes de périphérique, devez appliquer manuellement les pilotes de périphérique sur les serveurs sélectionnés.

Attention : Avant de tenter de mettre à jour les pilotes de périphérique sur les serveurs gérés, prenez soin d'examiner les points suivants et d'effectuer les actions préalables requises.

- Les appareils qui ne sont pas pris en charge ne peuvent pas être sélectionnés pour les mises à jour.
- Prenez connaissance des remarques relatives à la mise à jour du pilote de périphérique avant de tenter de mettre à jour les pilotes de périphérique sur vos serveurs gérés (voir Instructions de mise à jour du pilote de périphérique SE).
- Assurez-vous que le référentiel contient les UXSPs et les pilotes de périphérique que vous souhaitez déployer (voir Téléchargement des pilotes de périphérique Windows).

  Remarque : À l'origine, lorsque XClarity Administrator est installé, le catalogue et le référentiel sont vides.
- XClarity Administrator peut utiliser le service WinRM (Windows Remote Management) qui écoute via HTTPS ou HTTP pour exécuter des commandes de mise à jour du pilote de périphérique sur les systèmes Windows cibles. HTTP est la valeur par défaut. Pour utiliser HTTP, cliquez sur **Toutes les actions → Paramètres globaux** sur la page Mises à jour de pilote Windows : Appliquer, puis désélectionnez **Utiliser HTTPS pour les mises à jour de pilote Windows**.

  Attention : Lors de l'utilisation de HTTP, les données d'identification utilisateur Windows sont envoyées sur le réseau *sans* chiffrement et elles peuvent être facilement affichées à l'aide d'outils de dépannage réseau couramment disponibles.

  Important :

  – Vérifiez que Windows Remote Management (WinRM) sur le serveur cible est configuré pour l'utilisation du même paramètre (HTTPS ou HTTP) qui est défini dans XClarity Administrator (voir Configuration de Windows Server pour les mises à jour de pilote de périphérique SE).

  – Assurez-vous que WinRM sur le serveur cible est configuré avec l'authentification de base.

  – Lors de l'utilisation de HTTPS, assurez-vous que WinRM sur le serveur cible est configuré avec **allowUnencrypted=false**.
- Vérifiez que PowerShell est pris en charge sur le serveur cible.
- Vérifiez que le serveur cible est sous tension avant d'essayer de mettre à jour les pilotes de périphérique. Si le serveur n'est pas sous tension, sélectionnez le serveur cible, puis cliquez sur **Toutes les actions → Actions d'alimentation → Mettre sous tension**.
- Vérifiez que XClarity Administrator dispose des informations dont il a besoin pour accéder au système d'exploitation hôte (voir Gestion de l'accès aux systèmes d'exploitation sur les serveurs gérés.
- Si vous souhaitez utiliser un compte de domaine lors de la mise à jour des pilotes de périphérique S.E., assurez-vous d'avoir créé le fichier de configuration requis (voir Configuration d'un compte de domaine pour les mises à jour de pilotes de périphérique S.E.).
- Assurez-vous qu'aucun travail n'est en cours d'exécution sur le serveur cible. Vous ne pouvez pas mettre à jour les pilotes de périphérique sur un serveur géré qui est verrouillé par un travail en cours d'exécution. Si un autre travail de mise à jour est en cours d'exécution sur le serveur

cible, ce travail de mise à jour est mis en file d'attente jusqu'à ce que le travail de mise à jour en cours soit terminé. Pour afficher la liste des travaux actifs, cliquez sur **Surveillance → Travaux**.

Pour plus d'informations sur la mise à jour des pilotes de périphérique, voir Application de pilotes de périphérique Windows.

Instructions de mise à jour du pilote de périphérique SE

Avant de commencer à mettre à jour les pilotes de périphérique SE pour des appareils gérés à l'aide de Lenovo XClarity Administrator, prenez connaissance des remarques importantes présentées ci-après.

Remarque : Vous devez disposer de droits **lxc-os-admin**, **lxc-supervisor**, **lxc-admin** ou **lxc-hw-admin** pour gérer et déployer des pilotes de périphérique SE et pour effectuer des actions d'alimentation sur des serveur gérés à partir de pages Mises à joue de pilote Windows.

Remarques sur le réseau

- Les ports et les adresses Internet requis doivent être disponibles avant de tenter de télécharger UpdateXpress System Packs (UXSPs). Pour plus d'informations, voir Disponibilité de port et Pare-feux et serveurs proxy dans la documentation en ligne de XClarity Administrator.
- Pour la gestion du châssis et des serveurs, XClarity Administrator doit avoir accès au réseau de gestion et de données pour accéder au système d'exploitation.
- Veillez à ce que XClarity Administrator doit pouvoir communiquer avec le serveur cible (à la fois le contrôleur de gestion de la carte mère et le réseau de données du serveur) sur l'interface réseau (Eth0 ou Eth1) qui a été sélectionnée au moment de la configuration de l'accès réseau de XClarity Administrator et que l'interface est configurée avec une adresse IPv4 ou une adresse ULA IPv6 automatique.

  Pour indiquer une interface à utiliser pour le déploiement du système d'exploitation, voir Configuration de l'accès réseau).

  Pour plus d'informations sur le réseau et les interfaces de déploiement de système d'exploitation, voir Remarques sur le réseau dans la documentation en ligne de XClarity Administrator .
- Les adresses IP doivent être uniques pour le système d'exploitation hôte.
- XClarity Administrator peut utiliser le service WinRM (Windows Remote Management) qui écoute via HTTPS ou HTTP pour exécuter des commandes de mise à jour du pilote de périphérique sur les systèmes Windows cibles. HTTP est la valeur par défaut. Pour utiliser HTTP, cliquez sur **Toutes les actions → Paramètres globaux** sur la page Mises à jour de pilote Windows : Appliquer, puis désélectionnez **Utiliser HTTPS pour les mises à jour de pilote Windows**.

  Attention : Lors de l'utilisation de HTTP, les données d'identification utilisateur Windows sont envoyées sur le réseau *sans* chiffrement et elles peuvent être facilement affichées à l'aide d'outils de dépannage réseau couramment disponibles.

Remarques sur les appareils gérés

- Les pilotes de périphériques Windows ne sont pas pris en charge pour les serveurs ThinkAgile, ThinkSystem SR635 et ThinkSystemSR655.
- Seuls les serveurs ThinkSystem, Lenovo System x et Lenovo Flex System sont pris en charge.
- XClarity Administrator ne valide pas la relation entre le contrôleur de gestion et le système d'exploitation. Le contrôleur de gestion de la carte mère est utilisé pour mettre sous tension ou hors tension le serveur.
- Assurez-vous que l'interface locale via USB est activée. L'interface locale via USB est utilisée lors de la mise à jour les pilotes de périphérique SE.

Remarques relatives au système d'exploitation et au pilote de périphérique

- Vous pouvez mettre à jour les pilotes de périphériques pour les systèmes d'exploitation suivants.

  - Windows Server 2012 R2
  - Windows Server 2016
  - Windows Server 2019

  Remarque : XClarity Administrator est uniquement testé avec des versions Windows prises en charge par Microsoft au moment de la sortie de la version XClarity Administrator.
- Windows Remote Management (WinRM) doit être configuré pour HTTPS sur le serveur cible (voir Configuration de Windows Server pour les mises à jour de pilote de périphérique SE).
- PowerShell doit être pris en charge sur le serveur cible.
- Vous devez fournir les informations nécessaires pour accéder au système d'exploitation hôte sur le serveur cible, y compris l'adresse IP SE et les données d'identification (voir Gestion de l'accès aux systèmes d'exploitation sur les serveurs gérés). Vous devez fournir des données d'identification pour un compte utilisateur disposant de droits d'administrateur
- XClarity Administrator met à jour uniquement les pilotes de périphérique qui ne sont pas conformes. Les pilotes de périphérique ne sont pas conformes lorsque la version sur le serveur est antérieure à la version dans les UXSP sélectionnés. Les pilotes de périphérique qui sont égaux ou postérieurs à la version des UXSP sélectionnés sont ignorés.
- La conformité du pilote de périphérique est exacte lorsque le matériel est présent. Si le matériel n'est pas présent, les pilotes de périphérique sont toujours appliqués au serveur. Lorsque vous ajoutez le matériel manquant au serveur, Windows charge la version la plus récente.
- Les serveurs System x ne prennent pas en charge certains pilotes de périphérique prédéfinis fournis avec XClarity Administrator. Pour déployer les pilotes de périphérique sur ces serveurs, créez un profil personnalisé comprenant exclusivement les pilotes de périphérique nécessaires.

Gestion du référentiel des pilotes de périphérique SE

Le *référentiel des pilotes de périphérique SE* comprend le catalogue et les pilotes de périphérique Windows téléchargés.

À propos de cette tâche

Le *catalogue* présente des informations sur tous les Windows UpdateXpress System Packs (UXSP) et les mises à jour de pilotes de périphériques disponibles pour tous les serveurs Lenovo prenant en charge Windows. Le catalogue organise les mises à jour de pilote de périphérique par type de dispositif. Lorsque vous actualisez le catalogue, XClarity Administrator extrait des informations sur les UXSPs disponibles à partir du Site Web Assistance centre de données Lenovo (y compris les métadonnées .xml et les fichiers .txt readme) et stocke ces informations dans le référentiel. Le fichier de contenu (.exe) n'est pas téléchargé. Pour plus d'informations sur l'actualisation du catalogue, voir Actualisation du catalogue de pilotes de périphérique SE.

Les UpdateXpress System Packs (UXSPs) Windows contiennent des pilotes de périphérique Windows pour les versions Windows prises en charge et pour les serveurs Lenovo prenant en charge Windows. Vous pouvez télécharger ou importer les UXSP Windows dans le référentiel. Les UXSP Windows contiennent des pilotes de périphérique Windows pour les versions Windows prises en charge et pour les serveurs Lenovo prenant en charge Windows. Les UXSP doivent être disponibles dans le référentiel afin que vous puissiez mettre à jour les pilotes de périphérique Windows sur les serveurs gérés.Pour plus d'informations sur le téléchargement des pilotes de périphérique, voir Téléchargement des pilotes de périphérique Windows .

XClarity Administrator doit être connecté à Internet pour actualiser le catalogue et télécharger les UXSPs. S'ils ne sont pas connecté à Internet, vous pouvez télécharger manuellement les UXSPs sur un poste de travail disposant d'un accès réseau à l'hôte XClarity Administrator à l'aide d'un navigateur web. Ce téléchargement UXSPs est au format zip et il contient tous les fichiers de pilote de périphérique requis pour

UXSP, y compris le contenu (.exe), les métadonnées (.xml) et le fichier historique des modifications (.chg) ainsi que les fichiers readme (.txt).

Après le téléchargement d'un UXSP dans le référentiel, les informations sur chaque pilote de périphérique du module sont ajoutées à la page Référentiel des mises à jour de pilote Windows. Il s'agir de la date d'édition, de la taille et de la gravité. Le niveau de gravité indique l'impact et la nécessité d'appliquer la mise à jour pour vous aider à déterminer de quelle manière votre environnement peut être affecté.

- **Édition initiale**. Il s'agit de la première édition du pilote de périphérique.
- **Critique**. Le pilote de périphérique contient des correctifs urgents destinés à résoudre des problèmes d'altération de données, de sécurité et de stabilité.
- **Suggérée**. Le pilote de périphérique contient des correctifs significatifs destinés à résoudre des problèmes potentiels.
- **Non critique**. Le pilote de périphérique contient des correctifs mineurs, des améliorations de performances et des modifications textuelles.

Remarques :

- Le niveau de gravité est relatif à la version précédente du pilote de périphérique. Par exemple, si la version 1.01 du pilote de périphérique installée, que la version 1.02 de mise à jour est de type Critique et que la version 1.03 de mise à jour est de type Recommandé, cela signifie que la mise à jour de la version 1.02 vers la version 1.03 est recommandée, mais que la mise à jour de la version 1.01 vers la version 1.03 est critique car elle est cumulative (la version 1.03 inclut les problèmes critiques résolus par la version 1.02).
- Des cas particuliers peuvent exister lorsqu'une mise à jour est uniquement critique ou recommandée pour un type de machine spécifique. Pour plus d'informations, voir le document Notes sur l'édition.

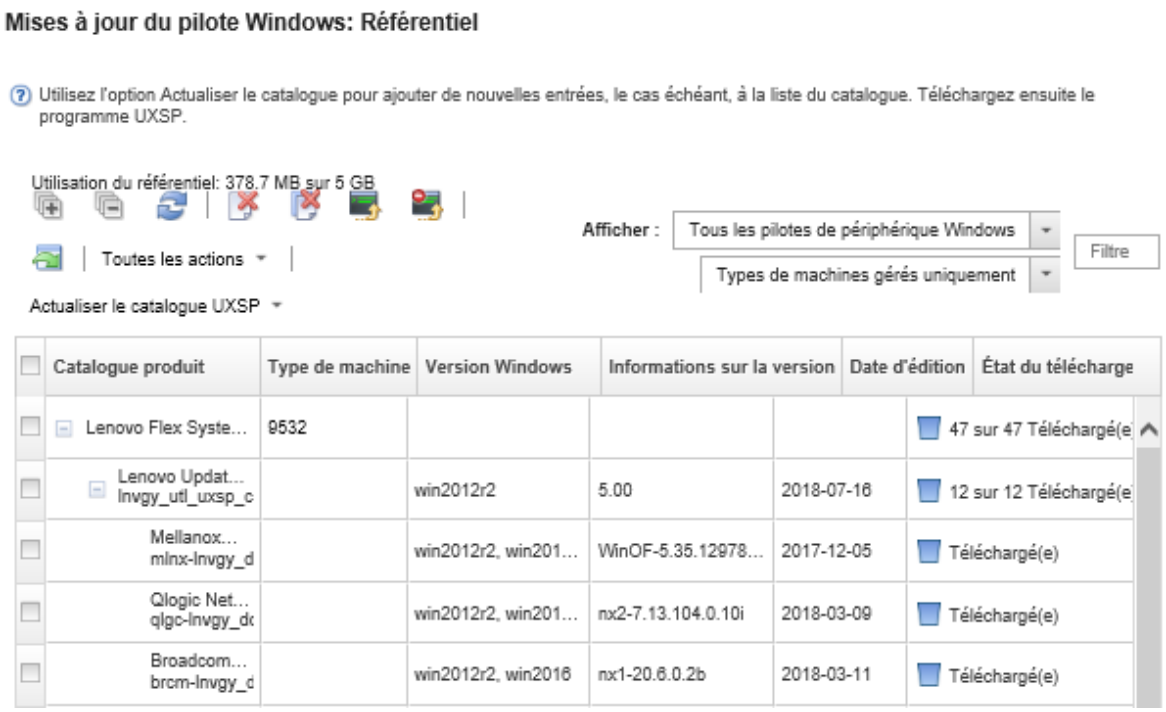
Procédure

Pour afficher les UXSPs et les pilotes de périphérique disponibles dans le référentiel, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Mises à jour de pilote Windows : Référentiel**. La page Référentiel des mises à jour de pilote Windows présente une liste des UXSPs disponibles, organisée par type d'appareil.

Etape 2. Développez un type de serveur, puis les UXSPs qui sont disponibles pour ce type de serveur afin d'afficher les pilotes de périphérique qui sont disponibles pour ce type de serveur.

Vous pouvez trier les colonnes du tableau et cliquer sur l'icône **Développer tout** () et **Icône Réduire** () afin de faciliter la recherche de pilotes de périphérique spécifiques. En outre, vous pouvez filtrer la liste des types de serveur et des pilote de périphérique affichés en sélectionnant une option dans le menu **Afficher** pour afficher uniquement les pilotes de périphérique d'un âge donné, les pilotes de périphérique de tous les types de serveurs ou uniquement des types de serveurs gérés, ou en entrant du texte dans la zone **Filtre**.



Depuis cette page, vous pouvez effectuer les actions suivantes :

- Procédez à l'extraction des dernières informations relatives aux UXSPs disponibles en cliquant sur l'icône **Actualiser le catalogue**.

  L'extraction de ces informations peut durer plusieurs minutes. Pour plus d'informations, voir Actualisation du catalogue de pilotes de périphérique SE.
- Téléchargez les UXSPs et les pilotes de périphérique à l'aide de XClarity Administrator en actualisant le catalogue et en cliquant sur l'icône **Télécharger** ( ). Une fois les UXSPs et les pilotes de périphérique téléchargés et ajoutés au référentiel, l'état prend la valeur « Téléchargé ».

  Pour plus d'informations sur le téléchargement des UXSPs et des pilotes de périphérique, voir Téléchargement des pilotes de périphérique Windows .
- Importez les UXSPs que vous avez téléchargées manuellement sur un poste de travail depuis le Web ou des pilotes de périphérique que vous avez exportés depuis XClarity Administrator (voir Téléchargement des pilotes de périphérique Windows).
- Arrêtez les téléchargements sélectionnés qui sont actuellement en cours en cliquant sur l'icône **Annuler les téléchargements** ( ).
- Supprimez les UXSPs sélectionnez ou les pilotes de périphérique individuels du référentiel en cliquant sur l'icône **Supprimer** ( ).

Actualisation du catalogue de pilotes de périphérique SE

Le catalogue de pilotes de périphérique SE contient des informations sur tous les UpdateXpress System Packs (UXSPs) Windows et les pilotes de périphérique qui sont disponibles pour tous les serveurs Lenovo prenant en charge les mises à jour de pilote de périphérique Windows.

Avant de commencer

Assurez-vous que Lenovo XClarity Administrator est connecté à Internet.

À propos de cette tâche

Lorsque vous actualisez le catalogue, XClarity Administrator extrait des informations sur les UXSPs disponibles à partir du Site Web Assistance centre de données Lenovo (y compris les métadonnées .xml et les fichiers .txt readme) et stocke ces informations dans le référentiel. Le fichier de contenu (.exe) n'est pas téléchargé. Vous devez télécharger les UXSP et les contenus de pilote de périphérique SE avant de mettre à jour les pilotes de périphérique sur des serveurs gérés. Pour plus d'informations sur le téléchargement des pilotes de périphérique, voir Téléchargement des pilotes de périphérique Windows .

Remarque : L'actualisation du catalogue peut durer plusieurs minutes.

Procédure

Pour actualiser le catalogue, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Mises à jour de pilotes Windows : Référentiel** pour afficher la page Mises à jour de pilotes Windows : Référentiel.

Etape 2. Cliquez sur **Actualiser le catalogue**, puis cliquez sur l'une des options suivantes pour obtenir des informations sur les derniers UXSPs disponibles.

- **Actualiser les éléments sélectionnés - Les éléments les plus récents uniquement**. Extrait des informations sur les dernières versions des UXSP disponibles uniquement pour les serveurs sélectionnés.
- **Actualiser tout - Les éléments les plus récents uniquement**. Extrait des informations sur les dernières versions des UXSP pour tous les serveurs pris en charge.
- **Actualiser les éléments sélectionnés**. Extrait des informations sur toutes les versions des UXSP disponibles uniquement pour les serveurs sélectionnés.
- **Actualiser tout**. Extrait des informations sur toutes les versions des UXSP disponibles uniquement pour tous les serveurs pris en charge.

Etape 3. Cliquez sur **Actualiser le catalogue** pour actualiser immédiatement, ou cliquez sur **Planning** pour planifier cette actualisation pour une exécution ultérieure.

Téléchargement des pilotes de périphérique Windows

Les UpdateXpress System Packs (UXSPs) Windows contiennent des pilotes de périphérique Windows pour les versions Windows prises en charge et pour les serveurs Lenovo prenant en charge Windows. Vous pouvez télécharger ou importer les UXSP Windows dans le référentiel. Les UXSP Windows contiennent des pilotes de périphérique Windows pour les versions Windows prises en charge et pour les serveurs Lenovo prenant en charge Windows. Les UXSP doivent être disponibles dans le référentiel afin que vous puissiez mettre à jour les pilotes de périphérique Windows sur les serveurs gérés.

Avant de commencer

Assurez-vous que tous les ports requis et toutes les adresses Internet sont disponibles avant de tenter de télécharger UpdateXpress System Packs (UXSPs). Pour plus d'informations, voir Disponibilité de port et Pare-feux et serveurs proxy dans la documentation en ligne de XClarity Administrator.

Pour télécharger UXSPs à l'aide de XClarity Administrator, assurez-vous que XClarity Administrator est connecté à Internet.

Internet Explorer et les navigateurs web Microsoft Edge ont une limite de téléchargement de 4 Go. Si le fichier que vous importez est supérieur à 4 Go, envisagez d'utiliser un autre navigateur web (par exemple, Chrome ou Firefox).

À propos de cette tâche

XClarity Administrator doit être connecté à Internet pour actualiser le catalogue et télécharger les UXSPs. Si XClarity Administrator n'est pas connecté à Internet, vous pouvez télécharger manuellement les fichiers sur un poste de travail disposant d'un accès réseau à l'hôte XClarity Administrator à l'aide d'un navigateur Web, puis importer ces mises à jour dans le référentiel des mises à jour de microprogramme.

Vous pouvez déterminer si des UXSPs sont stockés dans le référentiel depuis la colonne **État du téléchargement** sur la page Mises à jour de pilote Windows : Référentiel. Cette colonne contient les valeurs suivantes :

- **Téléchargé**. Tous les pilotes des UXSP ou le pilote de périphérique individuel est téléchargé dans le référentiel.
- *x* **sur** *y* **téléchargés**. Une partie seulement des pilotes de périphérique dans les UXSP sont téléchargés dans le référentiel. Les nombres entre parenthèses indiquent le nombre de pilotes de périphérique disponibles et le nombre de pilotes de périphérique téléchargés.
- **Non téléchargé**. Le UXSP ou le pilote de périphérique individuel est disponible sur le site du support Lenovo, mais non téléchargé dans le référentiel.

Un message s'affiche sur la page Référentiel des mises à jour de pilote Windows lorsque l'espace qui est disponible pour UXSPs et les pilotes de périphérique est supérieur à 50 %. Un autre message s'affiche sur la page lorsque le niveau de remplissage du référentiel est supérieur à 85 %. Pour réduire l'espace utilisé dans le référentiel, vous pouvez retirer les fichiers inutilisés en sélectionnant les fichiers cibles puis en cliquant sur l'icône **Supprimer** ( ). Pour plus d'informations, voir Gestion de l'espace disque.

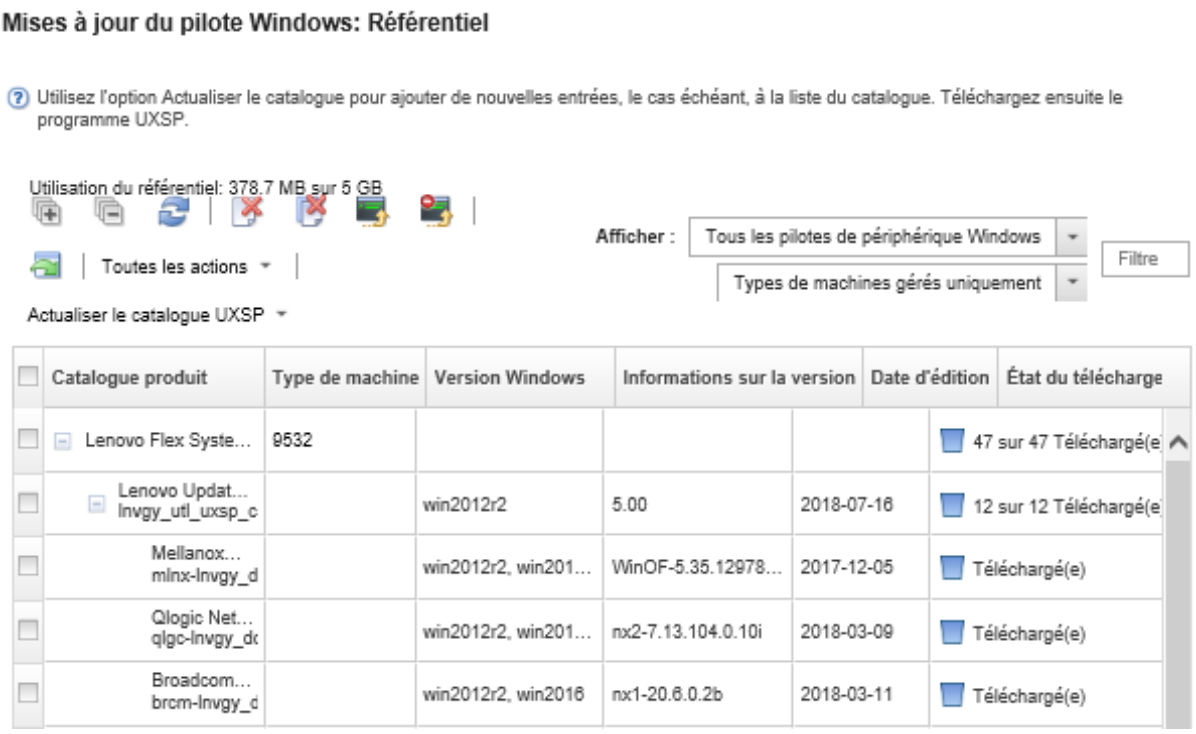
Attention : Les UXSPs Windows incluent des pilotes de périphérique et des mises à jour de microprogramme. Les mises à jour de microprogramme dans les UXSPs Windows sont supprimés lorsque les UXSPs sont importés dans le référentiel et un message d'avertissement s'affiche. Seuls les pilotes de périphérique sont importés.

Procédure

Pour télécharger les UXSPs et des pilotes de périphérique spécifiques, exécutez l'une des procédures suivantes.

- Lorsque XClarity Administrator est connecté à Internet :
  1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Mises à jour de pilotes Windows : Référentiel** pour afficher la page Mises à jour de pilotes Windows : Référentiel.
  2. Cliquez sur **Actualiser le catalogue**, puis cliquez sur l'une des options suivantes pour obtenir des informations sur les derniers UXSPs disponibles.
     - **Actualiser les éléments sélectionnés - Les éléments les plus récents uniquement**. Extrait des informations sur les dernières versions des UXSP disponibles uniquement pour les serveurs sélectionnés.
     - **Actualiser tout - Les éléments les plus récents uniquement**. Extrait des informations sur les dernières versions des UXSP pour tous les serveurs pris en charge.
     - **Actualiser les éléments sélectionnés**. Extrait des informations sur toutes les versions des UXSP disponibles uniquement pour les serveurs sélectionnés.
     - **Actualiser tout**. Extrait des informations sur toutes les versions des UXSP disponibles uniquement pour tous les serveurs pris en charge.

     Remarque : L'actualisation du catalogue peut durer plusieurs minutes.
  3. Développez le type de serveur pour afficher la liste des UXSPs disponibles. Développez les UXSP pour afficher une liste des pilotes de périphérique disponibles.



4. Sélectionnez un ou plusieurs UXSPs cible et pilotes de périphérique à télécharger.
5. Cliquez sur l'icône **Télécharger la sélection** ( ).
6. Cliquez sur **Télécharger** pour télécharger immédiatement, ou cliquez sur **Planning** pour planifier ce téléchargement pour une exécution ultérieure.

   Le téléchargement des UXSPs peut durer quelques minutes. Une fois les UXSPs et les pilotes de périphérique téléchargés et stockés dans le référentiel, la ligne du catalogue produit est mise en évidence et la colonne **État du téléchargement** contient la valeur « Téléchargé ».

   Vous pouvez surveiller l'état du processus de téléchargement en consultant le journal des travaux. Dans le menu XClarity Administrator, cliquez sur **Surveillance → Travaux**. Pour plus d'informations sur le journal des travaux, voir Surveillance des travaux.

- Lorsque XClarity Administrator n'est *pas* connecté à Internet :
  1. Téléchargez les UXSPs sur un poste de travail disposant d'une connexion réseau à l'hôte XClarity Administrator depuis le Site Web Assistance centre de données Lenovo.
  2. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Mises à jour de pilotes Windows : Référentiel** pour afficher la page Mises à jour de pilotes Windows : Référentiel.
  3. Cliquez sur l'icône **Importer** ( ).
  4. Cliquez sur **Sélectionner des fichiers** et recherchez l'emplacement des UXSP sur le poste de travail.
  5. Sélectionnez le fichier .zip UXSP (ne décompressez pas le fichier zip avant d'importer), puis cliquez sur **Ouvrir**.

     Le fichier.zip UXSP contient le fichier de métadonnées (.xml), le contenu (.exe), le fichier historique des modifications (.chg) et le fichier readme (.txt).
  6. Cliquez sur **Importer**.

     Vous pouvez surveiller l'état du processus d'importation en consultant le journal des travaux. Dans le menu XClarity Administrator, cliquez sur **Surveillance → Travaux**. Pour plus d'informations sur le journal des travaux, voir Surveillance des travaux.

Après avoir terminé

Depuis cette page, vous pouvez exécuter les actions suivantes sur les UXSPs sélectionnés.

- Annulez un téléchargement qui est actuellement en cours en cliquant sur l'icône **Annuler les téléchargements** ().
- Supprimez tous les fichiers associés à l'UXSP en cliquant sur l'icône **Supprimer** ().

Configuration de Windows Server pour les mises à jour de pilote de périphérique SE

Lenovo XClarity Administrator utilise le service WinRM (Windows Remote Management) qui écoute via HTTPS ou HTTP pour exécuter des commandes de mise à jour du pilote de périphérique sur les systèmes Windows cibles. Ce service WinRM doit être configuré correctement sur les serveurs cible avant de tenter de mettre à jour les pilotes de périphérique SE.

Avant de commencer

Les ports requis doivent être disponibles. Pour plus d'informations, voir Disponibilité de port dans la documentation en ligne de XClarity Administrator.

Pour plus d'informations sur la configuration de Windows Server avant la mise à jour d'un pilote de périphérique SE, voir Préparation de XClarity Administrator pour des mises à jour de pilote (livre blanc).

Procédure

Pour configurer Windows Server pour la prise en charge de la mise à jour des pilotes de périphérique SE, procédez comme suit.

- **Pour HTTPS**
  1. Connectez-vous et installez un certificat de serveur sur chacun des systèmes Windows cibles.

     Important : Le certificat doit contenir les informations suivantes.

     – Dans l'objet, vérifiez que le composant de domaine est défini (par exemple, DC=labs, DC=com, DC=company).

     – Dans l'autre nom de sujet, vérifiez que le nom DNS et l'hôte et l'adresse IP sont définis (par exemple, DNS Name=node1325C554A6F.labs.company.com et IP Address=10.245.43.149).
  2. Configurez les commandes et les données de gestion à distance via une connexion HTTPS en exécutant l'une des commandes suivantes à partir d'une invite de commande d'administration et confirmez les modifications de configuration suggérées.

     –
     ```
     winrm quickconfig -transport:https
     ```

     –
     ```
     winrm create winrm/config/Listener?Address=*+Transport=HTTPS
     @{Hostname="host_name";CertificateThumbprint="certificate_thumbprint"}
     ```

     Pour configurer manuellement un récepteur HTTPS WinRM en fonction de la documentation de WinRM, voir Comment configurer la page Web de HTTPS WinRM.
  3. Activez l'authentification de base des utilisateurs Windows locaux en exécutant la commande suivante à partir d'une invite de commande d'administration.
     ```
     winrm set winrm/config/service/Auth @{Basic="true"}
     ```

4. Pour éviter un possible dépassement de délai d'attente et l'envoi d'erreurs de requêtes WinRM dans le cadre de la vérification de la conformité et de la mise en œuvre des mises à jour de pilote, augmentez la valeur par défaut du délai de réponse de WinRM en exécutant la commande suivante à partir d'une invite de commande avec droits d'administration. Une valeur de 280000 est recommandée. Pour plus d'informations, voir le document Guide d'installation et de configuration pour la page Web Windows Remote Management.
   ```
   winrm set winrm/config @{MaxTimeoutms="280000"}
   ```
5. Ouvrez le port dans le pare-feu que vous avez configuré pour le programme d'écoute HTTPS WinRM. Le port HTTPS par défaut est 5986. Par exemple
   ```
   netsh advfirewall firewall add rule name="Windows Remote Management (HTTPS-In)" dir=in action=allow
   protocol=TCP localport=5986
   ```
6. Si vous utilisez des programmes d'écoute HTTPS, ajoutez le certificat du fichier de clés certifiées XClarity Administrator en procédant comme suit. L'ajout du certificat au fichier de clés certifiées permet à XClarity Administrator de faire confiance aux programmes d'écoute HTTPS WinRM auxquels il se connecte. Répétez les étapes suivantes pour les chemins de certification supplémentaires qui doivent être sécurisés pour le service Windows Remote Management.
   a. Identifiez et collectez le certificat racine d'Autorité de certification que vous avez utilisé pour la connexion aux certificats de serveur pour les systèmes Windows cibles. Si vous n'avez accès au certificat racine CA, collectez le certificat du serveur lui-même ou un autre certificat dans le chemin de certification.
   b. Dans la barre de menu de XClarity Administrator, cliquez sur **Administration → Sécurité** pour afficher la page Sécurité.
   c. Cliquez sur **Certificats sécurisés** sous la section Gestion des certificats.
   d. Cliquez sur l'icône **Créer** ( ) pour afficher la boîte de dialogue Ajouter un certificat.
   e. Recherchez le fichier de certificat que vous avez collecté à l'étape 1, ou copiez/collez le contenu du fichier de certificat dans la zone de texte.
   f. Cliquez sur **Créer**.
7. Une fois le programme d'écoute WinRM en cours d'exécution sur les systèmes cibles Windows, XClarity Administrator peut se connecter à ces systèmes et effectuer les mises à jour de pilote de périphérique.

- **Pour HTTP**
  1. Configurez les commandes et les données de gestion à distance via une connexion HTTP en exécutant la commande suivante à partir d'une invite de commande d'administration et confirmez les modifications de configuration suggérées.
     ```
     winrm quickconfig
     ```
  2. Activez l'authentification de base des utilisateurs Windows locaux en exécutant la commande suivante à partir d'une invite de commande d'administration.
     ```
     winrm set winrm/config/service/Auth @{Basic="true"}
     ```
  3. Allouez suffisamment de mémoire pour les commandes de mise à jour sur le système en exécutant la commande suivante à partir d'une invite de commande d'administration.
     ```
     winrm set winrm/config/winrs @{MaxMemoryPerShellMB="1024"}
     ```
  4. Autorisez les données non chiffrées en exécutant la commande suivante à partir d'une invite de commande d'administration.
     ```
     winrm set winrm/config/service @{AllowUnencrypted="true"}
     ```
  5. Ouvrez le port dans le pare-feu que vous avez configuré pour le programme d'écoute HTTP WinRM. Le port HTTPS par défaut est 5985. Par exemple
     ```
     netsh advfirewall firewall add rule name="Windows Remote Management (HTTP-In)" dir=in action=allow
     protocol=TCP localport=5985
     ```

  Une fois le programme d'écoute WinRM en cours d'exécution sur les systèmes cibles Windows, XClarity Administrator peut se connecter à ces systèmes et effectuer les mises à jour de pilote de périphérique.

Configuration d'un compte de domaine pour les mises à jour de pilotes de périphérique S.E.

Vous pouvez choisir d'utiliser des comptes de domaine pour gérer facilement les privilèges avec un contrôleur de domaine. Pour utiliser un compte de domaine lors de la mise à jour des pilotes de périphérique S.E, vous devez configurer un compte de domaine.

Avant de commencer

Assurez-vous que les serveurs Windows gérés sont dans un réseau de domaine avant de configurer des comptes de domaine.

Lorsque vous ajoutez le compte utilisateur Windows dans Lenovo XClarity Administrator, utilisez le format `USER@DOMAIN`. Le format `DOMAIN/USER` n'est pas supporté.

Procédure

Pour configurer un compte de domaine, procédez comme suit.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Distribution → Mises à jour de pilote Windows : Appliquer**. La page Mises à jour de pilote Windows : Appliquer s'affiche.

Etape 2. Cliquez sur **Toutes les actions → Gérer le compte de domaine**. La page comptes de domaine s'affiche.

Etape 3. Cliquez sur l'icône **Créer** ( ). Pour ajouter un domaine au compte de domaine. La boîte de dialogue Créer un domaine s'affiche.

Etape 4. Indiquez un nom et un ou plusieurs noms d'hôtes du centre de distribution clé pour le domaine. Utilisez l'icône ( ) **Ajouter** pour ajouter un autre nom d'hôte et utiliser l'icône ( ) **Retirer** pour le retirer.

Etape 5. Cliquez sur **OK** pour enregistrer le domaine.

Etape 6. Dans la page Comptes de domaine, sélectionnez éventuellement le domaine à utiliser par défaut.

Etape 7. Cliquez sur **Enregistrer** pour enregistrer la configuration.

Après avoir terminé

Depuis la page Configurer un Compte de domaine, vous pouvez effectuer les actions suivantes.

- Modifiez un domaine sélectionné en cliquant sur l'icône ( ) **Éditer**.
- Supprimez un domaine sélectionné en cliquant sur l'icône ( ) **Supprimer**.

Configuration des paramètres globaux de mise à jour de pilote de périphérique Windows

Les paramètres globaux sont utilisés en tant que paramètres par défaut lorsque des mises à jour de pilote de périphérique Windows sont appliquées.

À propos de cette tâche

La page Paramètres globaux vous permet de configurer les paramètres suivants :
- Utiliser HTTPS pour les mises à jour de pilote Windows
- Afficher les pilotes de périphérique pour le matériel installé

Procédure

Pour configurer les paramètres globaux à utiliser pour tous les serveurs, procédez comme suit.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Distribution → Mises à jour de pilote Windows : appliquer**. La page Mises à jour de pilote Windows : appliquer s'affiche.

Etape 2. Cliquez sur **Toutes les actions → Paramètres globaux** pour afficher la boîte de dialogue Paramètres globaux : appliquer les mises à jour de pilote Windows.

Etape 3. Vous pouvez aussi sélectionner l'une des options suivantes.

- Sélectionnez **Utiliser HTTPS pour les mises à jour de pilote Windows** pour utiliser le service WinRM (Windows Remote Management) qui écoute via HTTPS pour exécuter des commandes de mise à jour du pilote de périphérique sur les systèmes Windows cibles. HTTP est la valeur par défaut.

  Désélectionnez ce paramètre pour utiliser HTTP.

  Attention : Lors de l'utilisation de HTTP, les données d'identification utilisateur Windows sont envoyées sur le réseau *sans* chiffrement et elles peuvent être facilement affichées à l'aide d'outils de dépannage réseau couramment disponibles.
- Sélectionnez **Afficher les pilotes de périphérique pour le matériel installé** pour répertorier uniquement les pilotes de périphérique pour le matériel géré.

  Désélectionnez ce paramètre pour répertorier tous les pilotes de périphérique dans chaque UpdateXpress System Packs (UXSPs) importé.

  Important : Après avoir sélectionné cette option, vous devez effectuer une vérification de conformité en cliquant sur l'icône **Vérifier la conformité** ( ) à la page Mises à jour de pilote Windows : Appliquer.

Etape 4. Cliquez sur **OK** pour fermer la boîte de dialogue.

Application de pilotes de périphérique Windows

Vous pouvez appliquer des pilotes de périphérique sur des serveurs gérés exécutant Windows.

Avant de commencer

- Module Lenovo XClarity Administrator utilise le service WinRM (Windows Remote Management) qui écoute via HTTPS ou HTTP pour exécuter des commandes de mise à jour du pilote de périphérique sur les systèmes Windows cibles. Ce service WinRM doit être configuré correctement sur les serveurs cible avant de tenter de mettre à jour les pilotes de périphérique SE (voir Configuration de Windows Server pour les mises à jour de pilote de périphérique SE).
- Les appareils qui ne sont pas pris en charge ne peuvent pas être sélectionnés pour les mises à jour.

- Prenez connaissance des remarques relatives à la mise à jour du pilote de périphérique avant de tenter de mettre à jour les pilotes de périphérique sur vos serveurs gérés (voir Instructions de mise à jour du pilote de périphérique SE).
- Assurez-vous que le référentiel contient les UXSPs et les pilotes de périphérique que vous souhaitez déployer (voir Téléchargement des pilotes de périphérique Windows).

  Remarque : À l'origine, lorsque XClarity Administrator est installé, le catalogue et le référentiel sont vides.
- XClarity Administrator peut utiliser le service WinRM (Windows Remote Management) qui écoute via HTTPS ou HTTP pour exécuter des commandes de mise à jour du pilote de périphérique sur les systèmes Windows cibles. HTTP est la valeur par défaut. Pour utiliser HTTP, cliquez sur **Toutes les actions → Paramètres globaux** sur la page Mises à jour de pilote Windows : Appliquer, puis désélectionnez **Utiliser HTTPS pour les mises à jour de pilote Windows**.

  Attention : Lors de l'utilisation de HTTP, les données d'identification utilisateur Windows sont envoyées sur le réseau *sans* chiffrement et elles peuvent être facilement affichées à l'aide d'outils de dépannage réseau couramment disponibles.

  Important :

  – Vérifiez que Windows Remote Management (WinRM) sur le serveur cible est configuré pour l'utilisation du même paramètre (HTTPS ou HTTP) qui est défini dans XClarity Administrator (voir Configuration de Windows Server pour les mises à jour de pilote de périphérique SE).

  – Assurez-vous que WinRM sur le serveur cible est configuré avec l'authentification de base.

  – Lors de l'utilisation de HTTPS, assurez-vous que WinRM sur le serveur cible est configuré avec **allowUnencrypted=false**.
- Vérifiez que PowerShell est pris en charge sur le serveur cible.
- Vérifiez que le serveur cible est sous tension avant d'essayer de mettre à jour les pilotes de périphérique. Si le serveur n'est pas sous tension, sélectionnez le serveur cible, puis cliquez sur **Toutes les actions → Actions d'alimentation → Mettre sous tension**.
- Vérifiez que XClarity Administrator dispose des informations dont il a besoin pour accéder au système d'exploitation hôte (voir Gestion de l'accès aux systèmes d'exploitation sur les serveurs gérés.
- Si vous souhaitez utiliser un compte de domaine lors de la mise à jour des pilotes de périphérique S.E., assurez-vous d'avoir créé le fichier de configuration requis (voir Configuration d'un compte de domaine pour les mises à jour de pilotes de périphérique S.E.).
- Assurez-vous qu'aucun travail n'est en cours d'exécution sur le serveur cible. Vous ne pouvez pas mettre à jour les pilotes de périphérique sur un serveur géré qui est verrouillé par un travail en cours d'exécution. Si un autre travail de mise à jour est en cours d'exécution sur le serveur cible, ce travail de mise à jour est mis en file d'attente jusqu'à ce que le travail de mise à jour en cours soit terminé. Pour afficher la liste des travaux actifs, cliquez sur **Surveillance → Travaux**.

À propos de cette tâche

XClarity Administrator met à jour uniquement les pilotes de périphérique qui ne sont pas conformes. Les pilotes de périphérique ne sont pas conformes lorsque la version sur le serveur est antérieure à la version dans les UXSP sélectionnés. Les pilotes de périphérique qui sont égaux ou postérieurs à la version des UXSP sélectionnés sont ignorés.

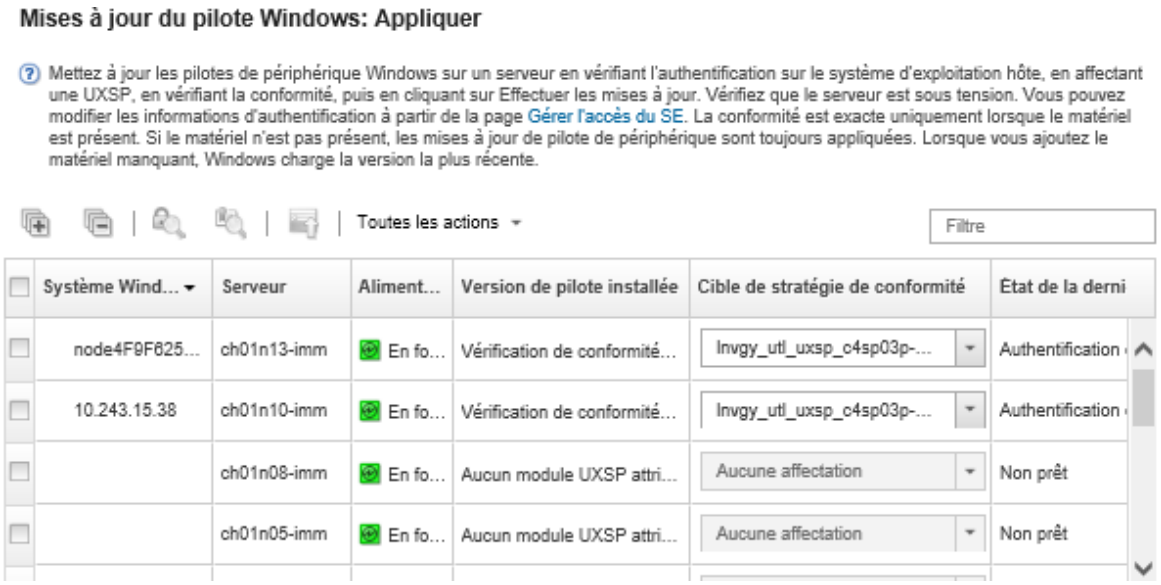
Procédure

Pour appliquer des pilotes de périphérique Windows à des serveurs gérés, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Mises à jour de pilote : Appliquer** pour afficher la page Mises à jour de pilote : Appliquer.

Important :

- Pour reconnaître les pilotes de périphérique sur le serveur cible et déterminer leur conformité, vous devez sélectionner le serveur cible et exécuter la vérification de conformité. Lorsque la vérification de conformité est exécutée pour la première fois, vous pouvez étendre la ligne pour afficher la liste des pilotes de périphérique sur le serveur cible.
- La colonne **Système Windows** identifie le nom d'hôte ou l'adresse IP du système d'exploitation hôte.
- La colonne **Serveur** identifie le nom et l'adresse IP du serveur géré.



Etape 2. Sélectionnez un ou plusieurs serveurs cible et pilotes de périphérique.

Vous pouvez trier les colonnes du tableau afin de faciliter la recherche de serveurs spécifiques. En outre, vous pouvez filtrer la liste des serveurs affichés en entrant du texte (par exemple, un nom ou une adresse IP) dans la zone **Filtre**.

Astuce :

- Vous pouvez choisir de mettre à jour tous les pilotes de périphérique d'un système d'exploitation spécifique, ou vous pouvez développer un système d'exploitation et choisir de mettre à jour des appareils spécifiques
- La colonne **Etat de mise à jour** affiche l'état d'authentification pour chaque serveur et l'état de mise à jour pour chaque pilote de périphérique.
- La colonne des **données d'identification du système d'exploitation** affiche les données d'identification stockées qui sont utilisée pour l'authentification auprès du système d'exploitation (par exemple, « 901 – company\USER1. »

  Si les données d'identification SE ne sont pas définies pour le système d'exploitation hôte sur le serveur cible, la boîte de dialogue Editer les données d'identification SE s'affiche. Pour un serveur cible unique, indiquez le nom d'utilisateur et le mot de passe que vous souhaitez utiliser pour cette opération. Pour plusieurs serveurs cible, sélectionnez les données d'identification stockées à utiliser pour chaque serveur. Cliquez ensuite sur **Enregistrer**.

Remarque : Les données d'identification SE que vous sélectionnez dans la boîte de dialogue Editer les données d'identification SE ne sont pas sauvegardées pour le système d'exploitation hôte. Pour sauvegarder les données d'identification SE, voir Gestion de l'accès aux systèmes d'exploitation sur les serveurs gérés.

Etape 3. Cliquez sur l'icône **Vérifier authentification** () pour exécuter les tests d'authentification et des prérequis.

XClarity Administrator se connecte au système d'exploitation à l'aide des données d'identification stockées qui figurent dans la colonne **Données d'identification SE**, détermine la version SE, vérifie que WinRM est activé, effectue des vérifications de prérequis supplémentaires, puis se déconnecte du SE hôte.

Pour plus d'informations sur les données d'identification stockées pour le système d'exploitation hôte, consultez Gestion de l'accès aux systèmes d'exploitation sur les serveurs gérés.

Etape 4. Pour chaque serveur cible, sélectionnez l'UXSP cible que vous souhaitez utiliser pour mettre à jour les pilotes de périphérique à partir de la colonne **Cible de conformité**.

Etape 5. Sélectionnez à nouveau les serveurs cible, puis cliquez sur l'icône **Vérifier la conformité** () afin de vérifier la conformité de chaque pilote de périphérique.

La vérification de conformité met à jour l'état de conformité dans la colonne **Version de pilote installée**. Cette colonne affiche l'état de conformité global pour le serveur et l'état de la version installée et de la conformité pour chaque pilote de périphérique, tels que mesurés sur les UXSP affectés.

-  **Conforme**. Le pilote de périphérique installé est égal à postérieur à la version de l'UXSP affecté.
-  **Non compatible**. Le pilote de périphérique installé est antérieur à la version de l'UXSP affecté. Vous pouvez cliquer sur le lien pour obtenir plus d'informations sur la non conformité.

Remarque : La conformité du pilote de périphérique est exacte lorsque le matériel est présent. Si le matériel n'est pas présent, les pilotes de périphérique sont toujours appliqués au serveur. Lorsque vous ajoutez le matériel manquant au serveur, Windows charge la version la plus récente.

Etape 6. Cliquez sur l'icône **Effectuer les mises à jour** ().

Etape 7. Sélectionnez l'une des règles de mise à jour.

- **Arrêter toutes les mises à jour en cas d'erreur**. Si une erreur se produit lors de la mise à jour d'un des pilotes de périphérique sur un appareil cible, le processus de mise à jour s'arrête pour tous les appareils cible dans le travail de mise à jour du pilote de périphérique en cours. Dans ce cas, aucune des mises à jour de pilote de périphérique de l'UXSP pour l'appareil cible n'est appliquée. Le pilote de périphérique actuellement installé sur tous les appareils cibles reste en vigueur.
- **Continuer en cas d'erreur**. Si une erreur se produit lors de la mise à jour de l'un des pilotes de périphérique sur l'appareil cible, le processus de mise à jour ne met pas à jour le pilote de périphérique de l'appareil concerné ; toutefois, le processus de mise à jour continue de mettre à jour les autres pilotes de périphérique sur l'appareil et de mettre à jour tous les autres appareils cibles dans le travail de mise à jour des pilotes de périphérique en cours.
- **Passer au système suivant en cas d'erreur**. Si une erreur se produit lors de la mise à jour de l'un des pilotes de périphérique sur l'appareil, le processus de mise à jour arrête toutes les tentatives de mise à jour des pilotes de périphérique pour cet appareil spécifique, de sorte que les pilotes de périphérique actuellement installés sur celui-ci restent en vigueur. Le processus

de mise à jour continue de mettre à jour tous les autres appareils du travail de mise à jour de pilote de périphérique.

Etape 8. Cliquez sur **Effectuer les mises à jour** pour mettre à jour immédiatement, ou cliquez sur **Planning** pour planifier cette mise à jour pour une exécution ultérieure.

Après avoir terminé

Lors de l'application d'une mise à jour, si le serveur cible ne passe pas en mode de maintenance, essayez à nouveau d'appliquer la mise à jour.

Si des mises à jour n'ont pas abouti, voir Instructions de mise à jour du pilote de périphérique SE pour savoir comment identifier et résoudre les problèmes.

Depuis la page Mises à jour de pilote Windows : Appliquer, vous pouvez effectuer les actions suivantes.

- Visualiser l'état de la mise à jour de pilote de périphérique directement à partir de la page Appliquer dans la colonne **État de mise à jour**.
- Surveiller l'état du processus de mise à jour du pilote de périphérique en consultant le journal des travaux. Dans le menu XClarity Administrator, cliquez sur **Surveillance → Travaux**.

  Pour plus d'informations sur le journal des travaux, voir Surveillance des travaux.

  Lorsque le travail de mise à jour est terminé, vous pouvez vérifier que les appareils sont conformes à partir de la page Mises à jour du pilote Windows : Appliquer. La version de pilote en cours qui est active sur chaque appareil est répertoriée dans la colonne **Version de pilote installée**.

Chapitre 15. Installation de systèmes d’exploitation sur des serveurs nus

Vous pouvez utiliser Lenovo XClarity Administrator pour gérer le Référentiel d'images SE et déployer des images du système d'exploitation sur un maximum de 28 serveurs nus simultanément.

En savoir plus :

- XClarity Administrator : du serveur au cluster
- XClarity Administrator : déploiement du système d'exploitation

Avant de commencer

Au bout de la période d'essai de 90 jours, vous pouvez continuer à utiliser XClarity Administrator pour gérer et surveiller votre matériel sans frais ; vous devez cependant acheter des licences d'activation de l'ensemble des fonctionnalités pour chaque serveur géré qui prend en charge les fonctionnalités avancées XClarity Administrator afin de continuer à utiliser la fonction de déploiement SE. Lenovo XClarity Pro fournit l'accès au service et au support, ainsi qu'une licence d'activation des fonctionnalités complètes. Pour plus d’informations sur l’achat de Lenovo XClarity Pro, contactez votre représentant Lenovo ou votre partenaire commercial agréé. Pour plus d'informations, voir Installation de la licence d'activation de l'ensemble des fonctionnalités dans la documentation en ligne de XClarity Administrator.

À propos de cette tâche

XClarity Administrator simplifie le déploiement d'images de systèmes d'exploitation sur des serveurs *nus*, sur lesquels un système d'exploitation n'a généralement pas été installé.

Attention : Si vous déployez un système d’exploitation sur un serveur doté d'un système d’exploitation, XClarity Administrator effectue une nouvelle installation qui remplace les partitions sur les disques cible

Plusieurs facteurs déterminent le temps nécessaire au déploiement d'un système d'exploitation sur un serveur :

- La quantité de mémoire RAM installée sur le serveur, qui affecte le délai d'amorçage du serveur.
- Le nombre et les types de cartes d’E-S qui sont installées sur le serveur, ce qui affecte le temps nécessaire à XClarity Administrator pour l'exécution d'un inventaire du serveur. Cela affecte également le temps nécessaire à l'amorçage du microprogramme UEFI une fois le serveur démarré. Lors du déploiement d'un système d'exploitation, le serveur redémarre plusieurs fois.
- Le trafic réseau. XClarity Administrator télécharge l'image du système d'exploitation via le réseau de données ou le réseau de déploiement du système d'exploitation.
- La configuration matérielle de l'hôte sur lequel le dispositif virtuel Lenovo XClarity Administrator est installé. La quantité de mémoire RAM, le nombre de processeurs et le stockage sur disque dur peuvent affecter les temps de téléchargement.

Important : Si vous souhaitez déployer une image du système d’exploitation à partir de XClarity Administrator, au moins l’une des interfaces XClarity Administrator (Eth0 ou Eth1) doit disposer d’une connectivité réseau IP à l’interface réseau du serveur qui est utilisée pour accéder au système d’exploitation hôte. Le déploiement du système d'exploitation utilise l'interface définie à la page Accès réseau. Pour plus d'informations sur les paramètres réseau, voir Configuration de l'accès réseau.

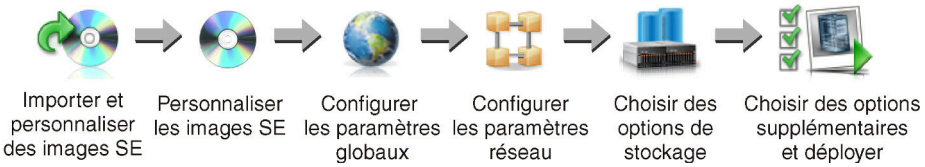
Avant d'exécuter un déploiement de système d'exploitation nu sur un serveur, préparez le serveur en mettant à jour le microprogramme aux niveaux les plus récents et en configurant le serveur à l'aide de Modèles de

configuration. Pour plus d'informations, voir Mise à jour du microprogramme sur les appareils gérés, Configuration des serveurs à l'aide de modèles de configuration.

Attention : Il est recommandé de *ne pas* utiliser XClarity Administrator pour exécuter un déploiement de système d'exploitation nu sur les dispositifs Converged et ThinkAgile.

Procédure

La figure suivante illustre le flux de travaux relatif au déploiement d'une image SE sur un serveur.



Etape 1. **Importez des images SE.**

Avant de pouvoir déployer une image SE sur un serveur, vous devez d'abord importer le système d'exploitation dans le référentiel. Lorsque vous importez une image SE, XClarity Administrator:

- Vérifie qu'il existe suffisamment d'espace dans Référentiel d'images SE avant d'importer le système d'exploitation. Si vous n'avez pas suffisamment d'espace pour importer une image, supprimez une image existante dans le référentiel, puis essayez de réimporter la nouvelle image.
- Crée un ou plusieurs profils de cette image et stocke le profil dans Référentiel d'images SE. Chaque *profil* comprend les options d'installation et d'image SE. Pour plus d'informations sur les profils d'image SE prédéfinis, voir Profils d'image de système d'exploitation.

Un *système d'exploitation de base* est l'image SE qui a été importée dans le référentiel d'images SE. L'image de base importée contient des profils prédéfinis qui décrivent les configurations d'installation pour cette image. Vous pouvez créer des profils personnalisés dans l'image SE de base qui peut être déployée pour des configurations spécifiques.

Vous pouvez également importer des *systèmes d'exploitation personnalisés* pris en charge. Cette image personnalisée contienne un profil de marque de réservation prédéfini, qui ne peut pas être déployé. Vous devez importer un profil personnalisé qui peut être déployé, ou créer vos propres profils personnalisés à partir du profil de marque de réservation. Une fois le profil personnalisé ajouté, il se peut que le profil de marque de réservation soit retiré automatiquement.

Pour Microsoft Windows Server 2016 et 2019, vous pouvez importer une image de système d'exploitation personnalisée pour chaque version. L'image de base importée contient des profils prédéfinis qui décrivent les configurations d'installation pour cette image. Vous ne pouvez pas créer de profils personnalisés dans l'image SE personnalisée.

Pour obtenir la liste des systèmes d'exploitation de base et personnalisés pris en charge, voir Systèmes d'exploitation pris en chargeSystèmes d'exploitation pris en charge dans la documentation en ligne de Lenovo XClarity Administrator.

Etape 2. **(Facultatif) Personnalisez l'image SE.**

Vous pouvez personnaliser une image SE en ajoutant des pilotes de périphérique, des fichiers d'amorçage (pour Windows seulement), des paramètres de configuration, des fichiers sans opérateur, des scripts de post-installation et des logiciels. Lorsque vous personnalisez un image SE, XClarity Administrator crée un profil d'image SE personnalisé qui contient les fichiers personnalisés et les options d'installation.

Le référentiel des images SE peut stocker un nombre illimité de fichiers prédéfinis et personnalisés, si l'espace disponible est suffisant pour stocker les fichiers.

Etape 3. **Configurez les paramètres globaux.**

Les paramètres globaux sont des options de configuration qui servent de valeurs par défaut pour le déploiement du système d'exploitation. Vous pouvez configurer les paramètres globaux suivants.

- Le mot de passe du compte utilisateur administrateur à utiliser pour le déploiement des systèmes d'exploitation
- La méthode à utiliser pour affecter des adresses IP aux serveurs
- Les clés de licence à utiliser lors de l'activation des systèmes d'exploitation installés
- Associer éventuellement un domaine Active Directory dans le cadre du déploiement de système d'exploitation Windows

Etape 4. **Configurez les paramètres réseau.**

Vous pouvez spécifier les paramètres réseau pour chaque serveur sur lequel doivent être déployés des systèmes d'exploitation.

Si vous utiliser DHCP pour affecter dynamiquement les adresses IP, vous devez configurer les adresses MAC.

Si vous utilisez des adresses IP statiques, vous devez configurer les paramètres réseau suivants pour un serveur spécifique, avant de pouvoir déployer un système d'exploitation sur ce serveur. Une fois ces paramètres configurés, l'état de déploiement du serveur est modifié à « Prêt. » (Notez que certaines zones ne sont pas disponibles pour les adresses IPv6 statiques.)

- Nom d'hôte

  Le nom d'hôte doit également respecter les règles suivantes :
  - Le nom d'hôte de chaque serveur géré doit être unique.
  - Le nom d'hôte peut contenir des chaînes (étiquettes) qui sont séparées par un point (.).
  - Chaque étiquette peut contenir des lettres ASCII, des chiffres et des tirets (-). Toutefois, la chaîne ne peut ni commencer ni se terminer par un tiret, et ne peut pas contenir uniquement des chiffres.
  - La première étiquettes doit contenir de 2 à 15 caractères. Les étiquettes suivantes doivent contenir de 2 à 63 caractères.
  - La longueur totale du nom d'hôte ne doit pas dépasser 255 caractères.
- Adresse MAC du port sur l'hôte sur lequel le système d'exploitation doit être installé.

  L'adresse MAC est définie à AUTO par défaut. Ce paramètre détecte automatiquement les ports Ethernet qui peuvent être configurés et utilisés pour le déploiement. La première adresse MAC (port) qui est détectée est utilisée par défaut. Si la connectivité est détectée sur un adresse MAC différente, l'hôte XClarity Administrator est automatiquement redémarré pour utiliser l'adresse MAC nouvellement détectée pour le déploiement.

  Vous pouvez déterminer l'état du port d'adresse MAC utilisé pour le déploiement SE en accédant au menu déroulant **Adresse MAC** de la boîte de dialogue Paramètres réseau. Si plusieurs ports sont activés ou si tous les ports sont arrêtés, AUTO est utilisé par défaut.

  Remarques :

  - Les ports réseau virtuels ne sont pas pris en charge. N'utilisez pas un port réseau physique pour simuler plusieurs ports réseau virtuels.

  - Lorsque le paramètre réseau du serveur est défini sur AUTO, XClarity Administrator peut détecter automatiquement les ports réseau dans les emplacements 1 à 16. Au moins un port des emplacements 1 à 16 doit disposer d'une connexion à XClarity Administrator.
  - Si vous souhaitez utiliser un port réseau dans l'emplacement 17 ou supérieur pour l'adresse MAC, vous ne pouvez pas utiliser AUTO. Au lieu de cela, vous devez définir le paramètre réseau du serveur sur l'adresse MAC du port spécifique que vous souhaitez utiliser.
  - Toutes les adresses MAC hôtes ne sont pas affichées pour les serveurs ThinkServer. Dans la plupart des cas, les adresses MAC pour les cartes Ethernet AnyFabric sont listées dans la boîte de dialogue Éditer les paramètres réseau. Les adresses MAC d'autres cartes Ethernet (tels que LAN-on-motherboard) ne sont pas listées. Dans le cas où les adresses MAC ne sont pas disponibles pour une carte, utilisez la méthode AUTO pour les déploiements non VLAN.
- Adresse IP et masque de sous-réseau
- Passerelle IP
- Jusqu'à deux serveurs DNS (Domain Name System)
- Vitesse d'unité MTU (unité de transmission maximale)
- ID VLAN, si le mode IP VLAN est activé

Si vous choisissez d'utiliser les réseaux VLAN, vous pouvez affecter un ID VLAN à la carte réseau qui est en cours de configuration.

Etape 5. **Choisissez les options de stockage.**

Pour chaque déploiement, vous pouvez choisir l'emplacement de stockage préféré sur lequel le système d'exploitation doit être déployé. Suivant le système d'exploitation, vous pouvez choisir d'effectuer le déploiement sur une unité de disque locale, une clé d'hyperviseur imbriqué ou un réseau SAN.

Etape 6. **Choisissez des options supplémentaires et des paramètres de configuration personnalisés, puis déployez l'image SE.**

Vous pouvez configurer d'autres options de déploiement, telles que la clé de licence pour le déploiement SE, ainsi que paramètres de configuration. Si vous installez Microsoft Windows, vous pouvez aussi configurer le domaine Active Directory à rejoindre.

Remarques :

- Si vous avez défini des paramètres de configuration personnalisés pour un profil SE personnalisé spécifique, vous devez définir des valeurs pour les paramètres de configuration de personnalisés requis avant de pouvoir déployer le profil sur un serveur.
- Lors du déploiement d'un profil personnalisé qui inclut les paramètres personnalisés, tous les serveurs cible doivent utiliser le même profil SE personnalisé et les valeurs des paramètres personnalisés s'appliquent à tous les serveurs cible.

Vous pouvez ensuite choisir les serveurs cible pour le déploiement et les images SE à déployer. Gardez à l'esprit que, pour déployer un système d'exploitation, le serveur doit être à l'état de déploiement « Prêt ».

Vous pouvez déployer des images du système d'exploitation sur un maximum de 28 serveurs simultanément.

Avant d'essayer de déployer une image du système d'exploitation, consultez la section Remarques sur le déploiement de systèmes d'exploitation.

Remarques sur le déploiement de systèmes d'exploitation

Avant d'essayer de déployer une image du système d'exploitation, prenez connaissance des remarques suivantes.

Lenovo XClarity Administrator remarques

- Assurez-vous qu'aucun travail n'est en cours d'exécution sur le serveur cible. Pour afficher la liste des travaux actifs, cliquez sur **Surveillance → Travaux**.
- Assurez-vous que le serveur cible ne possède pas un modèle de serveur reporté ou partiellement activé. Si un modèle de serveur a été reporté ou partiellement activé sur le serveur géré, vous devez redémarrer le serveur pour appliquer tous les paramètres de configuration. N'essayez pas de déployer un système d'exploitation sur un serveur doté d'un modèle de serveur partiellement activé. Pour déterminer l'état de la configuration du serveur, voir la zone **État de configuration** sur la page Récapitulatif du serveur géré (voir Affichage des détails d'un serveur géré).
- Assurez-vous que le mot de passe du compte administrateur qui doit être utilisé pour déployer le système d'exploitation est spécifié dans la boîte de dialogue Paramètres globaux : Déployer des systèmes d'exploitation. Pour plus d'informations sur la définition du mot de passe, voir Configuration des paramètres de déploiement SE.
- Assurez-vous que les paramètres par défaut globaux sont corrects pour ce déploiement de système d'exploitation (voir Configuration des paramètres de déploiement SE).

Remarques sur le système d'exploitation

- Vérifiez que vous disposez de toutes les licences de système d'exploitation applicables pour activer les systèmes d'exploitation installés. Il vous incombe de vous procurer les licences directement auprès du fabricant du système d'exploitation.
- Assurez-vous que l'image du système d'exploitation que vous souhaitez déployer est déjà chargée dans le Référentiel d'images SE. Pour plus d'informations sur l'importation d'images, voir Importation d'images du système d'exploitation.
- Des images du système d'exploitation se trouvant dans le référentiel XClarity Administrator peuvent ne pas être prises en charge que sur certaines plateformes matérielles. Seules les images du système d'exploitation qui sont prises en charge par le serveur sélectionné figurent sur la page Déployer des images de SE. Vous pouvez déterminer si un système d'exploitation est compatible avec un serveur donné avec Site Web du guide d'interopérabilité SE Lenovo.
- Pour Windows, vous devez importer un fichier d'amorçage dans le référentiel d'images SE avant de pouvoir déployer un profil Windows. Lenovo regroupe le fichier d'amorçage WinPE_64.wim prédéfini et un ensemble de pilotes de périphérique dans un seul module qui peut être téléchargé depuis page Web des pilotes Windows de Lenovo et référentiel d'images WinPE puis importé dans un référentiel d'images SE. Comme le fichier de lot contient des pilotes de périphérique et des fichiers d'amorçage, vous pouvez l'importer depuis l'onglet **Pilote de périphérique** ou **Fichiers d'amorçage**.
- Pour SLES 15 et 15 SP1, vous devez importer l'image du programme d'installation et l'image package associée depuis Page Web du centre de support pour le serveur du système d'exploitation. Pour SLES 15 SP2 ou version ultérieure, vous devez importer uniquement l'image de support d'installation complète car le programme d'installation unifié et les modules de DVD de SUSE Linux Enterprise Server 15 et 15 SP1 sont obsolètes.
- Pour les serveurs ThinkSystem XClarity Administrator inclut des pilotes de périphérique prêts à l'emploi pour permettre l'installation du système d'exploitation, ainsi qu'un réseau de base et une configuration de stockage pour le système d'exploitation final. Pour les autres serveurs, assurez-vous que l'image du système d'exploitation que vous avez l'intention de déployer inclut les pilotes de périphérique Ethernet, Fibre Channel et d'adaptateur de stockage appropriés pour votre matériel. Si le pilote de périphérique de carte d'E-S n'est pas inclus dans le système d'exploitation, la carte n'est pas prise en charge pour le déploiement de système d'exploitation. Installez toujours le système d'exploitation le plus récent de

manière à disposer des derniers pilotes de périphérique de carte d'E-S et des fichiers d'amorçage requis. Vous pouvez également ajouter des pilotes de périphérique prêts à l'emploi et des fichiers d'amorçage sur les systèmes d'exploitation importés dans XClarity Administrator (voir Personnalisation de profils d'image SE dans la documentation en ligne de XClarity Administrator).

Pour VMware, utilisez la dernière image personnalisée Lenovo pour ESXi, qui inclut la prise en charge des cartes les plus récentes. Pour plus d'informations sur l'obtention de cette image, voir le Support VMware - Site Web de téléchargement.

- Pour les serveurs ThinkSystem, si vous souhaitez déployer SLES 12 SP2, vous devez utilisez un profil kISO. Pour obtenir les profils kISO, vous devez importer l'image kISO appropriée après avoir importé le système d'exploitation SLES de base. Vous pouvez télécharger l'image kISO SLES depuis le Support Linux - Site Web de téléchargement.

  Remarques :

  – L'image kISO SLES compte le nombre maximum d'images SE importées.

    Pour obtenir la liste des systèmes d'exploitation de base et personnalisés pris en charge, voir Systèmes d'exploitation pris en chargeSystèmes d'exploitation pris en charge dans la documentation en ligne de Lenovo XClarity Administrator.

  – Si vous supprimez tous les profils kISO, vous devez supprimer le système d'exploitation SLES de base, puis le réimporter ainsi que l'image kISO pour déployer SLES 12 SP2 vers un serveur ThinkSystem.

  – Si vous créez un profil SE personnalisé basé sur un profil kISO, les pilotes de périphérique prédéfinis dans le système d'exploitation de base ne sont pas inclus. Les pilotes de périphérique qui sont inclus dans le kISO sont utilisés à la place. Vous pouvez également ajouter des pilotes de périphérique au profil SE personnalisé (voir Création d'un profil d'image SE personnalisé).

Pour plus d'informations sur les limitations de systèmes d'exploitation spécifiques, voir Systèmes d'exploitation pris en charge.

Remarques sur le réseau

- Vérifiez que tous les ports requis sont ouverts (voir Disponibilité de port pour les systèmes d'exploitation déployés).
- Veillez à ce que XClarity Administrator puisse communiquer avec le serveur cible (à la fois le contrôleur de gestion de la carte mère et le réseau de données des serveurs) sur l'interface (Eth0 ou Eth1) qui a été sélectionnée au moment de la configuration de l'accès réseau de XClarity Administrator.

  Pour indiquer une interface à utiliser pour le déploiement du système d'exploitation, voir Configuration de l'accès réseau).

  Pour plus d'informations sur le réseau et les interfaces de déploiement de système d'exploitation, voir Remarques sur le réseau dans la documentation en ligne de XClarity Administrator.
- Vérifiez que les adresses IP sont uniques pour le système d'exploitation hôte. XClarity Administrator recherche les adresses IP en double dans les adresses réseau que vous spécifiez lors du processus de déploiement.
- Si le réseau est lent ou instable, vous pouvez constater des résultats imprévisibles lors du déploiement de systèmes d'exploitation.
- L'interface réseau XClarity Administrator qui est utilisée pour la gestion doit être configuré pour la connexion au contrôleur de gestion de la carte mère à l'aide de la même méthode d'adresse IP que vous choisissez dans la boîte de dialogue Paramètres globaux : Déployer des systèmes d'exploitation. Par exemple, si XClarity Administrator est configuré pour utiliser eth0 pour la gestion et si vous choisissez d'utiliser des adresses IPv6 statiques affectées manuellement lors de la configuration du SE déployé, l'interface eth0 doit être configurée avec une adresse IPv6 qui dispose d'une connectivité au contrôleur de gestion de la carte mère.

- Si vous choisissez d’utiliser des adresses IPv6 pour les paramètres globaux de déploiement SE, l'adresse IPv6 de XClarity Administrator doit pouvoir être routée vers le contrôleur de gestion de la carte mère et le réseau de données des serveurs.
- Le mode IPv6 n'est pas pris en charge pour ThinkServer (voir Limitations de la configuration IPv6 dans la documentation en ligne de XClarity Administrator).
- Si vous utiliser DHCP pour affecter dynamiquement les adresses IP, vous devez configurer les adresses MAC.
- Si vous utilisez des adresses IP statiques, vous devez configurer les paramètres réseau suivants pour un serveur spécifique, avant de pouvoir déployer un système d'exploitation sur ce serveur. Une fois ces paramètres configurés, l'état de déploiement du serveur est modifié à « Prêt. » (Notez que certaines zones ne sont pas disponibles pour les adresses IPv6 statiques.)
  - Nom d'hôte

    Le nom d'hôte doit également respecter les règles suivantes :
    - Le nom d'hôte de chaque serveur géré doit être unique.
    - Le nom d'hôte peut contenir des chaînes (étiquettes) qui sont séparées par un point (.).
    - Chaque étiquette peut contenir des lettres ASCII, des chiffres et des tirets (-). Toutefois, la chaîne ne peut ni commencer ni se terminer par un tiret, et ne peut pas contenir uniquement des chiffres.
    - La première étiquettes doit contenir de 2 à 15 caractères. Les étiquettes suivantes doivent contenir de 2 à 63 caractères.
    - La longueur totale du nom d'hôte ne doit pas dépasser 255 caractères.
  - Adresse MAC du port sur l'hôte sur lequel le système d'exploitation doit être installé.

    L'adresse MAC est définie à AUTO par défaut. Ce paramètre détecte automatiquement les ports Ethernet qui peuvent être configurés et utilisés pour le déploiement. La première adresse MAC (port) qui est détectée est utilisée par défaut. Si la connectivité est détectée sur un adresse MAC différente, l'hôte XClarity Administrator est automatiquement redémarré pour utiliser l'adresse MAC nouvellement détectée pour le déploiement.

    Vous pouvez déterminer l’état du port d’adresse MAC utilisé pour le déploiement SE en accédant au menu déroulant **Adresse MAC** de la boîte de dialogue Paramètres réseau. Si plusieurs ports sont activés ou si tous les ports sont arrêtés, AUTO est utilisé par défaut.

    Remarques :

    - Les ports réseau virtuels ne sont pas pris en charge. N’utilisez pas un port réseau physique pour simuler plusieurs ports réseau virtuels.
    - Lorsque le paramètre réseau du serveur est défini sur AUTO, XClarity Administrator peut détecter automatiquement les ports réseau dans les emplacements 1 à 16. Au moins un port des emplacements 1 à 16 doit disposer d’une connexion à XClarity Administrator.
    - Si vous souhaitez utiliser un port réseau dans l’emplacement 17 ou supérieur pour l’adresse MAC, vous ne pouvez pas utiliser AUTO. Au lieu de cela, vous devez définir le paramètre réseau du serveur sur l’adresse MAC du port spécifique que vous souhaitez utiliser.
    - Toutes les adresses MAC hôtes ne sont pas affichées pour les serveurs ThinkServer. Dans la plupart des cas, les adresses MAC pour les cartes Ethernet AnyFabric sont listées dans la boîte de dialogue Éditer les paramètres réseau. Les adresses MAC d'autres cartes Ethernet (tels que LAN-on-motherboard) ne sont pas listées. Dans le cas où les adresses MAC ne sont pas disponibles pour une carte, utilisez la méthode AUTO pour les déploiements non VLAN.
  - Adresse IP et masque de sous-réseau
  - Passerelle IP
  - Jusqu'à deux serveurs DNS (Domain Name System)
  - Vitesse d'unité MTU (unité de transmission maximale)

  - ID VLAN, si le mode IP VLAN est activé
- Si vous choisissez d'utiliser les réseaux VLAN, vous pouvez affecter un ID VLAN à la carte réseau qui est en cours de configuration.

Pour plus d'informations sur le réseau de déploiement du système d'exploitation et les interfaces, voir Configuration des paramètres réseau pour les serveurs gérés et Configuration des paramètres réseau pour les serveurs gérés et Remarques sur le réseau dans la documentation en ligne de XClarity Administrator.

Remarques sur le stockage et l'option d'amorçage

- Assurez-vous que l'option d'amorçage UEFI sur le serveur cible a pour valeur « Amorçage UEFI uniquement » avant de déployer un système d'exploitation. L'option d'amorçage « Legacy-only » et « UEFI d'abord, puis Legacy » n'est pas prise en charge pour le déploiement du système d'exploitation.
- Chaque serveur doit disposer d'un adaptateur RAID matériel installé et configuré.

  Attention :

  - Seul le stockage configuré avec RAID matériel est pris en charge.
  - Le RAID logiciel généralement présent sur l'adaptateur de stockage Intel SATA embarqué ou sur le stockage qui est configuré comme JBOD n'est pas pris en charge. Toutefois si un adaptateur RAID matériel n'est pas présent, le fait de paramétrer l'adaptateur SATA en **mode AHCI SATA** activé pour le déploiement de système d'exploitation ou de configurer des disques corrects non configurés en mode JBOD peut fonctionner dans certains cas. Pour plus d'informations, voir Le programme d'installation du système d'exploitation ne trouve pas le disque sur lequel vous voulez effectuer l'installation XClarity Administrator dans la documentation en ligne de XClarity Administrator.

    Cette exception ne s'applique pas aux lecteurs M.2.
  - Si un appareil géré possède à la fois des unités locales (SATA, SAS ou SSD) qui ne sont pas configurées pour le RAID matériel et des unités M.2, vous devez désactiver les unités locales pour utiliser les unités M.2, ou désactiver les unités M.2 pour utiliser les unités locales. Vous pouvez désactiver les contrôleurs de stockage intégrés et les mémoires mortes en option du stockage hérité et UEFI à l'aide des modèles de configuration en sélectionnant Désactiver le disque local dans l'onglet Stockage local de l'assistant ou en créant un Modèle de configuration à partir d'un serveur existant, puis désactiver les appareils M.2 dans le modèle UEFI étendu.
  - Si un adaptateur SATA est activé, le mode SATA *ne doit pas* être paramétré sur « IDE ».
- Le stockage NVMe qui est connecté à une carte mère de serveur ou un contrôleur HBA n'est pas pris en charge et ne doit pas être installé dans l'appareil ; dans le cas contraire, le déploiement SE sur une unité de stockage non NVMe échouera.
- Lors du déploiement de RHEL, plusieurs ports connectés au même numéro d'unité logique sur le stockage cible ne sont pas pris en charge.
- Assurez-vous que le mode d'amorçage sécurisé est désactivé pour le serveur. Si vous déployez un système d'exploitation pour lequel le mode d'amorçage sécurisé est activé (par exemple, Windows), désactivez ce mode, déployez le système d'exploitation, puis réactivez le mode d'amorçage sécurisé.
- Lorsque vous déployez Microsoft Windows sur un serveur, les appareils associés ne doivent pas comporter de partitions système existantes (voir Le déploiement SE échoue en raison de partitions système existantes sur une unité de disque connectée dans la documentation en ligne de XClarity Administrator).
- Pour les serveurs ThinkServer, vérifiez que les conditions suivantes sont remplies :

  - Les paramètres d'amorçage sur le serveur doivent inclure une stratégie opROM de stockage à laquelle la valeur `UEFI Only` est attribuée. Pour plus d'informations, voir Le programme d'installation du système d'exploitation ne peut pas démarrer sur un serveur ThinkServer XClarity Administrator dans la documentation en ligne de XClarity Administrator.

- Si vous déployez ESXi et s'il existe des adaptateurs réseau amorçables sur PXE, désactivez le support PXE sur les cartes réseau avant de déployer le système d'exploitation. Le déploiement est terminé, vous pouvez réactiver le support PXE, si vous le souhaitez.
- Si vous déployez ESXi et si des appareils amorçables autres que l'appareil sur lequel le système d'exploitation doit être installé figurent dans la liste de l'ordre d'amorçage, supprimez les appareils amorçables de cette liste avant de déployer le système d'exploitation. Une fois le déploiement terminé, vous pouvez ajouter à nouveau l'appareil amorçable dans la liste. Vérifiez que l'appareil installé figure en haut de la liste.

Pour plus d'informations sur les paramètres de stockage local, voir Choix de l'emplacement de stockage pour les serveurs gérés.

Remarques sur les appareils gérés

- Pour plus d'informations sur les limitations du déploiement de système d'exploitation pour des dispositifs spécifiques, voir Support de XClarity Administrator – Page Web de compatibilité, cliquez sur l'onglet **Compatibilité**, puis cliquez sur le lien des types d'appareil appropriés.
- Vérifiez qu'il n'y a aucun support monté (par exemple, ISOs) sur le serveur cible. En outre, assurez-vous qu'il n'y a pas de sessions de support éloigné actives ouvertes sur le contrôleur de gestion.
- Vérifiez que l'horodatage dans le BIOS est défini à la date et à l'heure actuelles.
- Pour les serveurs équipés de XCC2 où System Guard est activé et où l'action est définie sur **Empêcher l'amorçage SE**, assurez-vous que System Guard est conforme sur l'appareil. Si System Guard n'est pas conforme, les appareils ne peuvent pas mener à bien le processus d'amorçage, ce qui entraîne l'échec du déploiement du système d'exploitation. Pour provisionner ces appareils, répondez manuellement à l'invite d'amorçage de System Guard afin d'autoriser l'amorçage normal des appareils.
- Pour les serveurs ThinkSystem et System x, assurez-vous que l'option Legacy BIOS est désactivée. Depuis l'utilitaire BIOS/UEFI (F1) Setup utility, cliquez sur **Configuration UEFI → Paramètres système**, puis vérifiez que Legacy BIOS est défini sur Disabled.
- Vérifiez que le châssis est sous tension s'il s'agit d'un serveur Flex System.
- Assurez-vous qu'une clé Feature On Demand (FoD) de présence à distance est installée sur les serveurs Converged, NeXtScale et System x. Vous pouvez déterminer si la présence à distance est activée, désactivée ou non installée sur un serveur depuis la page Serveurs (voir Affichage de l'état d'un serveur géré). Pour plus d'informations sur les clés FoD installées sur vos serveurs, voir Affichage des clés Features on Demand (FoD).
- Pour les serveurs ThinkSystem et les appareils ThinkAgile, la fonctionnalité XClarity Controller Enterprise est requise pour le déploiement du système d'exploitation. Pour plus d'informations, voir Affichage des clés Features on Demand (FoD).
- Pour les dispositifs Converged et ThinkAgile, il est recommandé de *ne pas* utiliser XClarity Administrator pour exécuter un déploiement de système d'exploitation nu.

Systèmes d'exploitation pris en charge

Lenovo XClarity Administrator prend en charge le déploiement de plusieurs systèmes d'exploitation. Seules les versions prises en charge des systèmes d'exploitation peuvent être chargées dans le Référentiel d'images SE de XClarity Administrator.

Important :

- Pour plus d'informations sur les limitations du déploiement de système d'exploitation pour des dispositifs spécifiques, voir Support de XClarity Administrator – Page Web de compatibilité, cliquez sur l'onglet **Compatibilité**, puis cliquez sur le lien des types d'appareil appropriés.
- La fonction de gestion cryptographique de XClarity Administrator permet de limiter la communication à certains modes SSL/TLS minimum. Par exemple, si TLS1.2 est sélectionné, seuls les systèmes

d'exploitation dotés d'un processus d'installation prenant en charge TLS1.2 et les algorithmes cryptographiques forts peuvent être déployés via XClarity Administrator.

- Des images du système d'exploitation se trouvant dans le référentiel XClarity Administrator peuvent ne pas être prises en charge que sur certaines plateformes matérielles. Seules les images du système d'exploitation qui sont prises en charge par le serveur sélectionné figurent sur la page Déployer des images de SE. Vous pouvez déterminer si un système d'exploitation est compatible avec un serveur donné avec Site Web du guide d'interopérabilité SE Lenovo.
- Pour les obtenir des informations sur la compatibilité et la prise en charge des systèmes d'exploitation et hyperviseurs associés et sur les ressources pour les serveurs et solutions Lenovo, consultez Page Web du centre de support pour le serveur du système d'exploitation.

Le tableau suivant répertorie les systèmes d'exploitation 64bits qui peuvent être déployés par XClarity Administrator.

Système d'exploitation	**Versions**	**Remarques**
Linux CentOS	7.2 and later 8.0 8.1 8.2	**Remarques :** • Toutes les versions mineures existantes et futures sont prises en charge sauf indication contraire. • Les adresses IPv4 statiques, IPv6 statiques et le protocole DHCP sont pris en charge. • Le marquage VLAN n'est pas pris en charge. • Les pilotes non fournis avec Windows ne sont pas pris en charge. • La personnalisation du profil SE n'est pas prise en charge. • CentOS8.3 n’est pas pris en charge.
Microsoft® Windows® Azure Stack HCI	20H2 21H2	La personnalisation du profil SE n'est pas prise en charge.
Client Microsoft Windows	10 21H2 10 22H2 11 22H2	

Système d'exploitation	Versions	Remarques
Microsoft Windows Server	2012 R2 2012 R2U1 2016 2019 2022	Les copies de licence de volume et de licence de détail sont prises en charge. **Remarque :** XClarity Administrator est uniquement testé avec des versions Windows prises en charge par Microsoft au moment de la sortie de la version XClarity Administrator. Les éléments suivants ne sont *pas pris en charge*: • Windows Reseller Option Kit (ROK) • Windows Server Semi-Annual Channel (SAC) v1709, v1803 et v1809 • Windows Server 2019 Essentials • Windows Server 2016 Nanoserver • Copie d'évaluation de Windows Server 2012 • Images WindowsServer sur des serveurs gérés équipés de clés d'hyperviseur imbriqué Windows Server 2012 R2 sur des serveurs contenant des processeurs Intel CLX Vous devez retirer physiquement la clé de l'hyperviseur imbriqué sur les serveurs cible avant de déployer une image Windows. Cela inclut Hyper-V via l'un des profils de virtualisation. – Centre de données – Cœur de centre de données – Virtualisation de centre de données (Hyper-V) – Cœur de virtualisation de centre de données (Hyper-V avec cœur) – Norme – Cœur standard – Virtualisation standard (Hyper-V) – Cœur de virtualisation standard (Hyper-V avec cœur)
Red Hat® Enterprise Linux (RHEL) Server	6.8 and later 7.2 and later 8.x 9.x	Inclut KVM **Remarques :** • Toutes les versions mineures existantes et futures sont prises en charge sauf indication contraire. • Lors de l'importation de la version DVD de l'image SE, seul DVD1 est pris en charge. • Lors de l'installation de RHEL sur des serveurs ThinkSystem, RHEL v7.4 ou version ultérieure est recommandé. • Pour déployer RHEL 7.2, l'affectation d'IP globale doit être définie pour l'utilisation d'adresses IPv4. Pour plus d'informations sur les paramètres globaux, voir Configuration des paramètres de déploiement SE. • Des échecs de déploiement de système d'exploitation ont été observés sur les réseaux IPv6 avec de faibles bandes passantes en raison de délais d'attente dans le programme d'installation du système d'exploitation. • Le marquage VLAN n'est pas pris en charge.
Rocky Linux	8.x 9.x	**Remarques :** • Toutes les versions mineures existantes et futures sont prises en charge sauf indication contraire. • Les adresses IPv4 statiques, IPv6 statiques et le protocole DHCP sont pris en charge. • Le marquage VLAN n'est pas pris en charge. • Les pilotes non fournis avec Windows ne sont pas pris en charge.

Système d'exploitation	Versions	Remarques
SUSE® Linux Enterprise Server (SLES)	12.x 15.x	Inclut KVM et les hyperviseurs Xen **Remarques :** • Tous les Service Packs existants et futurs sont pris en charge sauf indication contraire. • Lors de l'importation de la version DVD de l'image SE, seul DVD1 est pris en charge. • Des échecs de déploiement de SE ont été observés sur les réseaux IPv6 avec des bandes passantes inférieures en raison de délais d'attente dans le programme d'installation du SE. • Si vous souhaitez déployer SLES 12 SP2 sur un serveur ThinkSystem, vous devez utilisez un profil kISO. Pour obtenir les profils kISO, vous devez importer l'image kISO SLES appropriée. Pour plus d'informations, voir Remarques sur le déploiement de systèmes d'exploitation. • Pour SLES 15 et 15 SP1, vous devez importer l'image du programme d'installation et l'image package associée depuis Page Web du centre de support pour le serveur du système d'exploitation. Pour SLES 15 SP2 ou version ultérieure, vous devez importer uniquement l'image de support d'installation complète car le programme d'installation unifié et les modules de DVD de SUSE Linux Enterprise Server 15 et 15 SP1 sont obsolètes. • Le marquage VLAN n'est pas pris en charge.
Serveur Ubuntu	20.04.x 22.04.x	**Remarques :** • L'image peut être installée sur l'option de stockage sélectionnée (unité de disque local, unité M.2 ou volume SAN FC). • Toutes les versions mineures existantes et futures sont prises en charge sauf indication contraire. • Seul DHCP est pris en charge. Les adresses IPv4 et IPv6 statiques *ne sont pas* prises en charge. • Le marquage VLAN *n'est pas* pris en charge. • Les pilotes non fournis avec Windows *ne sont pas* pris en charge. • La personnalisation du profil SE *n'est pas* prise en charge.
VMware vSphere® Hypervisor (ESXi)	5.5 5.5u1 5.5u2 5.5u3 6.0.x 6.5.x 6.7.x 7.0.x 8.0.x	Les images de base VMware vSphere Hypervisor (ESXi) et les images personnalisées Lenovo VMware ESXi ne sont pas prises en charge. Les images personnalisées Lenovo VMware ESXi sont personnalisées pour certains matériels afin de vous fournir des fonctions de gestion de plateforme en ligne, y compris la mise à jour et la configuration de microprogramme, de diagnostics de plateforme et d'alertes matériel améliorées. Les outils de gestion de Lenovo prennent également en charge la gestion simplifiée de ESXi avec certains serveurs System x. Cette image n'est pas disponible au téléchargement à partir de Support VMware - Site Web de téléchargement. La licence fournie avec l'image est un essai gratuit de 60jours. Vous êtes responsable du respect de toutes les conditions de licence de VMware. **Important :** • Tous les modules de mise à jour existants et futurs sont pris en charge pour les versions 6.0, 6.5, 6.7, 7.0 et 8.0, sauf indication contraire. • Les images ESXi de base (sans personnalisation Lenovo) incluent uniquement des pilotes de périphériques prédéfinis et basiques pour le réseau et le stockage. Cette image de base n'inclut pas de pilotes de périphériques prédéfinis (qui sont inclus dans les images personnalisés Lenovo VMware ESXi). Vous pouvez ajouter des pilotes de périphérique

Système d'exploitation	Versions	Remarques
		prédéfinis en créant vos propres profils d'images SE personnalisées (voir Personnalisation de profils d'image SE). • Pour certaines versions des images Lenovo VMware ESXi avec personnalisation, des images distinctes peuvent être disponibles pour System x, ThinkSystem et ThinkServer. Une seule image pour une version spécifique peut exister à la fois dans le référentiel d'images SE. • Le déploiement de ESXi n'est pas pris en charge pour certains serveurs plus anciens. Pour plus d'informations sur les serveurs pris en charge, voir Site Web du guide d'interopérabilité SE Lenovo. • Les versions suivantes sont prises en charge pour les appareils ThinkServer: ESXi 6.0u3, 6.5 et ultérieurs. • Lors de l'installation de ESXi 5.5 (y compris les mises à jour éventuelles) ou 6.0 sur un serveur dans un châssis Flex System, il se peut que le serveur ne réponde plus ou redémarre rapidement après l'affichage du message suivant: `Chargement en cours image.pld` • ESXi 5.5 requiert qu'un espace MMIO (memory-mapped I/O) soit configuré dans les 4Go initiaux du système. Selon la configuration, certains systèmes tentent d'utiliser une mémoire supérieure à 4Go, ce qui peut provoquer une défaillance. Pour résoudre le problème, voir Le déploiement VMware provoque le blocage ou le redémarrage du système dans la documentation en ligne de XClarity Administrator. • Lors du déploiement d'ESXi via un mode IPv6 statique, le nom d'hôte défini dans la page Paramètres du réseau de XClarity Administrator n'est pas configuré dans l'instance ESXi déployée. À la place, le nom d'hôte par défaut `localhost` est utilisé. Vous devez définir manuellement le nom d'hôte dans l'instance ESXi déployée de manière à ce qu'il corresponde au nom d'hôte défini dans XClarity Administrator. • Lors du déploiement d'ESXi sur un serveur géré, le système d'exploitation ne déplace pas l'unité sur laquelle le système d'exploitation est installé en haut de la liste de l'ordre d'amorçage. Si un dispositif d'amorçage contenant un système d'exploitation amorçable ou un serveur PXE est spécifié avant le dispositif d'amorçage contenant ESXi, ESXi ne démarre pas. Pour le déploiement ESXi, XClarity Administrator met à jour la liste d'ordre d'amorçage de la plupart des serveurs afin que le dispositif d'amorçage ESXi figure en haut de la liste de l'ordre d'amorçage. Toutefois, les serveurs ThinkServer ne ne permettent pas à XClarity Administrator de mettre à jour cette liste. Vous devez désactiver le support d'amorçage PXE ou retirer les appareils amorçables autres que l'unité d'installation avant de déployer le système d'exploitation. Pour plus d'informations, voir Le système d'exploitation ne démarre pas après le déploiement d'ESXi sur un serveur ThinkServer dans la documentation en ligne de XClarity Administrator. **Astuce:** Au lieu de définir l'option **MM Config** via Setup Utility pour chaque serveur, envisagez d'utiliser l'un des modèles UEFI étendu prédéfinis liés à la virtualisation afin d'affecter la valeur 3GB à l'option MM Config et de désactiver l'allocation de la ressource PCI 64bits. Pour plus d'informations sur ces modèles, voir Définition de paramètres UEFI étendu.

Profils d'image de système d'exploitation

Lorsque vous importez une image SE dans le Référentiel d'images SE, Lenovo XClarity Administrator crée un ou plusieurs profils pour cette image et les stocke dans le Référentiel d'images SE. Chaque *profil* prédéfini inclut l'image SE et les options d'installation correspondantes.

Attributs de profil d'image SE

Les attributs de profil d'image SE fournissent des informations supplémentaires sur les profils d'images SE. Les attributs suivants peuvent s'afficher.

- **kISO**. Vous devez utiliser un profil kISO pour déployer SLES 12 SP2 vers un serveur ThinkSystem. Vous pouvez télécharger l'image kISO SLES depuis le Support Linux - Site Web de téléchargement.

Profils d'image SE prédéfinis

Le tableau suivant répertorie les profils qui sont prédéfinis par XClarity Administrator lorsque vous importez une image de système d'exploitation. Ce tableau indique également les modules inclus dans chaque profil.

Vous pouvez créer un profil d'image SE personnalisé pour un système d'exploitation de base. Pour plus d'informations, voir Personnalisation de profils d'image SE.

Système d'exploitation	Profil	Modules inclus dans le profil	

Linux CentOS	De base	`@X Window System`
		`@Desktop`
		`@Fonts`
		`compat-libstdc++-33`
		`compat-libstdc++-33.i686`
		`compat-libstdc++-296`
		`libstdc++.i686`
		`pam.i686`	

	Minimal	`compat-libstdc++-33`
		`compat-libstdc++-33.i686`
		`compat-libstdc++-296`
		`libstdc++.i686`
		`pam.i686`	

	Virtualisation	`%packages`
		`@virtualization`
		`@virtualization-client`
		`@virtualization-platform`
		`@virtualization-tools`
		`# begin additional packages`
		`@basic-desktop`
		`@desktop-debugging`
		`@desktop-platform`
		`@fonts`
		`@general-desktop`
		`@graphical-admin-tools`
		`@kde-desktop`
		`@remote-desktop-clients`
		`@x11`
		`@^graphical-server-environment`
		`@gnome-desktop`
		`@x11`
		`@virtualization-client`
		`# end additional packages`
			`libconfig`
			`libsysfs`
			`libicu`
			`lm_sensors-libs`
			`net-snmp`
			`net-snmp-libs`
			`redhat-lsb`
			`compat-libstdc++-33`
			`compat-libstdc++-296`
			`# begin additional rpms`
			`xterm`
			`xorg-x11-xdm`
			`rdesktop`
			`tigervnc-server`
			`device-mapper-multipath`
			`# end additional rpms`

Système d'exploitation	Profil	Modules inclus dans le profil

Microsoft® Windows® Azure Stack HCI	Azure	`<selection name="Microsoft-Hyper-V" state="true" />`
		`<selection name="MultipathIo" state="true" />`
		`<selection name="FailoverCluster-PowerShell" state="true" />`
		`<selection name="FailoverCluster-FullServer" state="true" />`
		`<selection name="FailoverCluster-CmdInterface" state="true" />`
		`<selection name="FailoverCluster-AutomationServer" state="true" />`
		`<selection name="FailoverCluster-AdminPak" state="true" />`
		`<selection name="Containers" state="true" />`
		`<selection name="MicrosoftWindowsPowerShellRoot" state="true" />`
		`<selection name="MicrosoftWindowsPowerShell" state="true" />`
		`<selection name="ServerManager-Core-RSAT" state="true" />`
		`<selection name="ServerManager-Core-RSAT-Role-Tools" state="true" />`

Client Microsoft Windows	Enterprise	
	Enterprise N	
	Postes de travail Pro	
	Postes de travail Pro N	

Microsoft Windows Hyper-V Server 2016	Hyper_V	`<selection name="Microsoft-Hyper-V" state="true" />`
		`<selection name="MultipathIo" state="true" />`
		`<selection name="FailoverCluster-PowerShell" state="true" />`
		`<selection name="FailoverCluster-FullServer" state="true" />`
		`<selection name="FailoverCluster-CmdInterface" state="true" />`
		`<selection name="FailoverCluster-AutomationServer" state="true" />`
		`<selection name="FailoverCluster-AdminPak" state="true" />`
		`<selection name="MicrosoftWindowsPowerShellRoot" state="true" />`
		`<selection name="MicrosoftWindowsPowerShell" state="true" />`
		`<selection name="ServerManager-Core-RSAT" state="true" />`
		`<selection name="ServerManager-Core-RSAT-Role-Tools" state="true" />`

Microsoft Windows Server **Remarque :** Inclut Hyper-V via le *profil de virtualisation*.	Centre de données	`GUI`
	Virtualisation de centre de données	`GUI` `Hyper-V role`
	Cœur de virtualisation de centre de données	`Hyper-V role`
	Cœur de centre de données	
	Norme	`GUI`
	Virtualisation standard	`GUI` `Hyper-V role`
	Cœur de virtualisation standard	`Hyper-V role`
	Cœur standard	

Système d'exploitation	Profil	Modules inclus dans le profil	
Microsoft Windows Server personnalisé	Datacenter_ customized		
	Standard_ customized		
Red Hat Enterprise Linux (RHEL) **Remarque :** Inclut KVM	De base	@X Window System @Desktop @Fonts compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	Minimal	compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	Virtualisation	%packages @virtualization @virtualization-client @virtualization-platform @virtualization-tools # begin additional packages @basic-desktop @desktop-debugging @desktop-platform @fonts @general-desktop @graphical-admin-tools @kde-desktop @remote-desktop-clients @x11 @^graphical-server-environment @gnome-desktop @x11 @virtualization-client # end additional packages	libconfig libsysfs libicu lm_sensors-libs net-snmp net-snmp-libs redhat-lsb compat-libstdc++-33 compat-libstdc++-296 # begin additional rpms xterm xorg-x11-xdm rdesktop tigervnc-server device-mapper-multipath # end additional rpms
Rocky Linux	De base	@X Window System @Desktop @Fonts compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	Minimal	compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	

Système d'exploitation	Profil	Modules inclus dans le profil	
	Virtualisation	%packages @virtualization @virtualization-client @virtualization-platform @virtualization-tools # begin additional packages @basic-desktop @desktop-debugging @desktop-platform @fonts @general-desktop @graphical-admin-tools @kde-desktop @remote-desktop-clients @x11 @^graphical-server-environment @gnome-desktop @x11 @virtualization-client # end additional packages	libconfig libsysfs libicu lm_sensors-libs net-snmp net-snmp-libs redhat-lsb compat-libstdc++-33 compat-libstdc++-296 # begin additional rpms xterm xorg-x11-xdm rdesktop tigervnc-server device-mapper-multipath # end additional rpms
SUSE Linux Enterprise Server (SLES) 15	Base et Base	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <package>wget</package>	
	Minimal et Minimal	<pattern>base</pattern> <pattern>minimal_base</pattern> <pattern>yast2_basis</pattern> <package>wget</package>	
	Virtualisation-KVM et Virtualisation-KVM	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern> <package>wget</package>	

Système d'exploitation	Profil	Modules inclus dans le profil
	Virtualisation-Xen et Virtualisation-Xen	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern> <package>wget</package>
Ubuntu	Minimal	Serveur OpenSSH
	Virtualisation	qemu qemu-kvm libvirt-daemon libvirt-clients bridge-utils virt-manager
VMware vSphere® Hypervisor (ESXi)	Virtualisation	Les images de base VMware vSphere Hypervisor (ESXi) et les images personnalisées Lenovo VMware ESXi ne sont pas prises en charge.

Disponibilité de port pour les systèmes d'exploitation déployés

Certains ports sont bloqués par certains profils de système d'exploitation. Les tableaux suivants répertorient les ports qui doivent être ouverts (non bloqués).

Communication	Profil de virtualisation RHEL, Centos et Rocky[1]	Profils minimal et de base RHEL, Centos et Rocky[1]	Profils minimal, de base et de virtualisation SLES[2]	Profils minimal et de virtualisation Ubuntu[3]	Profil de virtualisation VMware ESXi[4]	Profils Windows
Sortant (ports ouverts sur des systèmes externes)	• Communication avec les dispositifs réseau RHEL KVM - TCP et UDP sur les ports **53** et **67** • Communication avec les agents SNMP - UDP sur le port **161** • Communication avec l'agent de service SLP, l'agent de répertoire SLP - TCP et UDP sur le port **427** • Communication CIM-XML sur HTTP - TCP sur les ports **15988** et **15989** • Communication de serveur virtuel KVM - TCP sur les ports **49152 - 49215**					• Communication SMB - TCP sur le port **445**
Entrant (ports ouverts sur l'appareil XClarity	• SSH – TCP sur le port **22** • Dispositifs réseau RHEL KVM - TCP et UDP sur les ports **53** et **67**	• SSH – TCP sur le port **22** • Déploiement SE - TCP et UDP sur les ports **445, 3900** et **8443**	• Déploiement SE - TCP et UDP sur les ports **445, 3900** et **8443**	• Déploiement SE - TCP et UDP sur les ports **445, 3900** et **8443**	• Déploiement SE - TCP et UDP sur les ports **445, 3900** et **8443**	• Déploiement SE - TCP et UDP sur les ports **445, 3900** et **8443**

Com-munication	Profil de virtualisation RHEL, Centos et Rocky[1]	Profils minimal et de base RHEL, Centos et Rocky[1]	Profils minimal, de base et de virtualisation SLES[2]	Profils minimal et de virtualisation Ubuntu[3]	Profil de virtualisation VMware ESXi[4]	Profils Windows
Admi-nistra-tor)	• Agents SNMP - UDP sur le port **162** • Déploiement SE - TCP et UDP sur les ports **445, 3900** et **8443** • Agent de service SLP, agent de répertoire SLP - TCP et UDP sur le port **427** • Serveur virtuel KVM - TCP sur les ports **49152 - 49215**					

1. Par défaut, les profils RHEL (Red Hat Enterprise Linux) bloquent tous les ports sauf ceux qui sont répertoriés dans le tableau ci-après.
2. Pour SLES (SUSE Linux Enterprise Server), certains ports ouverts sont affectés dynamiquement en fonction de la version et des profils de système d'exploitation. Pour obtenir la liste complète des ports ouverts, voir la documentation de votre système SUSE Linux Enterprise Server.
3. Pour le serveur Ubuntu Linux, certains ports ouverts sont affectés dynamiquement en fonction de la version et des profils de système d'exploitation. Pour obtenir la liste complète des ports ouverts, voir la documentation du serveur Ubuntu.
4. Pour obtenir la liste complète des ports ouverts pour VMware vSphere Hypervisor (ESXi) avec personnalisation Lenovo, voir la documentation de VMware pour ESXi sur le Site Web de base de connaissances VMware.

Configuration d'un serveur de fichiers distant

Vous pouvez importer des images SE, des pilotes de périphérique et des fichiers d'amorçage dans le référentiel d'images SE à partir du système local ou d'un serveur de fichiers distant. Pour importer des fichiers à partir d'un serveur de fichiers distant, vous devez d'abord créer un profil qui est utilisé pour authentifier la connexion au serveur de fichiers distant.

À propos de cette tâche

Les algorithmes cryptographiques suivants sont pris en charge :
- RSA–2048 bits
- RSA–4096 bits
- ECDSA–521 bits (secp521r1 curve)

Les protocoles suivants sont pris en charge :

- HTTP sans authentification.
- HTTP avec authentification de base.
- HTTPS (validation de certificat) avec authentification de base.
- HTTPS (validation de certificat) sans authentification.
- FTP avec authentification par mot de passe.
- SFTP (validation de client) avec authentification par mot de passe.
- SFTP (validation de client) avec authentification par clé publique.

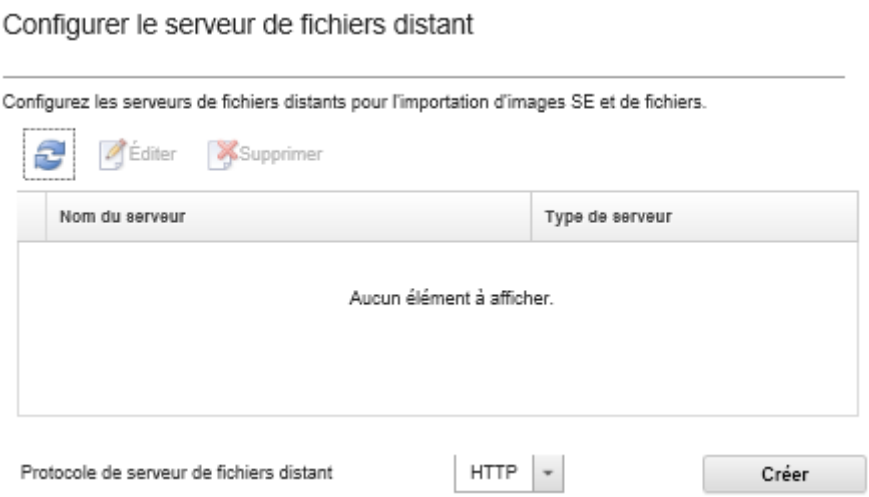
Pour l'authentification par clé publique SFTP et la validation de certificat HTTPS, Lenovo XClarity Administrator valide le certificat du serveur de fichiers distant. Si le certificat de serveur ne figure pas dans le fichier de clés certifiées, vous êtes invité à l'accepter et à l'ajouter au fichier de clés certifiées. Pour plus d'informations sur le dépannage des problèmes de validation, voir La validation de la certification du serveur a échoué dans la documentation en ligne de XClarity Administrator.

Procédure

Pour configurer un serveur de fichiers distant, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Gérer les images de SE** pour afficher la page Déployer un système d'exploitation : déployer des images de SE.

Etape 2. Cliquez sur l'icône **Configurer le serveur de fichiers** ( ) pour afficher la boîte de dialogue Configurer le serveur de fichiers distant.



Etape 3. Sélectionnez le protocole pour le serveur de fichiers distant dans la liste **Protocole de serveur de fichiers distant**.

Etape 4. Cliquez sur **Créer**. La boîte de dialogue Configurer le serveur de fichiers distant s'affiche.

Remarque : Cette boîte de dialogue varie en fonction du protocole que vous avez sélectionné.

Etape 5. Entrez le nom de serveur, l'adresse et le port.

Etape 6. Pour les protocoles HTTP, HTTPS, FTP et SFTP avec authentification de base, entrez un nom d'utilisateur et un mot de passe si une authentification est nécessaire pour accéder au serveur.

Etape 7. Pour le protocole SFTP avec authentification de base, cliquez sur **Valider le certificat du serveur** pour obtenir la signature de clé publique.

Remarque : Une boîte de dialogue peut s'afficher pour vous informer que le processus de déploiement SE ne pas confiance la clé publique du serveur de fichiers SFTP. Cliquez sur **OK** pour stocker et approuver la clé publique SFTP dans le magasin de clés certifiées du déploiement SE.

En cas de réussite, la signature de la clé publique apparaît dans la zone **Signature de clé publique du serveur SFTP**.

Etape 8. Pour le protocole SFTP avec authentification par clé publique :

a. Entrez une phrase de passe et un mot de passe de clé et sélectionnez le type de clé si une authentification est nécessaire pour accéder au serveur.

b. Cliquez sur **Générer une clé du serveur de gestion** pour obtenir la signature de clé publique.

c. Copiez la clé générée dans le fichier authorized_keys sur votre serveur de fichiers distant SFTP.

d. Activez la case à cocher **La clé de gestion a été copiée sur le serveur** dans XClarity Administrator.

e. Cliquez sur **Valider le certificat du serveur** pour valider la signature de la clé publique.

Remarque : Une boîte de dialogue peut s'afficher pour vous informer que le processus de déploiement SE ne pas confiance la clé publique du serveur de fichiers SFTP. Cliquez sur **OK** pour stocker et approuver la clé publique SFTP dans le magasin de clés certifiées du déploiement SE. En cas de réussite, la signature de la clé publique apparaît dans la zone **Signature de clé publique du serveur SFTP**.

f. Cliquez sur **Enregistrer**.

Etape 9. Cliquez sur **Serveur de sauvegarde**.

Après avoir terminé

La boîte de dialogue Configurer le serveur de fichiers distant vous permet d'effectuer les actions suivantes :

- Actualiser la liste de serveurs de fichiers distants en cliquant sur l'icône **Actualiser** ( ).
- Modifier un serveur de fichiers distant sélectionné en cliquant sur l'icône **Éditer** ( ).
- Retirer un serveur de fichiers distant sélectionné en cliquant sur l'icône **Supprimer** ( ).

Importation d'images du système d'exploitation

Pour pouvoir déployer un système d'exploitation sous licence sur les serveurs gérés, vous devez importer l'image dans le XClarity Administrator Référentiel d'images SE.

À propos de cette tâche

Pour plus d'informations sur les images de système d'exploitation que vous pouvez importer et déployer, voir Systèmes d'exploitation pris en charge.

Pour obtenir la liste des systèmes d'exploitation de base et personnalisés pris en charge, voir Systèmes d'exploitation pris en chargeSystèmes d'exploitation pris en charge dans la documentation en ligne de Lenovo XClarity Administrator.

Vous pouvez importer une seule image à la fois. Attendez que l'image s'affiche dans le Référentiel d'images SE avant de tenter d'importer une autre image. L'importation du système d'exploitation peut prendre un certain temps.

Pour ESXi uniquement, vous pouvez importer plusieurs images ESXi avec la même version majeure/mineure vers le référentiel d’image S.E.

Pour ESXi uniquement, vous pouvez importer plusieurs images ESXi personnalisées avec la même version majeure/mineure et le même numéro de build vers le référentiel d'image SE.

Lorsque vous importez une image du système d'exploitation, XClarity Administrator :

- Vérifie qu'il existe suffisamment d'espace dans Référentiel d'images SE avant d'importer le système d'exploitation. Si vous n'avez pas suffisamment d'espace pour importer une image, supprimez une image existante dans le référentiel, puis essayez de réimporter la nouvelle image.
- Crée un ou plusieurs profils de cette image et stocke le profil dans Référentiel d'images SE. Chaque *profil* comprend les options d'installation et d'image SE. Pour plus d'informations sur les profils d'image SE prédéfinis, voir Profils d'image de système d'exploitation.

Remarque : Internet Explorer et les navigateurs web Microsoft Edge ont une limite de téléchargement de 4 Go. Si le fichier que vous importez est supérieur à 4 Go, envisagez d'utiliser un autre navigateur web (par exemple, Chrome ou Firefox) ou copiez le fichier sur un serveur de fichiers distant et importez-le à l'aide de l'option **Importation à distance**.

Procédure

Pour importer une image du système d'exploitation dans le Référentiel d'images SE, procédez comme suit.

Etape 1. Procurez-vous une image ISO sous licence du système d'exploitation.

Remarque : Il vous incombe de vous procurer les licences applicables pour le système d'exploitation.

Etape 2. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Gérer les images de SE** pour afficher la page Déployer des systèmes d'exploitation : gérer des images de SE.

Etape 3. Cliquez sur l'icône **Importer des fichiers** () pour afficher la boîte de dialogue Importer des images SE/fichiers.

Etape 4. Cliquez sur l'onglet **Local** pour télécharger des fichiers à partir du système local ou cliquez sur l'onglet **Distant** pour télécharger des fichiers à partir d'un serveur de fichiers distant.

Remarque : Pour télécharger un fichier à partir d'un serveur de fichiers distant, vous devez d'abord créer un profil de serveur de fichiers distant en cliquant sur l'icône **Configurer le serveur de fichiers** (). Pour plus d'informations, voir Configuration d'un serveur de fichiers distant .

Etape 5. Si vous choisissez d'utiliser un serveur de fichiers distant, sélectionnez-le dans la liste **Serveur de fichiers distant**.

Etape 6. Entrez le chemin d'accès et le nom du fichier image ISO, ou cliquez sur **Parcourir** pour rechercher l'image ISO que vous souhaitez importer.

Si vous avez choisi d'utiliser le *serveur de fichiers local*, vous devez entrer le chemin d'accès absolu au fichier image ISO. Si vous avez choisi d'utiliser un *serveur de fichiers distant*, vous devez entrer le chemin d'accès absolu (par exemple, `/home/user/isos.osimage.iso`) ou le chemin relatif (par exemple, `/isos.osimage.iso`) au fichier image ISO (selon la configuration du serveur de fichiers distant). Si le fichier est introuvable, vérifiez que le chemin d'accès au fichier est correct et essayez à nouveau.

Etape 7. **Facultatif :** Entrez une description pour l'image SE.

Etape 8. **Facultatif :** Sélectionnez un type de total de contrôle pour vérifier que l'image ISO importée dans XClarity Administrator n'est pas endommagé et copiez et collez la valeur de total de contrôle dans la zone de texte fournie.

Si vous sélectionnez un type de total de contrôle, vous devez indiquer une valeur de total de contrôle pour vérifier l'intégrité et la sécurité de l'image SE téléchargée. La valeur doit venir de la

source sécurisée d'une organisation fiable. Si l'image téléchargée correspond à la valeur de total de contrôle, le déploiement peut être poursuivi en toute sécurité. Sinon, vous devez télécharger à nouveau l'image ou vérifier la valeur de total de contrôle.

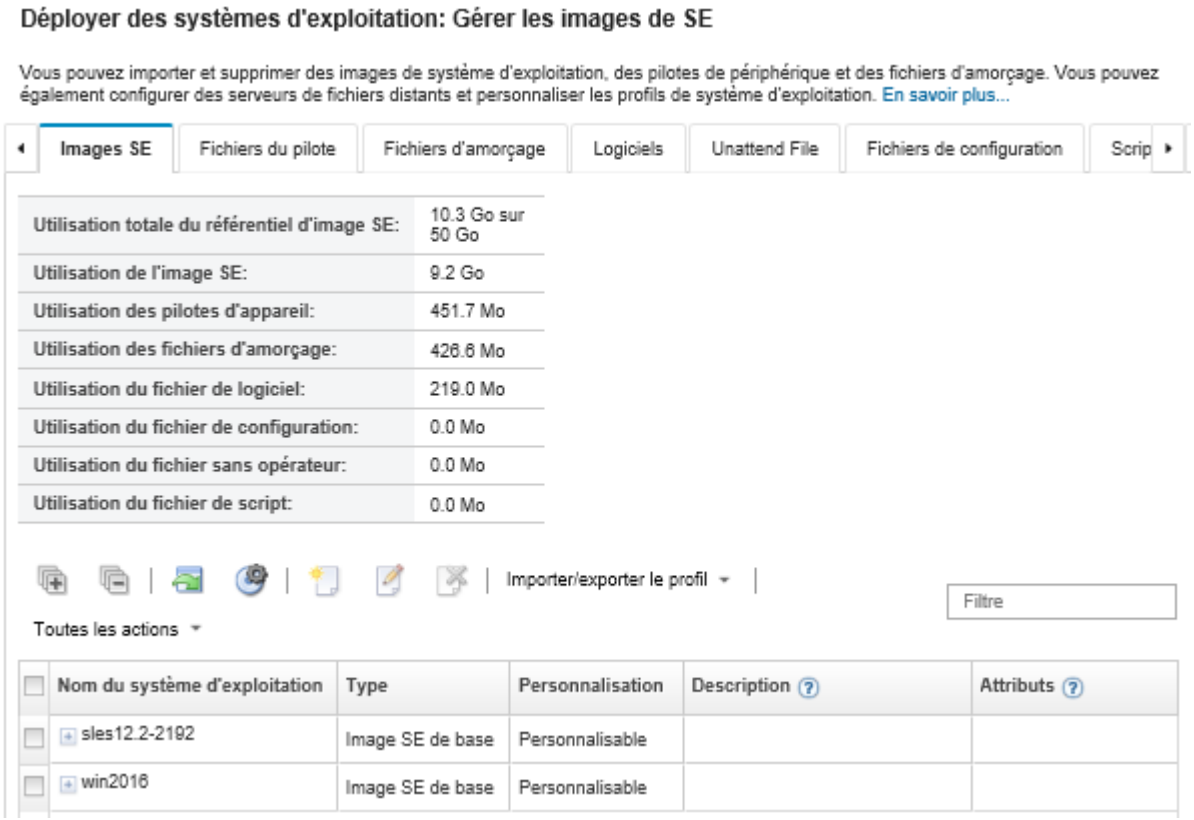
Trois types de total de contrôle sont pris en charge :
- **MD5**
- **SHA1**
- **SHA256**

Etape 9. Cliquez sur **Importer**.

Astuce : L'image ISO est téléchargée via une connexion réseau sécurisée. Par conséquent, la fiabilité et les performances du réseau ont une incidence sur le temps nécessaire à l'importation de l'image. Si vous fermez l'onglet ou la fenêtre de navigateur Web dans lesquels l'image du système d'exploitation est téléchargée avant la fin du téléchargement, l'importation échoue.

Résultats

XClarity Administrator permet de télécharger l'image SE et crée un profil d'image dans le Référentiel d'images SE.



Depuis cette page, vous pouvez effectuer les actions suivantes.

- Créez un profil de serveur de fichiers distant en cliquant sur l'icône **Configurer le serveur de fichiers** ( ).
- Personnalisez une image SE en cliquant sur l'icône **Créer un profil personnalisé** ( ).
- Modifiez une image SE en cliquant sur l'icône **Éditer** ( ).

- Importer un profil d'image SE personnalisé et l'appliquer à une image SE de base en cliquant sur **Importer/exporter le profil → Importer une image de profil personnalisé** (voir Importation d'un profil d'image SE personnalisé).
- Supprimez une image SE sélectionnée ou un profil d'image SE personnalisé en cliquant sur l'icône **Supprimer** ().
- Exporter un profil d'image SE personnalisé sélectionné en cliquant sur **Importer/exporter le profil → Exporter une image de profil personnalisé**.

Remarque : Lors de l'importation d'images Windows Server, vous devez également importer le fichier de lot associé. Lenovo regroupe le fichier d'amorçage WinPE_64.wim prédéfini et un ensemble de pilotes de périphérique dans un seul module qui peut être téléchargé depuis page Web des pilotes Windows de Lenovo et référentiel d'images WinPE puis importé dans un référentiel d'images SE. Comme le fichier de lot contient des pilotes de périphérique et des fichiers d'amorçage, vous pouvez l'importer depuis l'onglet **Pilote de périphérique** ou **Fichiers d'amorçage**..Pour plus d'informations, voir Importation de fichiers d'amorçage et Importation de pilotes de périphérique.

Personnalisation de profils d'image SE

Un *système d'exploitation de base* est l'image SE qui a été importée dans le référentiel d'images SE. L'image de base importée contient des profils prédéfinis qui décrivent les configurations d'installation pour cette image. Vous pouvez également créer des profils personnalisés dans l'image SE de base qui peut être déployée pour des configurations spécifiques. Le profil personnalisé comporte les fichiers personnalisés et des options d'installation.

Remarque : Vous ne pouvez pas créer de profil d'image SE personnalisé pour une image Microsoft Windows Server personnalisée.

Plusieurs exemples de scénarios de personnalisation et de déploiement d'images SE, y compris Windows et SLES, sont disponibles en anglais uniquement. Pour plus d'informations, voir Scénarios de bout en bout pour la configuration de nouveaux appareils.

Vous pouvez ajouter les types de fichiers suivants à un profil d'image SE personnalisé.

- **Fichiers d'amorçage**

  Un fichier d'amorçage fait office d'environnement d'installation d'amorce. Sous Windows, il s'agit d'un fichier de préinstallation Windows (WinPE). Un fichier d'amorçage WinPE est requis pour le déploiement Windows

  Lenovo XClarity Administrator prend en charge les fichiers d'amorçage prédéfinis et personnalisés.

  - **Fichiers d'amorçage prédéfinis**. Lenovo fournit un fichier d'amorçage WinPE_64.wim qui peut être utilisé pour déployer des profils d'image SE prédéfinis.

    Lenovo regroupe le fichier d'amorçage WinPE_64.wim prédéfini et un ensemble de pilotes de périphérique dans un seul module qui peut être téléchargé depuis page Web des pilotes Windows de Lenovo et référentiel d'images WinPE puis importé dans un référentiel d'images SE. Comme le fichier de lot contient des pilotes de périphérique et des fichiers d'amorçage, vous pouvez l'importer depuis l'onglet **Pilote de périphérique** ou **Fichiers d'amorçage**.

    Remarques :

    - Aucun fichier d'amorçage prédéfini n'est préchargé avec XClarity Administrator. Vous devez importer un fichier d'amorçage dans le référentiel d'images SE avant de pouvoir déployer un profil Windows.

  - Vous ne pouvez pas supprimer les fichiers d'amorçage qui ont été chargés lorsque vous avez installé XClarity Administrator ; toutefois, vous pouvez supprimer des fichiers d'amorçage qui ont été importés à partir d'un lot Lenovo.
  - XClarity Administrator requiert que les fichiers de lots importés soient signés par Lenovo. Lors de l'importation d'un fichier de lot, un fichier de signature .asc doit également être importé.
- **Fichiers d'amorçage personnalisés**. Vous pouvez créer un fichier d'amorçage WinPE pour personnaliser les options d'amorçage d'un déploiement Windows. Vous pouvez ensuite ajouter le fichier d'amorçage aux profils Windows personnalisés.

  XClarity Administrator fournit des scripts pour la création de fichiers d'amorçage dans le format approprié. Pour plus d'informations sur la création d'un fichier d'amorçage personnalisé, voir Création d'un fichier d'amorçage (WinPE) et Site Web de présentation de Windows PE (WinPE).

  Les types de fichier suivants sont pris en charge pour l'importation de fichiers d'amorçage personnalisés.

Système d'exploitation	Types de fichier d'amorçage pris en charge	Types de fichier de lot pris en charge
Linux CentOS	Non pris en charge	Non pris en charge
Microsoft® Windows® Azure Stack HCI	Non pris en charge	Non pris en charge
Microsoft Windows Hyper-V Server	Un fichier .zip contenant un fichier WinPE qui est créé à l'aide du script **genimage.cmd**	Un fichier .zip contenant les pilotes de périphérique et les fichiers d'amorçage
Microsoft Windows Server	Un fichier .zip contenant un fichier WinPE qui est créé à l'aide du script **genimage.cmd**	Un fichier .zip contenant les pilotes de périphérique et les fichiers d'amorçage
Red Hat® Enterprise Linux (RHEL) Server	Non pris en charge	Non pris en charge
Rocky Linux	Non pris en charge	Non pris en charge
SUSE® Linux Enterprise Server (SLES)	Non pris en charge	Non pris en charge
Ubuntu	Non pris en charge	Non pris en charge
VMware vSphere® Hypervisor (ESXi) avec personnalisation Lenovo	Non pris en charge	Non pris en charge

- **Pilotes de périphérique**

  Vous devez vous assurer que l'image du système d'exploitation que vous avez l'intention de déployer inclut les pilotes de périphérique Ethernet, Fibre Channel et d'adaptateur de stockage appropriés pour votre matériel. Si le pilote de périphérique de carte d'E-S n'est pas inclus dans l'image ou le profil du système d'exploitation, la carte n'est pas prise en charge pour le déploiement de système d'exploitation. Vous pouvez créer des profils d'image SE personnalisés qui incluent les pilotes de périphériques non fournis dont vous avez besoin.

  Lenovo XClarity Administrator prend en charge les pilotes de périphérique fournis ainsi que les pilotes de périphérique prédéfinis et personnalisés non fournis.

  - **Pilotes de périphérique fournis**. XClarity Administrator ne gère pas les pilotes de périphérique fournis. Installez toujours le système d'exploitation le plus récent de manière à disposer des derniers pilotes de périphérique de fournis.

Remarque : Vous pouvez ajouter des pilotes de périphérique fournis à un profil Windows personnalisé, en créant un fichier d'amorçage WinPE personnalisé et en copiant les fichiers de pilote de périphérique sur le système hôte dans le répertoire `C:\drivers`. Lorsque vous créez un profil d'images SE personnalisé qui utilise le fichier d'amorçage personnalisé, les pilotes de périphérique qui figurent dans le répertoire C:\drivers sont inclus à la fois dans WinPE et dans le système d'exploitation final. Ils sont traités comme s'ils étaient fournis par Windows. Par conséquent, vous n'avez pas besoin d'importer ces pilotes de périphérique fournis par Windows dans XClarity Administrator lorsque vous spécifiez des pilotes de périphérique à utiliser dans la création d'un profil d'images SE personnalisé.

- **Pilotes de périphérique prédéfinis**. Pour les serveurs ThinkSystem, XClarity Administrator est préchargé avec un ensemble de pilotes de périphérique prêts à l'emploi pour Linux pour permettre l'installation du système d'exploitation, ainsi qu'un réseau de base et une configuration de stockage pour le système d'exploitation final. Vous pouvez ajouter ces pilotes de périphérique prédéfinis à vos profils d'image SE personnalisés, puis déployer les profils sur vos serveurs gérés

  Lenovo regroupe également des ensembles de pilotes de périphérique prédéfinis dans un seul module qui peut être téléchargé à partir de page Web des pilotes Windows de Lenovo et référentiel d'images WinPE et importé dans le référentiel d'images SE. Actuellement, les fichiers de lots sont disponibles uniquement pour Windows. Si le fichier de lot contient des pilotes de périphérique et des fichiers d'amorçage, vous pouvez importer le fichier de lot depuis l'onglet **Pilote de périphérique** ou **Image d'amorçage**.

  Remarques :

  - Par défaut, les profils d'image SE prédéfinis incluent les pilotes de périphérique prédéfinis.
  - Vous ne pouvez pas supprimer les pilotes prédéfinis ont été chargés lorsque vous avez installé XClarity Administrator ; toutefois, vous pouvez supprimer des pilotes de périphérique prédéfinis qui ont été importés à partir d'un lot Lenovo.
  - XClarity Administrator requiert que les fichiers de lots importés soient signés par Lenovo. Lors de l'importation d'un fichier de lot, un fichier de signature .asc doit également être importé.
- **Pilotes de périphérique personnalisés**. Vous pouvez importer des pilotes de périphérique non fournis dans le référentiel d'images SE et les ajouter à un profil d'image SE personnalisé.

  Vous pouvez obtenir des pilotes de périphérique auprès de Page Web du référentiel YUM Lenovo, du fournisseur (par exemple, Red Hat) ou par le biais d'un pilote de périphérique personnalisé que vous générez vous-même. Pour certains pilotes de périphérique Windows, vous pouvez générer un pilote de périphérique personnalisé en extrayant le pilote de périphérique de l'exécutable d'installation sur votre système local et en créant un fichier d'archive .zip.

  Les types de fichier suivants sont pris en charge pour l'importation de fichiers d'appareils personnalisés.

Système d'exploitation	Types de fichier de pilote de périphérique pris en charge
Linux CentOS	Non pris en charge
Microsoft® Windows® Azure Stack HCI	Non pris en charge
Microsoft Windows Hyper-V Server	Fichier .zip contenant les fichiers de pilote de périphérique bruts qui sont généralement un regroupement de fichiers .inf, .cat et .dll.
Microsoft Windows Server	Fichier .zip contenant les fichiers de pilote de périphérique bruts qui sont généralement un regroupement de fichiers .inf, .cat et .dll.

Système d'exploitation	Types de fichier de pilote de périphérique pris en charge
Red Hat® Enterprise Linux (RHEL) Server	Disque de mise à jour de pilote au format .iso ou .rpm **Remarque :** Si vous appliquez un .rpm DUD au profil personnalisé, le .rpm est installé uniquement pour le système d'exploitation final. Il n'est pas installé dans l'environnement d'installation (initrd). Pour installer un pilote de périphérique personnalisé dans initrd, importez un .iso DUD et appliquez l'.iso au profil personnalisé.
Rocky Linux	Non pris en charge
SUSE® Linux Enterprise Server (SLES)	Disques de mise à jour de pilote au format .d'image rpm ou .iso. **Remarque :** Si vous appliquez un .rpm DUD au profil personnalisé, le .rpm est installé uniquement pour le système d'exploitation final. Il n'est pas installé dans l'environnement d'installation (initrd). Pour installer un pilote de périphérique personnalisé dans initrd, importez un .iso DUD et appliquez l'.iso au profil personnalisé.
Ubuntu	Non pris en charge
VMware vSphere® Hypervisor (ESXi) avec personnalisation Lenovo	Pilotes de périphérique au format d'image .vib

Remarque : Le référentiel des images SE peut stocker un nombre illimité de fichiers prédéfinis et personnalisés, si l'espace disponible est suffisant pour stocker les fichiers.

- **Paramètres de configuration personnalisés**

  Les paramètres de configuration décrivent les données qui doivent être collectées de manière dynamique pendant le déploiement SE. Lenovo XClarity Administrator utilise un ensemble de paramètres de configuration prédéfinis, notamment des paramètres d'emplacement global, réseau et stockage. Vous pouvez utiliser ces paramètres de configuration prédéfinis et ajouter des paramètres de configuration personnalisés qui ne sont pas disponibles via XClarity Administrator.

  Les paramètres de configuration personnalisés sont définis sous la forme d'un schéma JSON. Le schéma doit être conforme à la spécification JSON.

  Lorsque vous importez des paramètres de configuration personnalisés dans XClarity Administrator, XClarity Administrator valide le schéma JSON. Si la validation réussit, XClarity Administrator génère des macros personnalisées pour chaque paramètre.

  Vous pouvez utiliser les macros personnalisées dans le fichier sans opérateur et le script de post-installation.

  Dans des fichiers sans opérateur

  Vous pouvez associer le fichier de configuration personnalisé à un fichier sans opérateur et inclure ces macros personnalisées (et macros prédéfinies) dans le fichier sans opérateur.

  Vous pouvez ajouter un ou plusieurs fichiers de paramètres de configuration personnalisés dans un profil personnalisé. Lorsque vous déployez le profil SE sur un ensemble de serveurs cible, vous pouvez choisir le fichier de paramètres de configuration à utiliser. XClarity Administratoraffiche l'onglet **Paramètres personnalisés** dans la boîte de dialogue Déployer des images de SE en fonction du schéma JSON dans le fichier de paramètres de configuration et vous permet de définir des valeurs pour chaque paramètre (objet JSON) qui est défini dans le fichier.

  Remarque : Le déploiement SE ne se poursuivra pas si aucune entrée n'est spécifiée pour les paramètres de configuration personnalisés requis.

  Dans les scripts de post-installation

Une fois les données collectées pendant le déploiement SE, XClarity Administrator crée une instance des paramètres du fichier de configuration (qui inclut les paramètres personnalisés dans le fichier sélectionné et un sous-ensemble de paramètres prédéfinis) sur le système hôte qui peut être utilisé par le script de post-installation.

Remarques :

- Le fichier des paramètres de configuration est unique dans un profil d'image SE personnalisé.
- Vous ne pouvez pas modifier les paramètres de configuration des profils d'image SE prédéfinis.
- Les paramètres de configuration sont pris en charge uniquement pour les systèmes d'exploitation suivants :
  - Microsoft® Windows® Server
  - Red Hat® Enterprise Linux (RHEL) Server
  - Rocky Linux
  - SUSE® Linux Enterprise Server (SLES)
  - VMware vSphere® Hypervisor (ESXi) avec Lenovo Customization 6.0u3, mises à jour ultérieures et 6.5 et ultérieures.

Le référentiel des images SE peut stocker un nombre illimité de fichiers prédéfinis et personnalisés, si l'espace disponible est suffisant pour stocker les fichiers.

- **Fichiers sans opérateur personnalisés**

  Vous pouvez personnaliser les profils d'image SE pour l'utilisation de fichiers sans opérateur pour automatiser le déploiement du système d'exploitation.

  Les types de fichier suivants sont pris en charge pour les fichiers sans opérateur personnalisés.

Système d'exploitation	Types de fichier pris en charge	Informations complémentaires
Linux CentOS	Non pris en charge	
Microsoft® Windows® Azure Stack HCI	Non pris en charge	
Microsoft Windows Hyper-V Server	Non pris en charge	
Microsoft Windows Server	Sans opérateur (.xml)	Pour plus d'informations sur les fichiers sans opérateur, voir Page Web de référence à l'installation Windows sans opérateur.
Red Hat® Enterprise Linux (RHEL) Server	Kickstart (.cfg)	Pour plus d'informations sur les fichiers sans opérateur, voir Page Web Red Hat : Automatisation de l'installation avec Kickstart . Tenez compte des éléments suivants lors de l'ajout de sections %pre, %post, %firstboot dans le fichier. – Vous pouvez inclure plusieurs sections %pre, %post, % firstboot dans le fichier sans opérateur ; toutefois, tenez compte de l'ordre des sections. – Lorsque la macro recommandée **#predefined. unattendSettings.preinstallConfig#** est présente dans le fichier sans opérateur, XClarity Administrator ajoute une section %pre avant toutes les autres sections %pre dans le fichier. – Lorsque la macro recommandée **#predefined. unattendSettings.postinstallConfig#** est présente dans le fichier sans opérateur, XClarity Administrator ajoute une les sections %post et %firstboot avant toutes les autres sections %post et %firstboot dans le fichier.

Système d'exploitation	Types de fichier pris en charge	Informations complémentaires
Rocky Linux	Kickstart (.cfg)	Pour plus d'informations sur les fichiers sans opérateur, voir Page Web Red Hat : Automatisation de l'installation avec Kickstart . Tenez compte des éléments suivants lors de l'ajout de sections %pre, %post, %firstboot dans le fichier. – Vous pouvez inclure plusieurs sections %pre, %post, % firstboot dans le fichier sans opérateur ; toutefois, tenez compte de l'ordre des sections. – Lorsque la macro recommandée **#predefined. unattendSettings.preinstallConfig#** est présente dans le fichier sans opérateur, XClarity Administrator ajoute une section %pre avant toutes les autres sections %pre dans le fichier. – Lorsque la macro recommandée **#predefined. unattendSettings.postinstallConfig#** est présente dans le fichier sans opérateur, XClarity Administrator ajoute une les sections %post et %firstboot avant toutes les autres sections %post et %firstboot dans le fichier.
SUSE® Linux Enterprise Server (SLES)	AutoYast (.xml)	Pour plus d'informations sur les fichiers sans opérateur, voir SUSE : page Web AutoYaST.
Ubuntu	Non pris en charge	
VMware vSphere® Hypervisor (ESXi) avec personnalisation Lenovo	Kickstart (.cfg)	Pris en charge uniquement pour ESXi 6.0u3 et les mises à jour ultérieures et la version 6.5 et versions ultérieures. Pour plus d'informations sur les fichiers sans opérateur, voir VMware : Installation ou mise à niveau des hôtes à l'aide d'une page Web Script. Tenez compte des éléments suivants lors de l'ajout de sections %pre, %post, %firstboot dans le fichier. – Vous pouvez inclure plusieurs sections %pre, %post, % firstboot dans le fichier sans opérateur ; toutefois, tenez compte de l'ordre des sections. – Lorsque la macro recommandée **#predefined. unattendSettings.preinstallConfig#** est présente dans le fichier sans opérateur, XClarity Administrator ajoute une section %pre avant toutes les autres sections %pre dans le fichier. – Lorsque la macro recommandée **#predefined. unattendSettings.postinstallConfig#** est présente dans le fichier sans opérateur, XClarity Administrator ajoute une les sections %post et %firstboot avant toutes les autres sections %post et %firstboot dans le fichier.

Attention :

– Vous pouvez injecter des macros prédéfinies et personnalisées (paramètres de configuration) dans le fichier sans opérateur à l'aide du nom unique de l'objet. Les valeurs prédéfinies sont basées de manière dynamique basé sur les instances de XClarity Administrator. Les macros personnalisées sont basées de manière dynamique sur la saisie de l'utilisateur qui est spécifiée pendant le déploiement du système d'exploitation.

Remarques :

  - Placez le nom de macro entre des symboles dièse (#).
  - Pour les objets imbriqués, séparez chaque nom objet à l'aide d'un point (par exemple, **#server_settings.server0.locale#**).
  - Pour les macros personnalisées, n'incluez pas le nom d'objet le plus important. Pour les macros prédéfinies, ajoutez au nom de la macro le préfixe « prédéfini ».
  - Lorsqu'un objet est créé à partir d'un modèle, le nom est ajouté avec un numéro unique, en commençant par 0 (par exemple, **server0** et **server1**).
  - Vous pouvez également voir le nom de chaque macro à partir de la boîte de dialogue Déployer des images SE sous les onglets Paramètres personnalisés en passant le curseur sur l'icône Aide () en regard de chaque paramètre personnalisé.
  - Pour obtenir la liste des macros prédéfinies, voir Macros prédéfinies. Pour plus d'informations sur les paramètres de configuration et macros personnalisés, voir Macros personnalisées.
- XClarity Administratorfournit les macros prédéfinies suivantes qui sont utilisées pour communiquer l'état depuis le programme d'installation SE, ainsi que plusieurs autres étapes d'installation critique. Il est fortement recommandé d'inclure ces macros dans un fichier sans opérateur (voir Injection de macros prédéfinies et de macros personnalisées dans un fichier sans opérateur).
  - #predefined.unattendSettings.preinstallConfig#
  - #predefined.unattendSettings postinstallConfig#

- **Scripts d'installation personnalisés**

  Vous pouvez personnaliser les profils d'image SE pour exécuter un script d'installation une fois le déploiement du système d'exploitation terminé.

  Actuellement, seuls les scripts de post-installation sont pris en charge.

  Le tableau suivant répertorie les types de fichiers des scripts d'installation pris en charge par Lenovo XClarity Administrator pour chaque système d'exploitation. Notez que certaines versions du système opération ne prennent pas en charge tous les types de fichier pris en charge par XClarity Administrator(par exemple, des versions RHEL peuvent ne pas inclure Perl dans le profil minimal et, par conséquent, les scripts Perl ne s'exécuteront pas). Assurez-vous que vous utilisez le type de fichier approprié pour les versions de système d'exploitation que vous voulez déployer.

Système d'exploitation	Types de fichier pris en charge	Informations complémentaires
Linux CentOS	Non pris en charge	
Microsoft® Windows® Azure Stack HCI	Non pris en charge	
Microsoft Windows Hyper-V Server	Non pris en charge	
Microsoft® Windows® Server	Fichier de commande (.cmd), PowerShell (.ps1)	Le chemin d'accès aux fichiers et données personnalisés par défaut est `C:\lxca`. Pour plus d'informations sur les scripts d'installation, voir Site Web d'ajout d'un script personnalisé à la configuration Windows
Red Hat® Enterprise Linux (RHEL) Server	Bash (.sh), Perl (.pm ou .pl), Python (.py)	Le chemin d'accès aux fichiers et données personnalisés par défaut est `/home/lxca`. Pour plus d'informations sur les scripts d'installation, voir RHEL : Page Web des scripts de post-installation

Système d'exploitation	Types de fichier pris en charge	Informations complémentaires
Rocky Linux	Bash (.sh), Perl (.pm ou .pl), Python (.py)	Le chemin d'accès aux fichiers et données personnalisés par défaut est `/home/lxca`. Pour plus d'informations sur les scripts d'installation, voir RHEL : Page Web des scripts de post-installation
SUSE® Linux Enterprise Server (SLES)	Bash (.sh), Perl (.pm ou .pl), Python (.py)	Le chemin d'accès aux fichiers et données personnalisés par défaut est `/home/lxca`. Pour plus d'informations sur les scripts d'installation, voir SUSE : Page Web des scripts utilisateur personnalisés
Ubuntu	Non pris en charge	
VMware vSphere® Hypervisor (ESXi) avec personnalisation Lenovo	Bash (.sh), Python (.py)	Le chemin d'accès aux fichiers et données personnalisés par défaut est `/home/lxca`. Pour plus d'informations sur les scripts d'installation, voir VMware : Page Web de scripts d'installation et de mise à niveau

- **Logiciels personnalisés**

  Vous pouvez personnaliser les profils d'image SE pour installer des contenus logiciels personnalisés une fois le déploiement SE terminé et les scripts de post-installation exécutés.

  Les types de fichier suivants sont pris en charge pour les logiciels personnalisés.

Système d'exploitation	Types de fichier pris en charge	Informations complémentaires
Linux CentOS	Non pris en charge	
Microsoft® Windows® Azure Stack HCI	Non pris en charge	
Microsoft Windows Hyper-V Server	Non pris en charge	
Microsoft Windows® Server	Un fichier .zip contenant le contenu du logiciel.	Le chemin d'accès aux fichiers et données personnalisés par défaut est `C:\lxca`.
Red Hat® Enterprise Linux (RHEL) Server	Un fichier .tar.gz contenant le contenu du logiciel	Le chemin d'accès aux fichiers et données personnalisés par défaut est `/home/lxca`.
SUSE® Linux Enterprise Server (SLES)	Un fichier .tar.gz contenant le contenu du logiciel	Le chemin d'accès aux fichiers et données personnalisés par défaut est `/home/lxca`.
Rocky Linux	Un fichier .tar.gz contenant le contenu du logiciel	Le chemin d'accès aux fichiers et données personnalisés par défaut est `/home/lxca`.
Ubuntu	Non pris en charge	
VMware vSphere® Hypervisor (ESXi) avec personnalisation Lenovo	Un fichier .tar.gz contenant le contenu du logiciel	Le chemin d'accès aux fichiers et données personnalisés par défaut est `/home/lxca`.

Importation d'un profil d'image SE personnalisé

Vous pouvez importer un profil d'image SE personnalisé et l'ajouter à une image SE de base compatible existante.

À propos de cette tâche

L'image SE de base doit être préalablement importée pour que vous puissiez importer un profil personnalisé.

Un profil d'image SE personnalisé peut être ajouté uniquement à une image SE de base du même type. Par exemple, si le profil exporté s'applique à une image Windows 2016, il ne peut être importé et ajouté que dans une image Windows 2016 qui existe dans le référentiel des images SE.

Le référentiel des images SE peut stocker un nombre illimité de profils personnalisés, si l'espace disponible est suffisant pour stocker les fichiers.

Procédure

Pour importer un profil d'image SE personnalisé, procédez comme suit.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Distribution → Gérer les images de SE** pour afficher la page Déployer un système d'exploitation : déployer des images de SE.

Etape 2. Sur l'onglet **Images SE**, sélectionnez l'image SE de base à laquelle vous souhaitez ajouter le profil d'image SE personnalisé.

Etape 3. Cliquez sur **Importer/exporter le profil → Importer une image de profil personnalisé**. La boîte de dialogue Importer un profil d'image SE personnalisé s'affiche.

Etape 4. Cliquez sur l'onglet **Importation locale** pour télécharger des fichiers à partir du système local ou cliquez sur l'onglet **Importation à distance** pour télécharger des fichiers à partir d'un serveur de fichiers distant.

Remarque : Pour télécharger un fichier à partir d'un serveur de fichiers distant, vous devez d'abord créer un profil de serveur de fichiers distant en cliquant sur l'icône **Configurer le serveur de fichiers** (). Pour plus d'informations, voir Configuration d'un serveur de fichiers distant .

Etape 5. Si vous choisissez d'utiliser un serveur de fichiers distant, sélectionnez-le dans la liste **Serveur de fichiers distant**.

Etape 6. Entrez le nom du profil ou cliquez sur **Parcourir** pour rechercher le profil que vous souhaitez importer.

Etape 7. **Facultatif :** Pour les importations locales, sélectionnez un type de total de contrôle pour vérifier que le fichier en cours de téléchargement n'est pas endommagé et copiez et collez la valeur de total de contrôle dans la zone de texte fournie.

Si vous sélectionnez un type de total de contrôle, vous devez indiquer une valeur de total de contrôle pour vérifier l'intégrité et la sécurité du fichier téléchargé. La valeur doit venir de la source sécurisée d'une organisation fiable. Si le fichier téléchargé correspond à la valeur de total de contrôle, le déploiement peut être poursuivi en toute sécurité. Sinon, vous devez télécharger à nouveau le fichier ou vérifier la valeur de total de contrôle.

Trois types de total de contrôle sont pris en charge :
- **MD5**
- **SHA1**
- **SHA256**

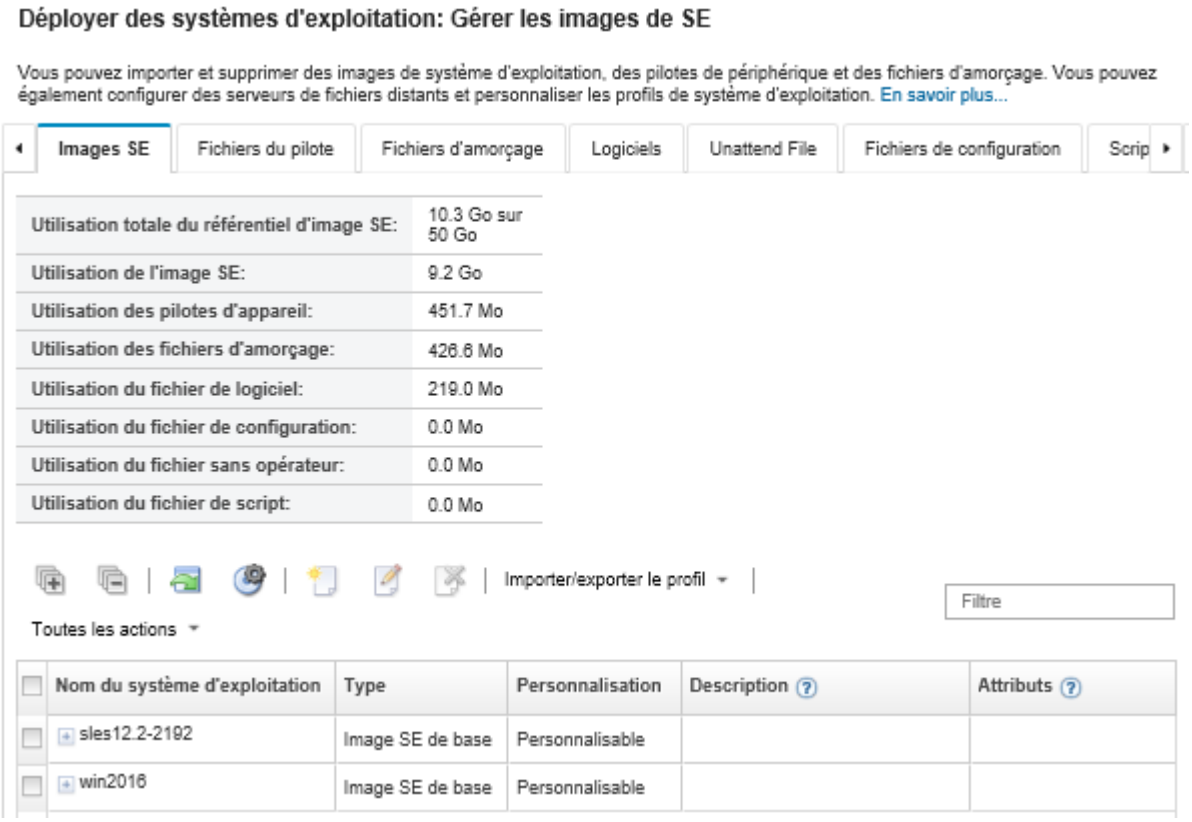
Etape 8. Cliquez sur **Importer**.

Astuce : Le fichier est téléchargé via une connexion réseau sécurisée. Par conséquent, la fiabilité et les performances du réseau ont une incidence sur le temps nécessaire à l'importation du fichier.

Si vous fermez l'onglet ou la fenêtre de navigateur Web dans lesquels le fichier est téléchargé en local avant la fin du téléchargement, l'importation échoue.

Après avoir terminé

Le profil d'image SE personnalisé est répertorié sous le système d'exploitation de base sur la page Gérer les images de SE.



Depuis cette page, vous pouvez effectuer les actions suivantes :

- Créer un profil d'image SE personnalisé (voir Création d'un profil d'image SE personnalisé).
- Exportez un profil d'image SE personnalisé sélectionné en cliquant sur **Importer/exporter le profil → Exporter une image de profil personnalisé**.

  Important : Vous pouvez exporter des profils d'image SE personnalisés sur un serveur de fichiers distant configuré pour l'utilisation des protocoles FTP ou SFTP. Vous ne pouvez pas exporter sur un serveur de fichiers distant configuré pour l'utilisation des protocoles HTTP ou HTTPS.
- Modifier un profil d'image SE personnalisé sélectionné en cliquant sur l'icône **Éditer** ( ).
- Retirer un profil d'image SE personnalisé sélectionné en cliquant sur l'icône **Supprimer** ( ).

Importation de fichiers d'amorçage

Vous pouvez importer des fichiers d'amorçage dans le référentiel d'images SE. Ces fichiers peuvent ensuite être utilisés pour personnaliser et déployer des images Windows.

À propos de cette tâche

Un fichier d'amorçage fait office d'environnement d'installation d'amorce. Sous Windows, il s'agit d'un fichier de préinstallation Windows (WinPE). Un fichier d'amorçage WinPE est requis pour le déploiement Windows

Lenovo XClarity Administrator prend en charge les fichiers d'amorçage prédéfinis et personnalisés.

- **Fichiers d'amorçage prédéfinis**. Lenovo fournit un fichier d'amorçage WinPE_64.wim qui peut être utilisé pour déployer des profils d'image SE prédéfinis.

  Lenovo regroupe le fichier d'amorçage WinPE_64.wim prédéfini et un ensemble de pilotes de périphérique dans un seul module qui peut être téléchargé depuis page Web des pilotes Windows de Lenovo et référentiel d'images WinPE puis importé dans un référentiel d'images SE. Comme le fichier de lot contient des pilotes de périphérique et des fichiers d'amorçage, vous pouvez l'importer depuis l'onglet **Pilote de périphérique** ou **Fichiers d'amorçage**.

  Remarques :

  – Aucun fichier d'amorçage prédéfini n'est préchargé avec XClarity Administrator. Vous devez importer un fichier d'amorçage dans le référentiel d'images SE avant de pouvoir déployer un profil Windows.

  – Vous ne pouvez pas supprimer les fichiers d'amorçage qui ont été chargés lorsque vous avez installé XClarity Administrator ; toutefois, vous pouvez supprimer des fichiers d'amorçage qui ont été importés à partir d'un lot Lenovo.

  – XClarity Administrator requiert que les fichiers de lots importés soient signés par Lenovo. Lors de l'importation d'un fichier de lot, un fichier de signature .asc doit également être importé.

- **Fichiers d'amorçage personnalisés**. Vous pouvez créer un fichier d'amorçage WinPE pour personnaliser les options d'amorçage d'un déploiement Windows. Vous pouvez ensuite ajouter le fichier d'amorçage aux profils Windows personnalisés.

  XClarity Administrator fournit des scripts pour la création de fichiers d'amorçage dans le format approprié. Pour plus d'informations sur la création d'un fichier d'amorçage personnalisé, voir Création d'un fichier d'amorçage (WinPE) et Site Web de présentation de Windows PE (WinPE).

  Les types de fichier suivants sont pris en charge pour l'importation de fichiers d'amorçage personnalisés.

Système d'exploitation	Types de fichier d'amorçage pris en charge	Types de fichier de lot pris en charge
Linux CentOS	Non pris en charge	Non pris en charge
Microsoft® Windows® Azure Stack HCI	Non pris en charge	Non pris en charge
Microsoft Windows Hyper-V Server	Un fichier .zip contenant un fichier WinPE qui est créé à l'aide du script **genimage.cmd**	Un fichier .zip contenant les pilotes de périphérique et les fichiers d'amorçage
Microsoft Windows Server	Un fichier .zip contenant un fichier WinPE qui est créé à l'aide du script **genimage.cmd**	Un fichier .zip contenant les pilotes de périphérique et les fichiers d'amorçage
Red Hat® Enterprise Linux (RHEL) Server	Non pris en charge	Non pris en charge
Rocky Linux	Non pris en charge	Non pris en charge
SUSE® Linux Enterprise Server (SLES)	Non pris en charge	Non pris en charge

Système d'exploitation	Types de fichier d'amorçage pris en charge	Types de fichier de lot pris en charge
Ubuntu	Non pris en charge	Non pris en charge
VMware vSphere® Hypervisor (ESXi) avec personnalisation Lenovo	Non pris en charge	Non pris en charge

Remarque : Le référentiel des images SE peut stocker un nombre illimité de fichiers prédéfinis et personnalisés, si l'espace disponible est suffisant pour stocker les fichiers.

Procédure

- Pour importer un fichier de lot contenant les fichiers d'amorçage dans le référentiel d'images SE, procédez comme suit.
  1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Gérer les images de SE** pour afficher la page Déployer un système d'exploitation : déployer des images de SE.
  2. Cliquez sur l'onglet **Fichiers d'amorçage**.

  3. Cliquez sur **Téléchargements → Fichiers de lots Windows** pour accéder à la page Web de Support Lenovo, puis téléchargez le fichier de lot approprié et le fichier de signature associé pour l'image SE sur le système local.
  4. Cliquez sur l'icône **Importer le fichier de lot** ( ). La boîte de dialogue Importer le fichier de lot s'affiche.
  5. Cliquez sur l'onglet **Importation locale** pour télécharger des fichiers à partir du système local ou cliquez sur l'onglet **Importation à distance** pour télécharger des fichiers à partir d'un serveur de fichiers distant.

     Remarque : Pour télécharger un fichier à partir d'un serveur de fichiers distant, vous devez d'abord créer un profil de serveur de fichiers distant en cliquant sur l'icône **Configurer le serveur de fichiers** ( ). Pour plus d'informations, voir Configuration d'un serveur de fichiers distant .
  6. Si vous choisissez d'utiliser un serveur de fichiers distant, sélectionnez-le dans la liste **Serveur de fichiers distant**.
  7. Sélectionnez le type et la version du système d'exploitation.
  8. Entrez le nom de fichier du fichier de lot et du fichier de signature associé, ou cliquez sur **Parcourir** pour rechercher les fichiers que vous souhaitez importer.
  9. **Facultatif :** Entrez une description pour le fichier de lot.
  10. Cliquez sur **Importer**.

Astuce : Le fichier est téléchargé via une connexion réseau sécurisée. Par conséquent, la fiabilité et les performances du réseau ont une incidence sur le temps nécessaire à l'importation du fichier.

Si vous fermez l'onglet ou la fenêtre de navigateur Web dans lesquels le fichier est téléchargé en local avant la fin du téléchargement, l'importation échoue.

- Pour importer un fichier d'amorçage dans le référentiel d'images SE, procédez comme suit.
  1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Gérer les images de SE** pour afficher la page Déployer un système d'exploitation : déployer des images de SE.
  2. Cliquez sur l'onglet **Fichiers d'amorçage**.
  3. Cliquez sur l'icône **Importer fichier** (). La boîte de dialogue Importer un fichier s'affiche.
  4. Cliquez sur l'onglet **Importation locale** pour télécharger des fichiers à partir du système local ou cliquez sur l'onglet **Importation à distance** pour télécharger des fichiers à partir d'un serveur de fichiers distant.

     Remarque : Pour télécharger un fichier à partir d'un serveur de fichiers distant, vous devez d'abord créer un profil de serveur de fichiers distant en cliquant sur l'icône **Configurer le serveur de fichiers** (). Pour plus d'informations, voir Configuration d'un serveur de fichiers distant .
  5. Si vous choisissez d'utiliser un serveur de fichiers distant, sélectionnez-le dans la liste **Serveur de fichiers distant**.
  6. Sélectionnez le type et la version du système d'exploitation.
  7. Entrez le nom de fichier ou cliquez sur **Parcourir** pour rechercher le fichier d'amorçage que vous souhaitez importer.
  8. **Facultatif :** Entrez une description pour le fichier d'amorçage.
  9. **Facultatif :** Sélectionnez un type de total de contrôle pour vérifier que le fichier en cours de téléchargement n'est pas endommagé et copiez et collez la valeur de total de contrôle dans la zone de texte fournie.

     Si vous sélectionnez un type de total de contrôle, vous devez indiquer une valeur de total de contrôle pour vérifier l'intégrité et la sécurité du fichier téléchargé. La valeur doit venir de la source sécurisée d'une organisation fiable. Si le fichier téléchargé correspond à la valeur de total de contrôle, le déploiement peut être poursuivi en toute sécurité. Sinon, vous devez télécharger à nouveau le fichier ou vérifier la valeur de total de contrôle.

     Trois types de total de contrôle sont pris en charge :
     - **MD5**
     - **SHA1**
     - **SHA256**
  10. Cliquez sur **Importer**.

      Astuce : Le fichier est téléchargé via une connexion réseau sécurisée. Par conséquent, la fiabilité et les performances du réseau ont une incidence sur le temps nécessaire à l'importation du fichier.

      Si vous fermez l'onglet ou la fenêtre de navigateur Web dans lesquels le fichier est téléchargé en local avant la fin du téléchargement, l'importation échoue.

Après avoir terminé

Le fichier d'amorçage est répertorié sous l'onglet **Fichiers d'amorçage** de la page Gérer les images de SE.

Depuis cette page, vous pouvez effectuer les actions suivantes.

- Créez un profil de serveur de fichiers distant en cliquant sur l'icône **Configurer le serveur de fichiers** ( ).
- Retirez un fichier d'amorçage sélectionné en cliquant sur l'icône **Supprimer** ( ).
- Ajoutez un fichier d'amorçage à un profil d'image SE personnalisé (voir Création d'un profil d'image SE personnalisé).

Création d'un fichier d'amorçage (WinPE)

Vous pouvez créer des fichiers d'amorçage qui peuvent être utilisés pour créer des images Windows.

Avant de commencer

- Assurez-vous que la version la plus récente du système d'exploitation que vous allez mettre à disposition est installée sur l'hôte. Par exemple, si vous prévoyez de mettre à disposition Windows 2016 à l'aide des fichiers WinPE, installez Windows 2016 sur l'hôte.
- Vérifiez que la version de Microsoft ADK compatible avec le système d'exploitation installé est également installée sur l'hôte. Par exemple, Windows 2012R2 requiert la mise à jour ADK version 8.1.
- Obtenez les pilotes de périphérique, au format .inf, que vous souhaitez ajouter au fichier d'amorçage.

  Vous pouvez obtenir des pilotes de périphérique auprès de Page Web du référentiel YUM Lenovo, du fournisseur (par exemple, Red Hat) ou par le biais d'un pilote de périphérique personnalisé que vous générez vous-même. Pour certains pilotes de périphérique Windows, vous pouvez générer un pilote de périphérique personnalisé en extrayant le pilote de périphérique de l'exécutable d'installation sur votre système local et en créant un fichier d'archive .zip.

  Lenovo regroupe également des ensembles de pilotes de périphérique prédéfinis dans un seul module qui peut être téléchargé à partir de page Web des pilotes Windows de Lenovo et référentiel d'images WinPE et importé dans le référentiel d'images SE. Actuellement, les fichiers de lots sont disponibles uniquement pour Windows. Si le fichier de lot contient des pilotes de périphérique et des fichiers d'amorçage, vous pouvez importer le fichier de lot depuis l'onglet **Pilote de périphérique** ou **Image d'amorçage**.
- Téléchargez les fichiers `genimage.cmd` et `startnet.cmd` sur l'hôte dans un répertoire temporaire, par exemple `C:\customwim`.

  La commande `genimage.cmd` permet de générer les fichiers d'amorçage WinPE, y compris le fichier .wim. La commande `startnet.cmd` est utilisée par XClarity Administrator pour amorcer le programme d'installation de Windows.
- Déterminez comment vous voulez injecter des pilotes de périphérique dans le fichier d'amorçage. Utilisez pour cela l'une des deux méthodes suivantes :
  - Ajoutez des pilotes de périphérique fournis avec Windows à un profil Windows personnalisé en copiant les fichiers de pilote de périphérique sur le système hôte dans le répertoire C:\drivers. Ceux-ci seront inclus ultérieurement dans le fichier d'amorçage lors de l'exécution de genimage.cmd.

    Remarque : Lorsque vous créez un profil d'images SE personnalisé qui utilise le fichier d'amorçage personnalisé, les pilotes de périphérique qui figurent dans le répertoire C:\drivers sont inclus à la fois dans WinPE et dans le système d'exploitation final. Ils sont traités comme s'ils étaient fournis par Windows. Par conséquent, vous n'avez pas besoin d'importer ces pilotes de périphérique fournis par Windows dans XClarity Administrator lorsque vous spécifiez des pilotes de périphérique à utiliser dans la création d'un profil d'images SE personnalisé.
  - Ajoutez des pilotes de périphérique non fournis avec Windows directement dans le fichier d'amorçage.

    Remarque : Si vous utilisez cette méthode, les pilotes de périphérique sont uniquement appliqués au fichier d'amorçage et, par conséquent, à l'environnement d'installation WinPE. Les pilotes de périphérique ne sont pas appliqués au système d'exploitation installé final. Vous devez les importer

manuellement dans le référentiel d'images SE et les sélectionner lors de la personnalisation du profil d'image SE.

- Pour plus d'informations sur les fichiers d'amorçage, voir Site Web de présentation de Windows PE (WinPE).

Procédure

Pour créer un fichier d'amorçage, procédez comme suit.

Etape 1. À l'aide d'un ID utilisateur disposant de droits d'administrateur, exécutez la commande Windows ADK « Deployment and Imaging Tools Environment. » Une session de commande s'affiche.

Etape 2. Depuis la session de commande, accédez au répertoire contenant les fichiers `genimage.cmd` et `starnet.cmd` téléchargés (par exemple `C:\customwim`).

Etape 3. Assurez-vous qu'aucune image préalablement monté ne se trouve sur l'hôte, en exécutant la commande suivante :
```
dism /get-mountedwiminfo
```

S'il y a des images montées, supprimez-les à l'aide de la commande suivante :

```
dism /unmount-wim /MountDir:C:\<mount_path> /Discard
```

Etape 4. Si vous ajoutez des pilotes de périphérique fournis avec Windows à un profil Windows personnalisé, copiez les fichiers de pilote de périphérique bruts, au format .inf, sur le système hôte dans le répertoire `C:\drivers`.

Etape 5. Exécutez la commande suivante pour générer le fichiers d'amorçage, au format .wim, puis patientez quelques minutes le temps que la commande s'exécute.
```
genimage.cmd amd64 <ADK_Version>
```

Où <*ADK_Version*> est l'une des valeurs suivantes.

- **8.1**. Pour Windows 2012 R2
- **10**. Pour Windows 2016

Cette commande crée le fichier d'amorçage : `C:\WinPE_64\media\Boot\WinPE_64.wim`.

Etape 6. Montez le fichier d'amorçage en exécutant la commande suivante :
```
DISM /Mount-Image /ImageFile:C:\WinPE_64\media\Boot\WinPE_64.wim /index:1 /MountDir:C:\WinPE_64\mount
```

Etape 7. Si vous ajoutez des pilotes de périphérique non fournis avec Windows directement dans le fichier d'amorçage, procédez comme suit.

1. Créez la structure de répertoire suivante, où <*os_release*> est `2012`, `2012R2` ou `2016`
   `drivers\<os_release>\`
2. Copiez les pilotes de périphérique, au format .inf, dans un répertoire de ce chemin, par exemple :
   `drivers\<os_release>\<driver1>\<driver1_files>`
3. Copiez le répertoire `drivers` dans le répertoire de montage, par exemple :
   `C:\WinPE_64\mount\drivers`

Etape 8. Apportez des personnalisations supplémentaires au fichier d'amorçage, comme l'ajout de dossiers, de fichiers, de scripts de démarrage, de modules linguistiques et d'applications. Pour plus d'informations sur la personnalisation des fichiers d'amorçage, consultez le Site Web sur le montage et la personnalisation WinPE.

Etape 9. Démontez l'image en exécutant la commande suivante.
```
DISM /Unmount-Image /MountDir:C:\WinPE_64\mount /commit
```

Etape 10. Compressez le contenu du répertoire `C:\WinPE_64\media` dans un fichier zip appelé `WinPE_64.zip`.

Etape 11. Importez le fichier .zip dans XClarity Administrator (voir Importation de fichiers d'amorçage).

Importation de pilotes de périphérique

Vous pouvez importer des pilotes de périphériques et des fichiers d'amorçage dans le référentiel d'images SE. Ces fichiers peuvent ensuite être utilisés pour personnaliser des images Linux et Windows.

À propos de cette tâche

Vous devez vous assurer que l'image du système d'exploitation que vous avez l'intention de déployer inclut les pilotes de périphérique Ethernet, Fibre Channel et d'adaptateur de stockage appropriés pour votre matériel. Si le pilote de périphérique de carte d'E-S n'est pas inclus dans l'image ou le profil du système d'exploitation, la carte n'est pas prise en charge pour le déploiement de système d'exploitation. Vous pouvez créer des profils d'image SE personnalisés qui incluent les pilotes de périphériques non fournis dont vous avez besoin.

Lenovo XClarity Administrator prend en charge les pilotes de périphérique fournis ainsi que les pilotes de périphérique prédéfinis et personnalisés non fournis.

- **Pilotes de périphérique fournis**. XClarity Administrator ne gère pas les pilotes de périphérique fournis. Installez toujours le système d'exploitation le plus récent de manière à disposer des derniers pilotes de périphérique de fournis.

  Remarque : Vous pouvez ajouter des pilotes de périphérique fournis à un profil Windows personnalisé, en créant un fichier d'amorçage WinPE personnalisé et en copiant les fichiers de pilote de périphérique sur le système hôte dans le répertoire `C:\drivers`. Lorsque vous créez un profil d'images SE personnalisé qui utilise le fichier d'amorçage personnalisé, les pilotes de périphérique qui figurent dans le répertoire C:\drivers sont inclus à la fois dans WinPE et dans le système d'exploitation final. Ils sont traités comme s'ils étaient fournis par Windows. Par conséquent, vous n'avez pas besoin d'importer ces pilotes de périphérique fournis par Windows dans XClarity Administrator lorsque vous spécifiez des pilotes de périphérique à utiliser dans la création d'un profil d'images SE personnalisé.
- **Pilotes de périphérique prédéfinis**. Pour les serveurs ThinkSystem, XClarity Administrator est préchargé avec un ensemble de pilotes de périphérique prêts à l'emploi pour Linux pour permettre l'installation du système d'exploitation, ainsi qu'un réseau de base et une configuration de stockage pour le système d'exploitation final. Vous pouvez ajouter ces pilotes de périphérique prédéfinis à vos profils d'image SE personnalisés, puis déployer les profils sur vos serveurs gérés

  Lenovo regroupe également des ensembles de pilotes de périphérique prédéfinis dans un seul module qui peut être téléchargé à partir de page Web des pilotes Windows de Lenovo et référentiel d'images WinPE et importé dans le référentiel d'images SE. Actuellement, les fichiers de lots sont disponibles uniquement pour Windows. Si le fichier de lot contient des pilotes de périphérique et des fichiers d'amorçage, vous pouvez importer le fichier de lot depuis l'onglet **Pilote de périphérique** ou **Image d'amorçage**.

  Remarques :

  - Par défaut, les profils d'image SE prédéfinis incluent les pilotes de périphérique prédéfinis.
  - Vous ne pouvez pas supprimer les pilotes prédéfinis ont été chargés lorsque vous avez installé XClarity Administrator ; toutefois, vous pouvez supprimer des pilotes de périphérique prédéfinis qui ont été importés à partir d'un lot Lenovo.
  - XClarity Administrator requiert que les fichiers de lots importés soient signés par Lenovo. Lors de l'importation d'un fichier de lot, un fichier de signature .asc doit également être importé.
- **Pilotes de périphérique personnalisés**. Vous pouvez importer des pilotes de périphérique non fournis dans le référentiel d'images SE et les ajouter à un profil d'image SE personnalisé.

  Vous pouvez obtenir des pilotes de périphérique auprès de Page Web du référentiel YUM Lenovo, du fournisseur (par exemple, Red Hat) ou par le biais d'un pilote de périphérique personnalisé que vous générez vous-même. Pour certains pilotes de périphérique Windows, vous pouvez générer un pilote de

périphérique personnalisé en extrayant le pilote de périphérique de l'exécutable d'installation sur votre système local et en créant un fichier d'archive .zip.

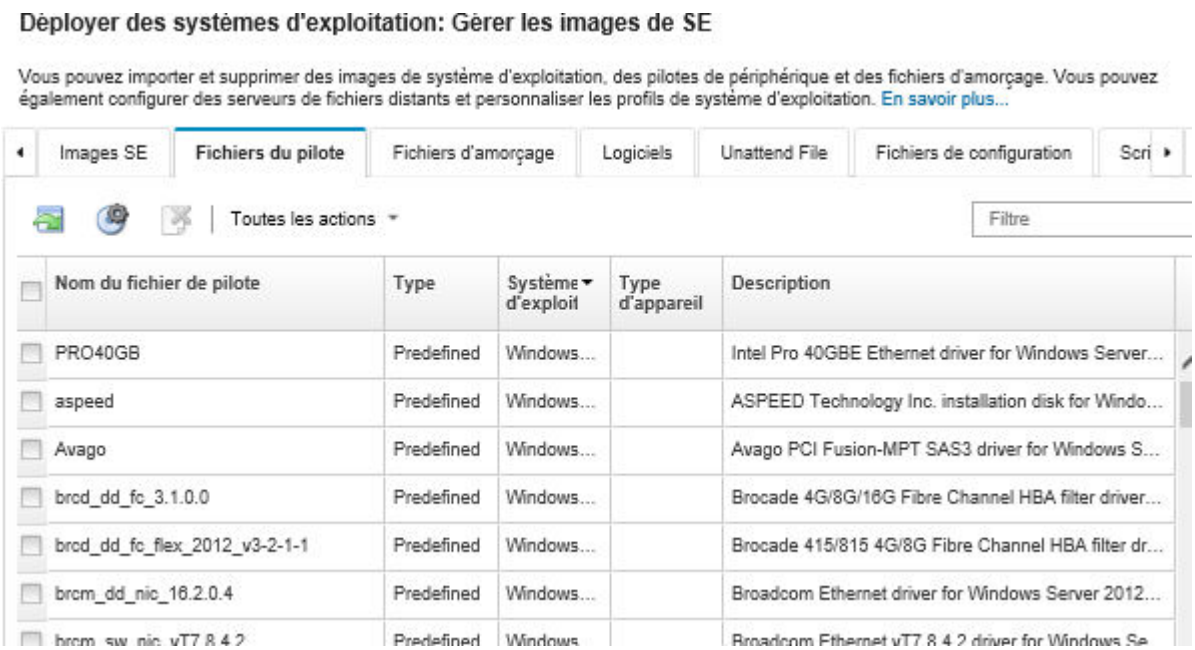
Les types de fichier suivants sont pris en charge pour l'importation de fichiers d'appareils personnalisés.

Système d'exploitation	Types de fichier de pilote de périphérique pris en charge
Linux CentOS	Non pris en charge
Microsoft® Windows® Azure Stack HCI	Non pris en charge
Microsoft Windows Hyper-V Server	Fichier .zip contenant les fichiers de pilote de périphérique bruts qui sont généralement un regroupement de fichiers .inf, .cat et .dll.
Microsoft Windows Server	Fichier .zip contenant les fichiers de pilote de périphérique bruts qui sont généralement un regroupement de fichiers .inf, .cat et .dll.
Red Hat® Enterprise Linux (RHEL) Server	Disque de mise à jour de pilote au format .iso ou .rpm **Remarque :** Si vous appliquez un .rpm DUD au profil personnalisé, le .rpm est installé uniquement pour le système d'exploitation final. Il n'est pas installé dans l'environnement d'installation (initrd). Pour installer un pilote de périphérique personnalisé dans initrd, importez un .iso DUD et appliquez l'. iso au profil personnalisé.
Rocky Linux	Non pris en charge
SUSE® Linux Enterprise Server (SLES)	Disques de mise à jour de pilote au format .d'image rpm ou .iso. **Remarque :** Si vous appliquez un .rpm DUD au profil personnalisé, le .rpm est installé uniquement pour le système d'exploitation final. Il n'est pas installé dans l'environnement d'installation (initrd). Pour installer un pilote de périphérique personnalisé dans initrd, importez un .iso DUD et appliquez l'. iso au profil personnalisé.
Ubuntu	Non pris en charge
VMware vSphere® Hypervisor (ESXi) avec personnalisation Lenovo	Pilotes de périphérique au format d'image .vib

Remarque : Le référentiel des images SE peut stocker un nombre illimité de fichiers prédéfinis et personnalisés, si l'espace disponible est suffisant pour stocker les fichiers.

Procédure

- Pour importer un fichier de lot Windows contenant des pilotes de périphérique dans le référentiel d'images SE, procédez comme suit.
  1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Gérer les images de SE** pour afficher la page Déployer un système d'exploitation : déployer des images de SE.
  2. Cliquez sur l'onglet **Fichiers du pilote**.



3. Cliquez sur **Téléchargements → Fichiers de lots Windows** pour accéder à la page Web de Support Lenovo, puis téléchargez le fichier de lot approprié et le fichier de signature associé pour l'image SE sur le système local.
4. Cliquez sur l'icône **Importer le fichier de lot** ( ). La boîte de dialogue Importer le fichier de lot s'affiche.
5. Cliquez sur l'onglet **Importation locale** pour télécharger des fichiers à partir du système local ou cliquez sur l'onglet **Importation à distance** pour télécharger des fichiers à partir d'un serveur de fichiers distant.

   Remarque : Pour télécharger un fichier à partir d'un serveur de fichiers distant, vous devez d'abord créer un profil de serveur de fichiers distant en cliquant sur l'icône **Configurer le serveur de fichiers** ( ). Pour plus d'informations, voir Configuration d'un serveur de fichiers distant .
6. Si vous choisissez d'utiliser un serveur de fichiers distant, sélectionnez-le dans la liste **Serveur de fichiers distant**.
7. Sélectionnez le type et la version du système d'exploitation.
8. Entrez le nom de fichier du fichier de lot et du fichier de signature associé, ou cliquez sur **Parcourir** pour rechercher les fichiers que vous souhaitez importer.
9. **Facultatif :** Entrez une description pour le fichier de lot.
10. Cliquez sur **Importer**.

    Astuce : Le fichier est téléchargé via une connexion réseau sécurisée. Par conséquent, la fiabilité et les performances du réseau ont une incidence sur le temps nécessaire à l'importation du fichier.

    Si vous fermez l'onglet ou la fenêtre de navigateur Web dans lesquels le fichier est téléchargé en local avant la fin du téléchargement, l'importation échoue.

- Pour importer un fichier de pilote de périphérique dans le référentiel d'images SE, procédez comme suit.
  1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Gérer les images de SE** pour afficher la page Déployer un système d'exploitation : déployer des images de SE.
  2. Cliquez sur l'onglet **Fichiers du pilote**.
  3. Cliquez sur l'icône **Importer fichier** ( ). La boîte de dialogue Importer un fichier s'affiche.

4. Cliquez sur l'onglet **Importation locale** pour télécharger des fichiers à partir du système local ou cliquez sur l'onglet **Importation à distance** pour télécharger des fichiers à partir d'un serveur de fichiers distant.

   Remarque : Pour télécharger un fichier à partir d'un serveur de fichiers distant, vous devez d'abord créer un profil de serveur de fichiers distant en cliquant sur l'icône **Configurer le serveur de fichiers** (). Pour plus d'informations, voir Configuration d'un serveur de fichiers distant .
5. Si vous choisissez d'utiliser un serveur de fichiers distant, sélectionnez-le dans la liste **Serveur de fichiers distant**.
6. Sélectionnez le type et la version du système d'exploitation.
7. Entrez le nom de fichier ou cliquez sur **Parcourir** pour rechercher le pilote de périphérique que vous souhaitez importer.
8. **Facultatif :** Entrez une description pour le pilote de périphérique.
9. **Facultatif :** Sélectionnez un type de total de contrôle pour vérifier que le fichier en cours de téléchargement n'est pas endommagé et copiez et collez la valeur de total de contrôle dans la zone de texte fournie.

   Si vous sélectionnez un type de total de contrôle, vous devez indiquer une valeur de total de contrôle pour vérifier l'intégrité et la sécurité du fichier téléchargé. La valeur doit venir de la source sécurisée d'une organisation fiable. Si le fichier téléchargé correspond à la valeur de total de contrôle, le déploiement peut être poursuivi en toute sécurité. Sinon, vous devez télécharger à nouveau le fichier ou vérifier la valeur de total de contrôle.

   Trois types de total de contrôle sont pris en charge :
   - **MD5**
   - **SHA1**
   - **SHA256**
10. Cliquez sur **Importer**.

    Astuce : Le fichier est téléchargé via une connexion réseau sécurisée. Par conséquent, la fiabilité et les performances du réseau ont une incidence sur le temps nécessaire à l'importation du fichier.

    Si vous fermez l'onglet ou la fenêtre de navigateur Web dans lesquels le fichier est téléchargé en local avant la fin du téléchargement, l'importation échoue.

Après avoir terminé

L'image de pilote de périphérique est répertoriée sur l'onglet **Fichiers du pilote** de la page Gérer les images de SE.

Depuis cette page, vous pouvez effectuer les actions suivantes.

- Créez un profil de serveur de fichiers distant en cliquant sur l'icône **Configurer le serveur de fichiers** ().
- Retirer un pilote de périphérique sélectionné en cliquant sur l'icône **Supprimer** ().
- Ajoutez un pilote de périphérique à un profil d'image SE personnalisé (voir Création d'un profil d'image SE personnalisé).

Importation de paramètres de configuration personnalisés

Les paramètres de configuration décrivent les données qui doivent être collectées de manière dynamique pendant le déploiement SE. Lenovo XClarity Administrator utilise un ensemble de paramètres de configuration prédéfinis, notamment des paramètres d'emplacement global, réseau et stockage. Vous

pouvez utiliser ces paramètres de configuration prédéfinis et ajouter des paramètres de configuration personnalisés qui ne sont pas disponibles via XClarity Administrator.

À propos de cette tâche

Les paramètres de configuration personnalisés sont définis sous la forme d'un schéma JSON. Le schéma doit être conforme à la spécification JSON.

Lorsque vous importez des paramètres de configuration personnalisés dans XClarity Administrator, XClarity Administrator valide le schéma JSON. Si la validation réussit, XClarity Administrator génère des macros personnalisées pour chaque paramètre.

Vous pouvez utiliser les macros personnalisées dans le fichier sans opérateur et le script de post-installation.

Dans des fichiers sans opérateur

Vous pouvez associer le fichier de configuration personnalisé à un fichier sans opérateur et inclure ces macros personnalisées (et macros prédéfinies) dans le fichier sans opérateur.

Vous pouvez ajouter un ou plusieurs fichiers de paramètres de configuration personnalisés dans un profil personnalisé. Lorsque vous déployez le profil SE sur un ensemble de serveurs cible, vous pouvez choisir le fichier de paramètres de configuration à utiliser. XClarity Administratoraffiche l'onglet **Paramètres personnalisés** dans la boîte de dialogue Déployer des images de SE en fonction du schéma JSON dans le fichier de paramètres de configuration et vous permet de définir des valeurs pour chaque paramètre (objet JSON) qui est défini dans le fichier.

Remarque : Le déploiement SE ne se poursuivra pas si aucune entrée n'est spécifiée pour les paramètres de configuration personnalisés requis.

Dans les scripts de post-installation

Une fois les données collectées pendant le déploiement SE, XClarity Administrator crée une instance des paramètres du fichier de configuration (qui inclut les paramètres personnalisés dans le fichier sélectionné et un sous-ensemble de paramètres prédéfinis) sur le système hôte qui peut être utilisé par le script de post-installation.

Remarques :

- Le fichier des paramètres de configuration est unique dans un profil d'image SE personnalisé.
- Vous ne pouvez pas modifier les paramètres de configuration des profils d'image SE prédéfinis.
- Les paramètres de configuration sont pris en charge uniquement pour les systèmes d’exploitation suivants :
  - Microsoft® Windows® Server
  - Red Hat® Enterprise Linux (RHEL) Server
  - Rocky Linux
  - SUSE® Linux Enterprise Server (SLES)
  - VMware vSphere® Hypervisor (ESXi) avec Lenovo Customization 6.0u3, mises à jour ultérieures et 6.5 et ultérieures.

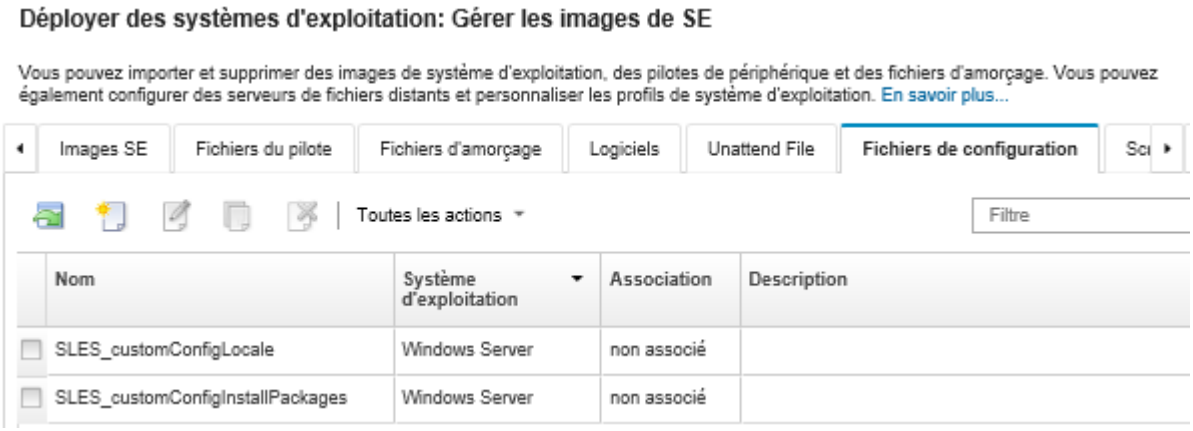
Le référentiel des images SE peut stocker un nombre illimité de fichiers prédéfinis et personnalisés, si l’espace disponible est suffisant pour stocker les fichiers.

Procédure

Pour importer des fichiers de paramètres de configuration dans le référentiel d'images SE, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Gérer les images de SE** pour afficher la page Déployer un système d'exploitation : déployer des images de SE.

Etape 2. Cliquez sur l'onglet **Paramètres de configuration**.



Etape 3. Cliquez sur l'icône **Importer fichier** ( ). La boîte de dialogue Importation des paramètres de configuration s'affiche.

Etape 4. Cliquez sur l'onglet **Importation locale** pour télécharger des fichiers à partir du système local ou cliquez sur l'onglet **Importation à distance** pour télécharger des fichiers à partir d'un serveur de fichiers distant.

Remarque : Pour télécharger un fichier à partir d'un serveur de fichiers distant, vous devez d'abord créer un profil de serveur de fichiers distant en cliquant sur l'icône **Configurer le serveur de fichiers** ( ). Pour plus d'informations, voir Configuration d'un serveur de fichiers distant .

Etape 5. Si vous choisissez d'utiliser un serveur de fichiers distant, sélectionnez-le dans la liste **Serveur de fichiers distant**.

Etape 6. Sélectionnez le type de système d'exploitation.

Etape 7. Entrez le nom de fichier du fichier de paramètres de configuration ou cliquez sur **Parcourir** pour rechercher le fichier que vous souhaitez importer.

Etape 8. **Facultatif :** Entrez une description des paramètres de configuration.

Astuce : Utilisez les zones **Description** pour différencier les fichiers personnalisés portant le même nom.

Etape 9. **Facultatif :** Sélectionnez un type de total de contrôle pour vérifier que le fichier en cours de téléchargement n'est pas endommagé et copiez et collez la valeur de total de contrôle dans la zone de texte fournie.

Si vous sélectionnez un type de total de contrôle, vous devez indiquer une valeur de total de contrôle pour vérifier l'intégrité et la sécurité du fichier téléchargé. La valeur doit venir de la source sécurisée d'une organisation fiable. Si le fichier téléchargé correspond à la valeur de total de contrôle, le déploiement peut être poursuivi en toute sécurité. Sinon, vous devez télécharger à nouveau le fichier ou vérifier la valeur de total de contrôle.

Trois types de total de contrôle sont pris en charge :
- **MD5**
- **SHA1**
- **SHA256**

Etape 10. Cliquez sur **Importer**. Le format JSON est validé lorsque vous importez le fichier. Si des erreurs sont détectées, une boîte de dialogue s'affiche avec le message d'erreur et l'emplacement.

Astuce : Le fichier est téléchargé via une connexion réseau sécurisée. Par conséquent, la fiabilité et les performances du réseau ont une incidence sur le temps nécessaire à l'importation du fichier.

Attention : Si vous fermez l'onglet ou la fenêtre de navigateur Web dans lesquels le fichier est téléchargé en local avant la fin du téléchargement, l'importation échoue.

Après avoir terminé

Les fichiers de paramètres de configuration sont répertoriés sous l'onglet **Paramètres de configuration** de la page Gérer les images de SE.

Depuis cette page, vous pouvez aussi effectuer les actions suivantes.

- Créer un fichier de paramètres de configuration en cliquant sur l'icône **Créer** (), puis en spécifiant le nom de fichier, la description, le type SE, les paramètres de configuration et les valeurs. Cliquez sur **Valider** pour valider le schéma avant d'enregistrer le fichier.

  L'éditeur identifie l'emplacement de toutes les erreurs qui se trouvent dans le fichier. Notez que certains messages sont uniquement en anglais.

- Consulter et modifier un fichier de paramètres de configuration en cliquant sur l'icône **Éditer** ().

  Vous ne pouvez pas modifier un fichier de paramètres de configuration qui est associé à un fichier sans opérateur.

  L'éditeur identifie l'emplacement de toutes les erreurs qui se trouvent dans le fichier. Notez que certains messages sont uniquement en anglais.

- Copier un fichier de paramètres de configuration en cliquant sur l'icône **Copier** ().

  Si vous copiez un fichier de paramètres de configuration qui est associé à un fichier sans opérateur, le fichier sans opérateur associé est également copié et l'association est automatiquement créée entre les deux fichiers copiés.

- Retirer un fichier de paramètres de configuration sélectionné en cliquant sur l'icône **Supprimer** ().

- Créez un profil de serveur de fichiers distant en cliquant sur l'icône **Configurer le serveur de fichiers** ().

Pour plus d'informations sur l'ajout de paramètres de configuration dans un profil d'image SE personnalisé, voir Création d'un profil d'image SE personnalisé.

Macros personnalisées

Les *macros* vous permettent d'ajouter des données variables (paramètres de configuration) à un fichier sans opérateur ou un script de post-installation. Lenovo XClarity Administrator vous permet de définir vos propres paramètres personnalisés en créant un fichier de paramètres de configuration personnalisés, en utilisant le format JSON.

La valeur de chaque paramètre de configuration personnalisée varie en fonction de l'entrée utilisateur spécifiée pendant le déploiement du système d'exploitation.

Lorsque vous importez des paramètres de configuration personnalisés dans XClarity Administrator, XClarity Administrator valide le schéma JSON. Si la validation réussit, XClarity Administrator génère des macros personnalisées pour chaque paramètre.

Pour injecter des macros personnalisés dans un fichier sans opérateur ou un script de post-installation, utilisez le nom unique de l'objet, les objets imbriqués distincts à l'aide d'un point, puis placez le nom de macro entre des dièses (#), par exemple, **#server_settings.server0.locale#**.

Remarques :

- N'incluez pas le nom d'objet supérieur.
- Lorsqu'un objet est créé à partir d'un modèle, le nom est ajouté avec un numéro unique, en commençant par 0 (par exemple, server0 et server1).
- Vous pouvez également voir le nom de chaque macro à partir de la boîte de dialogue Déployer des images SE sous les onglets Paramètres personnalisés en passant le curseur sur l'icône **Aide** () en regard de chaque paramètre personnalisé.

Paramètres de configuration

Vous pouvez définir des paramètres de configuration personnalisés qui:

- Sont communs à tous les serveurs cible ou uniques sur un serveur cible spécifique.
- Comportent des valeur statiques (non configurables) ou avec des valeurs dynamiques (configurables) qui sont entrées lors du déploiement de votre profil d'image SE.
- Comportent un nombre variable d'éléments basé sur un modèle. Par exemple, vous pouvez définir un paramètre de configuration qui vous permet d'indiquer 0 à 3 serveurs NTP pendant le déploiement.

Paramètres globaux

Pendant le Déploiement SE, les éléments d'interface au niveau des onglets **Paramètres globaux** dans la boîte de dialogue Déployer l'image SE sont rendus d'après les objets qui sont représentés dans l'objet **content**. Les objets décrivent les paramètres et les valeurs nécessaires à tous les serveurs cible pour le déploiement SE.

Pour représenter les paramètres communs à tous les serveurs, le fichier JSON doit contenir un objet parent avec un objet imbriqué qui contient la paire nom/valeur `"common":true`.

L'exemple suivant utilise les mêmes serveurs NTP configurables (dynamiques) pour tous les serveurs.

```
{
   "category": "dynamic",
   "content": [{
      "category": "dynamic",
      "common": true,
      "description": "NTP Servers",
      "label": "NTP Servers",
      "maxElements": 3,
      "minElements": 0,
      "name": "common-ntpservers",
      "optional": true,
      "template": [{
         "autoCreateInstance": true,
         "category": "dynamic",
         "common": true,
         "description": "A NTP Server",
         "label": "NTP Server",
         "name": "ntpserver",
         "optional": true,
         "regex": "[\\w\\.]{1,64}$",
         "type": "string"
      }],
      "type": "array"
   },
   ...,
}
```

L'exemple suivant utilise le même répertoire de journal de script de post-installation (statique) non configurable.

```
{
   "category": "dynamic",
   "content": [{
      "category": "static",
      "common": true,
      "description": "Directory location for post-installation script logging.",
      "name": "logpath",
      "optional": false,
      "type": "string",
      "value": "/tmp/mylogger.log"
   },
   ...,
}
```

Paramètres spécifiques au serveur

Pendant le déploiement SE, les éléments d'interface au niveau de l'onglet **Paramètres spécifiques au serveur** dans la boîte de dialogue Déployer l'image SE sont rendus d'après les objets qui sont représentés dans les objets **content** du modèle. Les objets décrivent les paramètres et les valeurs nécessaires à un serveur cible spécifique pour le déploiement SE.

Une fois les valeurs spécifiques au serveur collectées dans l'interface utilisateur, un objet **content** est créée dans JSON pour chaque serveur cible d'après l'objet **template**. Chaque objet **content** contient une zone **name** et **targetServer** uniques, et les valeurs qui ont été entrées pour ce serveur.

Pour représenter les paramètres spécifiques au serveur, le fichier JSON doit contenir un objet parent avec le contenu suivant:

- La paire nom/valeur `"category":"dynamic"`.
- Un objet imbriqué qui contient la paire nom/valeur `"common":false`. Un seul objet `"common": false` est pris en charge dans le contenu de l'objet parent.
- Un objet modèle avec un objet content imbriqué. Ce tableau modèle peut contenir un seul objet.

Par exemple, si vous souhaitez définir des paramètres régionaux SE uniques pour chaque serveur cible

```
{
   "category": "dynamic",
   "content": [{
      "category": "dynamic",
      "common": false,
      "name": "server-settings",
      "optional": false,
      "template": [{
         "category": "dynamic",
         "common": false,
         "content": [{
            "category": "dynamic",
            "choices": ["en_US", "pt_BR", "ja_JP"],
            "common": false,
            "label": "OS Locale",
            "name": "locale",
            "optional": false,
            "type": "string",
            "value": "en_US"
         }],
         "name": "server",
         "optional": false,
         "type": "assoc_array"
      }],
```

```
        "type": "assoc_array"
    },
    ...,
}
```

spécification JSON

Le tableau suivant décrit les zones qui sont autorisées dans la spécification JSON.

Paramètre	Obligatoire / Facultative	Type	Description
autoCreateInstance	en option	booléenne	Indique si une instance de l'objet modèle est créée automatiquement dans un fichier JSON lors du déploiement. Les valeurs possibles sont les suivantes. • **true**. Une instance de l'objet modèle est créée automatiquement dans un fichier JSON lors du déploiement. • **false**. (par défaut) Une instance de l'objet modèle n'est *pas* créée automatiquement dans un fichier JSON lors du déploiement. **Remarque :** Cette zone peut être placée uniquement dans l'objet modèle.
catégorie	Requis	String	Indique la façon dont la valeur de chaque paramètre est indiquée. Les valeurs possibles sont les suivantes: • **dynamique**. La valeur est entrée par l'utilisateur lors de l'exécution. Lenovo XClarity Administrator vous invite à saisir cette valeur pendant le déploiement SE. • **prédéfini**. La valeur est prédéfinie par Lenovo XClarity Administrator. • **statique**. La valeur est indiquée dans le schéma et ne change pas lors de l'exécution. Les objets imbriqués héritent de la valeur de cette zone à partir de son objet parent. Si la **catégorie** est définie sur `static` dans l'objet parent, elle doit être définie sur `static` dans tous les objets imbriqués également. Si la **catégorie** est défini sur `dynamic` dans l'objet parent, elle peut être définie sur `static` ou `dynamic` dans les objets imbriqués.
choix	en option	Tableau de valeurs correspondant à la propriété **type**	Tableau de valeurs statiques (chaînes ou entiers, par exemple) pour le paramètre de configuration que l'utilisateur peut choisir pendant le déploiement SE (par exemple, `["enabled","disabled"]`).

Paramètre	Obligatoire / Facultative	Type	Description
commun	en option	booléenne	Indique si ce schéma de configuration s'applique à tous les serveurs cible. • **true**. L'objet s'applique à tous les serveurs cible. • **false**. (default) L'objet s'applique à un serveur cible spécifique. Les objets imbriqués héritent de la valeur de cette zone à partir de son objet parent. Si le paramètre **common** est défini sur `true` dans l'objet parent, il doit être défini sur `true` dans tous les objets imbriqués également. Si le paramètre **common** est défini sur `false` dans l'objet parent, il doit être défini sur `false` dans tous les objets imbriqués.
content	en option	Tableau d'objets	Modèle qui représente les objets imbriqués dans le schéma. Une fois les données entrées par l'utilisateur collectées lors du déploiement SE, cette zone est utilisée pour représenter les valeurs finales d'un modèle donné dans l'instance du fichier de paramètres de configuration qui est créé pour le déploiement.
par défaut	en option	Varie en fonction du **type**	Valeur par défaut.
description	en option	String	Description de l'objet
étiquette	en option	String	Étiquette pour le paramètre dans l'interface utilisateur qui s'affiche lors du déploiement SE
max	en option	Entier	Valeur maximum, lorsque **type** est défini sur integer. La valeur par défaut est unlimited.
maxElements	en option	Entier	Nombre maximum d'entrées du tableau pour cet objet.
min	en option	Entier	Valeur minimum, lorsque **type** est défini sur integer. La valeur par défaut est 0.
minElements	en option	Entier	Nombre minimum d'entrées du tableau pour cet objet.
name	Requis	String	Nom unique de l'objet. Ce nom peut contenir uniquement les caractères suivants: caractères alphanumériques (a-z, A-Z et 0-9), traits de soulignement (_) et tirets (-). Vous pouvez faire référence à **name** en tant que macro personnalisée dans le fichier sans opérateur. Lors de la référence à un objet **name** imbriqué, séparez chaque objet à l'aide d'un point (par exemple, `mydeploy.node.locale`).
optional	Requis	booléenne	Indique si l'objet est facultatif. Les valeurs possibles sont les suivantes. • **true**. La zone est facultative. • **false**. La zone est obligatoire.
regex	en option	String	Expression régulière pour la validation de la valeur (par exemple, `"[\\w\\.]{1,64}$"`)

Paramètre	Obligatoire / Facultative	Type	Description
script	en option	Tableau de chaînes	Liste de scripts, séparés par une virgule, qui ont des dépendances sur les données dans ce objet (par exemple, ["/opt/lenovo/saphana/bin/saphana-create-saphana.sh", "create_hana.sh"]). **Remarque :** Les scripts doivent être disponibles pour le profil d'image SE en tant que script d'installation ou logiciel personnalisé.
targetServer	en option	String	UUID du serveur qui est la cible du déploiement SE. Si common est défini sur true, cette zone peut être vide ou nulle, et le serveur cible est spécifié pendant le déploiement SE.

Paramètre	Obligatoire / Facultative	Type	Description

template	en option	Tableau d'objets	Modèle qui représente les objets réutilisables. Pendant le déploiement SE, ce modèle peut représenter plusieurs instances de l'objet. Les zones **minElements** et **maxElements** peuvent être utilisées pour limiter le nombre d'instances.
			
			L'exemple suivant utilise un modèle pour représenter un groupe de serveurs NTP 1-3.
			`{`
			`"category": "dynamic",`
			`"common": true,`
			`"description": "NTP Servers",`
			`"label": "NTP Servers",`
			`"maxElements": 3,`
			`"minElements": 0,`
			`"name": "common-ntpservers",`
			`"optional": true,`
			`"template": [{`
			`"autoCreateInstance": true,`
			`"category": "dynamic",`
			`"common": true,`
			`"description": "A NTP Server",`
			`"label": "NTP Server",`
			`"name": "ntpserver",`
			`"optional": true,`
			`"regex": "[\\w\\.]{1,64}$",`
			`"type": "string"`
			`}],`
			`"type": "array"`
			`},`
			
			Une fois les données entrées par l'utilisateur collectées lors du déploiement SE, une instance du fichier de paramètres de configuration est créée avec du contenu spécifique pour chaque appareil sur lequel le SE doit être déployé.
			`{`
			`"category": "dynamic",`
			`"common": true,`
			`"description": "NTP Servers",`
			`"label": "NTP Servers",`
			`"maxElements": 3,`
			`"minElements": 0,`
			`"name": "common-ntpservers",`
			`"optional": true,`
			`"content": [{`
			`"category": "dynamic",`
			`"common": true,`
			`"description": "A NTP Server",`
			`"label": "NTP Server",`
			`"name": "ntpserver0",`
			`"optional": true,`
			`"regex": "[\\w\\.]{1,64}$",`
			`"type": "string",`
			`"value": "192.0.2.1"`
			`}],`

Paramètre	Obligatoire / Facultative	Type	Description

			<pre>"template": [{
			"category": "dynamic",
			"common": true,
			"description": "A NTP Server",
			"label": "NTP Server",
			"name": "ntpserver",
			"optional": true,
			"regex": "[\\w\\.]{1,64}$",
			"type": "string"
			}],
			"type": "array"
			}</pre> **Remarques :**
			• Un modèle est *requis* au niveau supérieur des objets serveur (common=false).
			• Si **category** est défini sur `static`, la zone de modèle est ignorée.

type	Requis	String	Type de données de l'objet. Les valeurs possibles sont les suivantes. • **array** • **assoc_array** • **boolean** • **integer** • **password** • **string** • **user_data**
value	en option	String	Valeur statique unique pour le paramètre de configuration. **Remarques :** • Si **default** est défini, cette zone peut être vide ou nulle. Sinon, indiquez une valeur qui correspond à **type**. • Si **type** est défini sur `password`, spécifiez une chaîne non chiffrée. • Si **type** est défini sur `assoc_array` ou `array`, vous devez également spécifier une zone **content** vide. • Si **type** est défini sur `user_data`, indiquez une valeur **value** au format JSON valide. • Si **regex** est défini, cette valeur validée à l'aide de l'expression régulière spécifiée.

Les exemples de paramètres de configuration suivants définissent les paramètres régionaux pour les déploiements SLES qui peuvent être ajoutés à un profil personnalisé.

```
{
    "category": "dynamic",
    "content": [{
        "category": "dynamic",
        "common": false,
        "name": "server-settings",
        "optional": false,
        "template": [{
```

```
        "autoCreateInstance": true,
        "category": "dynamic",
        "common": false,
        "content": [{
            "category": "dynamic",
            "choices": ["en_US", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the OS language locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "OS Locale",
            "name": "locale",
            "optional": false,
            "type": "string",
            "value": "en_US"
        },
        {
            "category": "dynamic",
            "choices": ["english-us", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the keyboard locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "Keyboard Locale",
            "name": "keyboardLocale",
            "optional": false,
            "type": "string",
            "value": "english-us"
        }],
        "name": "server",
        "optional": false,
        "type": "assoc_array"
    }],
    "type": "assoc_array"
},
{
    "category": "dynamic",
    "common": true,
    "description": "NTP Servers",
    "label": "NTP Servers",
    "maxElements": 3,
    "minElements": 0,
    "name": "common-ntpservers",
    "optional": true,
    "template": [{
        "category": "dynamic",
        "common": true,
        "description": "A NTP Server",
        "label": "NTP Server",
        "name": "ntpserver",
        "optional": true,
        "regex": "[\\w\\.]{1,64}$",
        "type": "string"
    }],
    "type": "array"
},
{
    "category": "static",
    "common": true,
    "description": "Directory for post-installation script logging.",
    "name": "logpath",
    "optional": false,
    "type": "string",
```

```
        "value": "/tmp/mylogger.log"
    }],
    "description": "Custom configuration file for deployment of custom locale, NTP server,
                    and directory for post-installation script logs.",
    "label": "My Custom Deployment",
    "name": "myCustomDeploy",
    "optional": false,
    "type": "array"
}
```

L'exemple suivant est l'instance du fichier de paramètres de configuration qui est créée sur le système hôte, une fois les valeurs entrée par l'utilisateur définies lors du déploiement.

```
{
    "category": "dynamic",
    "content": [{
        "category": "dynamic",
        "common": false,
        "name": "server-settings",
        "optional": false,
        "content": [{
            "category": "dynamic",
            "common": false,
            "content": [{
                "category": "dynamic",
                "choices": ["en_US", "pt_BR", "ja_JP"],
                "common": false,
                "description": "This parameter defines the OS language locale to use with this deployment.
                                English, Brazilian Portuguese, and Japanese are supported.",
                "label": "OS Locale",
                "name": "locale",
                "optional": false,
                "type": "string",
                "value": "en_US"
            },
            {
                "category": "dynamic",
                "choices": ["english-us", "pt_BR", "ja_JP"],
                "common": false,
                "description": "This parameter defines the keyboard locale to use with this deployment.
                                English, Brazilian Portuguese, and Japanese are supported.",
                "label": "Keyboard Locale",
                "name": "keyboardLocale",
                "optional": false,
                "type": "string",
                "value": "english-us"
            }],
            "name": "server0",
            "optional": false,
            "type": "assoc_array",
            "targetServer": "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
        },
        {
            "category": "dynamic",
            "common": false,
            "content": [{
                "category": "dynamic",
                "choices": ["en_US", "pt_BR", "ja_JP"],
                "common": false,
                "description": "This parameter defines the OS language locale to use with this deployment.
                                English, Brazilian Portuguese, and Japanese are supported.",
                "label": "OS Locale",
```

```
            "name": "locale",
            "optional": false,
            "type": "string",
            "value": "en_US"
        },
        {
            "category": "dynamic",
            "choices": ["english-us", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the keyboard locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "Keyboard Locale",
            "name": "keyboardLocale",
            "optional": false,
            "type": "string",
            "value": "english-us"
        }],
        "name": "server1",
        "optional": false,
        "type": "assoc_array",
        "targetServer": "BBBBBBBBBBBBBBBBBBBBBBBBBBBBBB"
    }],
    "template": [{
        "category": "dynamic",
        "common": false,
        "content": [{
            "category": "dynamic",
            "choices": ["en_US", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the OS language locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "OS Locale",
            "name": "locale",
            "optional": false,
            "type": "string",
            "value": "en_US"
        },
        {
            "category": "dynamic",
            "choices": ["english-us", "pt_BR", "ja_JP"],
            "common": false,
            "description": "This parameter defines the keyboard locale to use with this deployment.
                            English, Brazilian Portuguese, and Japanese are supported.",
            "label": "Keyboard Locale",
            "name": "keyboardLocale",
            "optional": false,
            "type": "string",
            "value": "english-us"
        }],
        "name": "server",
        "optional": false,
        "type": "assoc_array"
    }],
    "type": "assoc_array"
},
{
    "category": "dynamic",
    "common": true,
    "description": "NTP Servers",
    "label": "NTP Servers",
    "maxElements": 3,
```

```
        "minElements": 0,
        "name": "common-ntpservers",
        "optional": true,
        "content": [{
            "category": "dynamic",
            "common": true,
            "description": "A NTP Server",
            "label": "NTP Server",
            "name": "ntpserver0,
            "optional": true,
            "regex": "[\\w\\.]{1,64}$",
            "type": "string",
            "value": "192.0.2.1"
        },
        {
            "category": "dynamic",
            "common": true,
            "description": "A NTP Server",
            "label": "NTP Server",
            "name": "ntpserver1",
            "optional": true,
            "regex": "[\\w\\.]{1,64}$",
            "type": "string",
            "value": "192.0.2.2"
        }],
        "template": [{
            "category": "dynamic",
            "common": true,
            "description": "A NTP Server",
            "label": "NTP Server",
            "name": "ntpserver",
            "optional": true,
            "regex": "[\\w\\.]{1,64}$",
            "type": "string"
        }],
        "type": "array"
    },
    {
        "category": "static",
        "common": true,
        "description": "Directory for post-installation script logs.",
        "name": "logpath",
        "optional": false,
        "type": "string",
        "value": "/tmp/mylogger.log"
    }],
    "description": "Custom configuration file for deployment of custom locale, NTP server,
                    and directory for post-installation script logs.",
    "label": "My Custom Deployment",
    "name": "myCustomDeploy",
    "optional": false,
    "type": "array"
}
```

Macros prédéfinies

Les *macros* vous permettent d'ajouter des données variables (paramètres de configuration) à un fichier sans opérateur ou un script de post-installation. Lenovo XClarity Administrator fournit un ensemble de paramètres de configuration prédéfinis que vous pouvez utiliser.

Pour injecter des macros prédéfinies dans un fichier sans opérateur ou de script de post-installation, préfixez la macro avec « predefined » pour les macros prédéfinies, séparez les objets imbriqués à l'aide d'une point, puis placez le nom de macro entre dièses (#), par exemple **# predefined.globalSettings.ipAssignment#**.

La valeur de chaque macro prédéfinie varie en fonction de l'instance XClarity Administrator. Par exemple, la zone **Déployer des images de SE → Paramètres globaux → Affectation d'IP** vous permet d'indiquer le mode IP. Une fois la valeur entrée par l'utilisateur collectée pendant le déploiement SE, la valeur est représentée dans les paramètres de configurations prédéfinis par la macro prédéfinie **#predefined.globalSettings.ipAssignment#** et dans l'instance du fichier JSON de paramètres de configuration sous le nom d'objet ipAssignment.

Le tableau suivant répertorie les macros prédéfinies (paramètres de configuration) qui sont disponibles dans XClarity Administrator.

Nom de macro	Type	Description
prédéfinies	Objet	Informations sur les tous les paramètres de déploiement SE prédéfinis
globalSettings	Objet	Informations sur les paramètres de déploiement SE globaux
credentials	Tableau d'objets	Informations sur les données d'identification utilisateur
name	String	
type	String	Type de système d'exploitation. Les valeurs possibles sont les suivantes. • **ESXi** • **LINUX** • **WINDOWS**
ipAssignment	String	Option de paramètre réseau hôte pour le déploiement du système d'exploitation. Les valeurs possibles sont les suivantes. • **dhcpv4** • **staticv4** • **staticv6**
isVLANMode	String	Indique si le mode VLAN est utilisé. Les valeurs possibles sont les suivantes. • **true**. Le mode VLAN est utilisé. • **false**. Le mode VLAN n'est pas utilisé.
hostPlatforms	Objet	Paramètres de déploiement des plateformes hôte
licenseKey	String	Clé de licence à utiliser pour Microsoft Windows ou VMware ESXi. Si vous n'avez pas de clé de licence, vous pouvez définir cette zone sur null.
networkSettings	Grappe	Informations sur les paramètres réseau
dns1	String	Serveur DNS préféré pour le serveur hôte à utiliser après le déploiement du système d'exploitation
dns2	String	Serveur DNS secondaire pour le serveur hôte à utiliser après le déploiement du système d'exploitation
passerelle	String	Passerelle du serveur hôte à utiliser après le déploiement du système d'exploitation Utilisé lorsque le paramètre de réseau est défini sur static dans les paramètres de déploiement du système d'exploitation globaux. **Astuce :** pour déterminer le mode IP, utilisez GET /osdeployment/globalSettings.

Nom de macro	Type	Description
Nom d'hôte	String	Nom d'hôte du serveur hôte. Si aucun un nom d'hôte n'est spécifié, un nom d'hôte par défaut est affecté.
ipAddress	String	Adresse IP du serveur hôte à utiliser après le déploiement du système d'exploitation. Utilisé lorsque le paramètre de réseau est défini sur static dans les paramètres de déploiement du système d'exploitation globaux.
mtu	Long	Vitesse d'unité MTU (unité de transmission maximale) pour l'hôte à utiliser après le déploiement du système d'exploitation.
prefixLength	String	Longueur de préfixe de l'adresse IP hôte à utiliser après le déploiement du système d'exploitation. Utilisé lorsque le paramètre de réseau est défini sur static IPv6 dans les paramètres de déploiement du système d'exploitation globaux.
selectedMAC	String	Adresse MAC du serveur hôte à laquelle l'adresse IP doit être liée. L'adresse MAC est définie à AUTO par défaut. Ce paramètre détecte automatiquement les ports Ethernet qui peuvent être configurés et utilisés pour le déploiement. La première adresse MAC (port) qui est détectée est utilisée par défaut. Si la connectivité est détectée sur un adresse MAC différente, l'hôte XClarity Administrator est automatiquement redémarré pour utiliser l'adresse MAC nouvellement détectée pour le déploiement, et selectedMAC sont définis sur l'adresse MAC nouvellement détectée. Le mode VLAN est pris en charge uniquement pour les serveurs qui ont des adresses MAC dans leur inventaire. Si AUTO est la seule adresse MAC disponible pour un serveur, les VLAN ne peuvent pas être utilisés pour déployer des systèmes d'exploitation sur ce serveur. **Astuce :** pour obtenir l'adresse MAC, utilisez la propriété de réponse **macaddress** dans GET /hostPlatforms.
subnetCIDRNumber	Entier	Masque de sous-réseau du serveur hôte à utiliser après le déploiement du système d'exploitation, au format CIDR (Classless Inter-Domain Routing). Utilisé lorsque le paramètre de réseau est défini sur static dans les paramètres de déploiement du système d'exploitation globaux. Le numéro CIDR est généralement précédé d'une barre oblique « / » et suit l'adresse IP. Par exemple, une adresse IP de 131.10.55.70 avec un masque de sous-réseau de 255.0.0.0 (qui comporte 8 bits de réseau) serait représentée sous la forme 131.10.55.70/8. Pour plus d'informations, voir le document Page Web de tutoriel de notation CIDR. **Astuce :** pour déterminer le mode IP, utilisez GET /osdeployment/globalSettings.
subnetMask	String	Masque de sous-réseau du serveur hôte à utiliser après le déploiement du système d'exploitation, en format d'adresse décimale à point (par exemple, 255.0.0.0). Utilisé lorsque le paramètre de réseau est défini sur static dans les paramètres de déploiement du système d'exploitation globaux. **Astuce :** pour déterminer le mode IP, utilisez GET /osdeployment/globalSettings.

Nom de macro	Type	Description
vlanId	String	ID VLAN pour le marquage VLAN du système d'exploitation. Ce paramètre est valide uniquement si le mode VLAN est activé. Pour déterminer si le mode VLAN est activé, utilisez GET /osdeployment/globalSettings dans la documentation en ligne de XClarity Administrator). **Important :** Indiquez un ID VLAN uniquement lorsqu'un marquage VLAN est requis pour fonctionner sur le réseau. L'utilisation de balises VLAN peut affecter la routabilité de réseau entre le système d'exploitation hôte et XClarity Administrator.
selectedImage	String	ID de profil de l'image du système d'exploitation à déployer. **Astuce :** pour obtenir les ID de profil de l'image du système d'exploitation, utilisez la propriété de réponse **availableImages** dans GET /hostPlatforms.
storageSettings	Grappe	Emplacement de stockage préféré où vous souhaitez déployer les images de système d'exploitation
targetDevice	String	Appareil cible. Les valeurs possibles sont les suivantes. • **localdisk**. Unité de disque locale. La première unité de disque locale énumérée dans le serveur géré est utilisée. • **M.2drive**. Unité M.2. La première unité M.2 énumérée dans le serveur géré est utilisée. • **usbdisk**. Hyperviseur USB imbriqué. Cet emplacement s'applique uniquement lorsqu'une image VMware ESXi est déployée sur les serveurs gérés. Si deux clés d'hyperviseur sont installées sur le serveur géré, le programme d'installation de VMware sélectionne la première clé répertoriée pour le déploiement. • **lunpluswwn=***LUN@WWN*. Stockage SAN FC (par exemple, `lunpluswwn=2@50:05:07:68:05:0c:09:bb`). • **lunplusiqn=***LUN@IQN*. Stockage SAN iSCI (par exemple, `lunplusiqn=0@iqn.1990-01.com.lenovo:tgt1`). La spécification de *IQN* est facultative si une seule cible iSCSI est configurée. Si *IQN* n'est pas spécifié, la première cible iSCSI détectée est sélectionnée pour OSDN. Si cette option est spécifiée, une concordance exacte est effectuée. **Remarque :** Pour les serveurs ThinkServer, cette valeur est toujours « localdisk. »
unattendFileId	String	ID du fichier sans opérateur à utiliser avec ce déploiement
UUID	String	Adresse UUID du serveur hôte sur lequel le système d'exploitation doit être déployé
imageSettings	Objet	Informations sur chaque image et profil d'image SE
name	String	Nom de l'image du système d'exploitation
profil	String	nom du profil d'image
otherSettings	Objet	Paramètres supplémentaires qui sont associés aux travaux de déploiement SE actuellement en cours d'exécution
deployDataAndSoftwareLocation	String	Chemin d'accès au contenu logiciel extrait, aux fichiers personnalisés et aux données de déploiement (tels que les certificats et les journaux)

Nom de macro	Type	Description

installRepoUrl	String	(SLES 15 et versions ultérieures uniquement) URL de l'image de module importé
		Vous pouvez utiliser cette macro prédéfinie dans le fichier sans opérateur personnalisé pour media_url dans la section add-on, par exemple : example:
		`<add-on>`
		`<add_on_products config:type="list">`
		`<listentry>`
		`<media_url>`**#predefined.otherSettings.installRepoUrl#**
		`</media_url>`
		`<product>sle-module-basesystem</product>`
		`<product_dir>/Module-Basesystem</product_dir>`
		`</listentry>`
		`</add_on_products>`
		`</add-on>`

lxcaIp	String	Adresse IP de l'instance XClarity Administrator
lxcaRelease	String	Version de XClarity Administrator (par exemple, 2.0.0)
jobId	String	ID du travail de déploiement SE en cours d'exécution
ntpServer	String	Serveur NTP qui est associé à XClarity Administrator
statusSettings	Objet	Paramètres de l'état de déploiement SE
urlStatus	String	URL HTTPS (y compris le port) utilisée par XClarity Administrator pour la génération de rapports d'état
certLocation	String	Dossier contenant les certificats qui sont nécessaires pour accéder au service Web **urlStatus** depuis le système d'exploitation hôte au premier amorçage
sdkLocation	String	Emplacement des scripts d'assistance et interfaces fournis par XClarity Administrator pour accéder à XClarity Administrator
timezone	String	Fuseau horaire qui est défini pour XClarity Administrator (par exemple, Amérique/New_York)
unattendSettings	Objet	Paramètres qui sont utilisés pour remplir le fichier sans opérateur. Ces valeurs sont spécifiques à la version de XClarity Administrator
networkConfig	String	(ESXi et RHEL uniquement) Contenu XClarity Administrator prédéfini à utiliser lors de l'installation sans opérateur. Cela permet de configurer les paramètres réseau pour le système d'exploitation
preinstallConfig	String	Contenu XClarity Administrator prédéfini à utiliser lors de la préinstallation sans opérateur. Cela inclut l'état de la préinstallation. • Pour ESXi et RHEL, utilise le point d'ancrage des scripts de préinstallation %pre. • Pour SLES, utilise le point d'ancrage des scripts de préinstallation <scripts>. **Attention :** Il est fortement recommandé d'inclure cette macro dans le fichier sans opérateur personnalisé. Vous pouvez placer la macro dans le fichier sans opérateur à n'importe quel endroit après la ligne 1 (après la balise <xml>).

Nom de macro	Type	Description
postinstallConfig	String	Contenu XClarity Administrator prédéfini à utiliser après la configuration du système et le premier amorçage du système d'exploitation. Cela inclut l'état de post-installation. • Pour ESXi et RHEL, utilise le point d'ancrage des scripts de post-installation %post • Pour SLES, utilise le point d'ancrage des scripts de post-installation <scripts>. • Pour Windows, utilise la section « paramètres spécialisés ». **Attention :** Il est fortement recommandé d'inclure cette macro dans le fichier sans opérateur personnalisé. Vous pouvez placer la macro dans le fichier sans opérateur à n'importe quel endroit après la ligne 1 (après la balise <xml>).
reportWorkloadNotComplete	String	Lorsque cette macro est présente, la macro postinstallConfig ne signale pas l'état OS Installation Completed (17). Le profil personnalisé doit indiquer un rapport terminé.
storageConfig	String	(ESXi et RHEL uniquement) Contenu XClarity Administrator prédéfini à utiliser lors de l'installation sans opérateur. Cela permet de configurer les paramètres de stockage pour le système d'exploitation.

Importation de fichiers sans opérateur personnalisés

Vous pouvez importer des fichiers sans opérateur personnalisés dans le référentiel d'images SE. Ces fichiers peuvent ensuite être utilisés pour personnaliser des profils d'images SE Linux et Windows.

À propos de cette tâche

Les types de fichier suivants sont pris en charge pour les fichiers sans opérateur personnalisés.

Système d'exploitation	Types de fichier pris en charge	Informations complémentaires
Linux CentOS	Non pris en charge	
Microsoft® Windows® Azure Stack HCI	Non pris en charge	
Microsoft Windows Hyper-V Server	Non pris en charge	
Microsoft Windows Server	Sans opérateur (.xml)	Pour plus d'informations sur les fichiers sans opérateur, voir Page Web de référence à l'installation Windows sans opérateur.

Système d'exploitation	Types de fichier pris en charge	Informations complémentaires
Red Hat® Enterprise Linux (RHEL) Server	Kickstart (.cfg)	Pour plus d'informations sur les fichiers sans opérateur, voir Page Web Red Hat : Automatisation de l'installation avec Kickstart . Tenez compte des éléments suivants lors de l'ajout de sections %pre, %post, %firstboot dans le fichier. • Vous pouvez inclure plusieurs sections %pre, %post, % firstboot dans le fichier sans opérateur ; toutefois, tenez compte de l'ordre des sections. • Lorsque la macro recommandée **#predefined. unattendSettings.preinstallConfig#** est présente dans le fichier sans opérateur, XClarity Administrator ajoute une section %pre avant toutes les autres sections %pre dans le fichier. • Lorsque la macro recommandée **#predefined. unattendSettings.postinstallConfig#** est présente dans le fichier sans opérateur, XClarity Administrator ajoute une les sections %post et %firstboot avant toutes les autres sections %post et %firstboot dans le fichier.
Rocky Linux	Kickstart (.cfg)	Pour plus d'informations sur les fichiers sans opérateur, voir Page Web Red Hat : Automatisation de l'installation avec Kickstart . Tenez compte des éléments suivants lors de l'ajout de sections %pre, %post, %firstboot dans le fichier. • Vous pouvez inclure plusieurs sections %pre, %post, % firstboot dans le fichier sans opérateur ; toutefois, tenez compte de l'ordre des sections. • Lorsque la macro recommandée **#predefined. unattendSettings.preinstallConfig#** est présente dans le fichier sans opérateur, XClarity Administrator ajoute une section %pre avant toutes les autres sections %pre dans le fichier. • Lorsque la macro recommandée **#predefined. unattendSettings.postinstallConfig#** est présente dans le fichier sans opérateur, XClarity Administrator ajoute une les sections %post et %firstboot avant toutes les autres sections %post et %firstboot dans le fichier.
SUSE® Linux Enterprise Server (SLES)	AutoYast (.xml)	Pour plus d'informations sur les fichiers sans opérateur, voir SUSE : page Web AutoYaST.

Système d'exploitation	Types de fichier pris en charge	Informations complémentaires
Ubuntu	Non pris en charge	
VMware vSphere® Hypervisor (ESXi) avec personnalisation Lenovo	Kickstart (.cfg)	Pris en charge uniquement pour ESXi 6.0u3 et les mises à jour ultérieures et la version 6.5 et versions ultérieures. Pour plus d'informations sur les fichiers sans opérateur, voir VMware : Installation ou mise à niveau des hôtes à l'aide d'une page Web Script. Tenez compte des éléments suivants lors de l'ajout de sections %pre, %post, %firstboot dans le fichier. • Vous pouvez inclure plusieurs sections %pre, %post, % firstboot dans le fichier sans opérateur ; toutefois, tenez compte de l'ordre des sections. • Lorsque la macro recommandée **#predefined. unattendSettings.preinstallConfig#** est présente dans le fichier sans opérateur, XClarity Administrator ajoute une section %pre avant toutes les autres sections %pre dans le fichier. • Lorsque la macro recommandée **#predefined. unattendSettings.postinstallConfig#** est présente dans le fichier sans opérateur, XClarity Administrator ajoute une les sections %post et %firstboot avant toutes les autres sections %post et %firstboot dans le fichier.

Attention :

- Vous pouvez injecter des macros prédéfinies et personnalisées (paramètres de configuration) dans le fichier sans opérateur à l'aide du nom unique de l'objet. Les valeurs prédéfinies sont basées de manière dynamique basé sur les instances de XClarity Administrator. Les macros personnalisées sont basées de manière dynamique sur la saisie de l'utilisateur qui est spécifiée pendant le déploiement du système d'exploitation.

  Remarques :

  – Placez le nom de macro entre des symboles dièse (#).
  – Pour les objets imbriqués, séparez chaque nom objet à l'aide d'un point (par exemple, **#server_ settings.server0.locale#**).
  – Pour les macros personnalisées, n'incluez pas le nom d'objet le plus important. Pour les macros prédéfinies, ajoutez au nom de la macro le préfixe « prédéfini ».
  – Lorsqu'un objet est créé à partir d'un modèle, le nom est ajouté avec un numéro unique, en commençant par 0 (par exemple, **server0** et **server1**).
  – Vous pouvez également voir le nom de chaque macro à partir de la boîte de dialogue Déployer des images SE sous les onglets Paramètres personnalisés en passant le curseur sur l'icône Aide ( ) en regard de chaque paramètre personnalisé.
  – Pour obtenir la liste des macros prédéfinies, voir Macros prédéfinies. Pour plus d'informations sur les paramètres de configuration et macros personnalisés, voir Macros personnalisées.
- XClarity Administratorfournit les macros prédéfinies suivantes qui sont utilisées pour communiquer l'état depuis le programme d'installation SE, ainsi que plusieurs autres étapes d'installation critique. Il est fortement recommandé d'inclure ces macros dans un fichier sans opérateur (voir Injection de macros prédéfinies et de macros personnalisées dans un fichier sans opérateur).
  – #predefined.unattendSettings.preinstallConfig#
  – #predefined.unattendSettings postinstallConfig#

Le référentiel des images SE peut stocker un nombre illimité de fichiers prédéfinis et personnalisés, si l'espace disponible est suffisant pour stocker les fichiers.

Procédure

Pour importer des fichiers sans opérateur dans le référentiel d'images SE, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Gérer les images de SE** pour afficher la page Déployer un système d'exploitation : déployer des images de SE.

Etape 2. Cliquez sur l'onglet **Fichiers sans opérateur**.

Etape 3. Cliquez sur l'icône **Importer fichier** ( ). La boîte de dialogue Importer un fichier s'affiche.

Etape 4. Cliquez sur l'onglet **Importation locale** pour télécharger des fichiers à partir du système local ou cliquez sur l'onglet **Importation à distance** pour télécharger des fichiers à partir d'un serveur de fichiers distant.

Remarque : Pour télécharger un fichier à partir d'un serveur de fichiers distant, vous devez d'abord créer un profil de serveur de fichiers distant en cliquant sur l'icône **Configurer le serveur de fichiers** ( ). Pour plus d'informations, voir Configuration d'un serveur de fichiers distant

Etape 5. Si vous choisissez d'utiliser un serveur de fichiers distant, sélectionnez-le dans la liste **Serveur de fichiers distant**.

Etape 6. Sélectionnez le type de système d'exploitation.

Etape 7. Entrez le nom de fichier du fichier sans opérateur, ou cliquez sur **Parcourir** pour rechercher le fichier que vous souhaitez importer.

Etape 8. **Facultatif :** Entrez une description pour le fichier sans opérateur.

Astuce : Utilisez les zones **Description** pour différencier les fichiers personnalisés portant le même nom.

Etape 9. **Facultatif :** Sélectionnez un type de total de contrôle pour vérifier que le fichier en cours de téléchargement n'est pas endommagé et copiez et collez la valeur de total de contrôle dans la zone de texte fournie.

Si vous sélectionnez un type de total de contrôle, vous devez indiquer une valeur de total de contrôle pour vérifier l'intégrité et la sécurité du fichier téléchargé. La valeur doit venir de la source sécurisée d'une organisation fiable. Si le fichier téléchargé correspond à la valeur de total de contrôle, le déploiement peut être poursuivi en toute sécurité. Sinon, vous devez télécharger à nouveau le fichier ou vérifier la valeur de total de contrôle.

Trois types de total de contrôle sont pris en charge :

- **MD5**
- **SHA1**
- **SHA256**

Etape 10. Cliquez sur **Importer**.

Astuce : Le fichier est téléchargé via une connexion réseau sécurisée. Par conséquent, la fiabilité et les performances du réseau ont une incidence sur le temps nécessaire à l'importation du fichier.

Si vous fermez l'onglet ou la fenêtre de navigateur Web dans lesquels le fichier est téléchargé en local avant la fin du téléchargement, l'importation échoue.

Après avoir terminé

L'image de fichier sans opérateur est répertoriée sous l'onglet **Fichiers sans opérateur** de la page Gérer les images de SE.

Depuis cette page, vous pouvez effectuer les actions suivantes.

- Créez un fichier sans opérateur en cliquant sur l'icône **Créer** ( ).

  L'éditeur identifie l'emplacement de toutes les erreurs qui se trouvent dans le fichier. Notez que certains messages sont uniquement en anglais.
- Associez un fichier sans opérateur à un fichier de paramètres de configuration (voir Association d'un fichier sans opérateur à un fichier de paramètres de configuration).
- Consultez et modifiez un fichier sans opérateur en cliquant sur l'icône **Éditer** ( ).

  L'éditeur identifie l'emplacement de toutes les erreurs qui se trouvent dans le fichier. Notez que certains messages sont uniquement en anglais.
- Copiez un fichier sans opérateur en cliquant sur l'icône **Copier** ( ).

  Si vous copiez un fichier sans opérateur qui est associé à un fichier de paramètres de configuration, le fichier de paramètres de configuration associé est également copié et l'association est automatiquement créée entre les deux fichiers copiés.
- Retirez des fichiers sans opérateur sélectionnés en cliquant sur l'icône **Supprimer** ( ).
- Créez un profil de serveur de fichiers distant en cliquant sur l'icône **Configurer le serveur de fichiers** ( ).

Pour plus d'informations sur l'ajout d'un fichier sans opérateur dans un profil d'image SE personnalisé, voir Création d'un profil d'image SE personnalisé.

Injection de macros prédéfinies et de macros personnalisées dans un fichier sans opérateur

Vous pouvez injecter des macros prédéfinies et des macros personnalisées dans un fichier sans opérateur.

À propos de cette tâche

Les *Macros* vous permettent d'ajouter des données dynamiques (des paramètres de configuration) à un fichier sans opérateur. Vous indiquez les valeurs des données au moment du déploiement du profil d'image SE.

Lenovo XClarity Administrator fournit un ensemble de macros *prédéfinies* que vous pouvez associer à un fichier sans opérateur sans y associer de fichier de paramètres de configuration. Pour obtenir la liste des macros prédéfinies, voir Macros prédéfinies.

Il est fortement recommandé d'inclure les macros prédéfinies suivantes dans les fichiers sans opérateur personnalisés.

- **#predefined.unattendSettings.preinstallConfig#** et **#predefined.unattendSettings postinstallConfig#**. Utilisées pour communiquer l'état depuis le programme d'installation SE, ainsi que plusieurs autres étapes d'installation critique.

  Consultez les exemples de scénarios de déploiement SE suivants pour plus d'informations sur la manière d'inclure les macros de configuration d'installation.
  - Déploiement de RHEL et d'une application PHP Hello World à l'aide d'un fichier sans opérateur personnalisé
  - Déploiement de SLES 12 SP3 avec des paramètres régionaux configurable et des serveurs NTP
  - Déploiement de VMware ESXi v6.7 avec personnalisation Lenovo sur un disque local à l'aide d'une adresse IP statique
  - Déploiement de Windows 2016 avec des fonctions personnalisées
- **#predefined.unattendSettings.networkConfig#**. (Pour ESXi et RHEL uniquement) Permet à XClarity Administrator de configurer le réseau. Cette macro utilise les paramètres réseau qui sont spécifiés dans la page Déployer des images SE. Si vous n'incluez pas cette macro dans le fichier sans opérateur ou si les paramètres réseau ne sont pas définis dans XClarity Administrator, vous devez configurer l'interface IP dans le cadre du fichier sans opérateur, de sorte que l'hôte dispose d'une route de réseau de retour vers XClarity Administrator.

  Consultez les exemples de scénarios de déploiement SE suivants pour plus d'informations sur la manière d'inclure la macros de configuration réseau.
  - Déploiement de RHEL et d'une application PHP Hello World à l'aide d'un fichier sans opérateur personnalisé
  - Déploiement de VMware ESXi v6.7 avec personnalisation Lenovo sur un disque local à l'aide d'une adresse IP statique
- **#predefined.unattendSettings.storageConfig#**. (Pour ESXi et RHEL uniquement) Permet à XClarity Administrator de configurer le stockage sur l'hôte. Cette macro utilise les paramètres de stockage qui sont spécifiés dans la page Déployer des images SE. Si vous n'incluez pas cette macro dans le fichier sans opérateur ou si les paramètres de stockage ne sont pas définis dans XClarity Administrator, vous devez spécifier la configuration de stockage dans le fichier sans opérateur.

  Consultez les exemples de scénarios de déploiement SE suivants pour plus d'informations sur la manière d'inclure la macros de configuration de stockage.
  - Déploiement de RHEL et d'une application PHP Hello World à l'aide d'un fichier sans opérateur personnalisé
  - Déploiement de VMware ESXi v6.7 avec personnalisation Lenovo sur un disque local à l'aide d'une adresse IP statique

Vous pouvez créer des macros *personnalisés* en créant un fichier de paramètres de configuration personnalisé et en associant le fichier sans opérateur à un fichier de paramètres de configuration personnalisé. Lorsque vous importez le fichier de paramètres de configuration personnalisé, XClarity Administrator crée une macro pour chaque paramètre de configuration du fichier.

Procédure

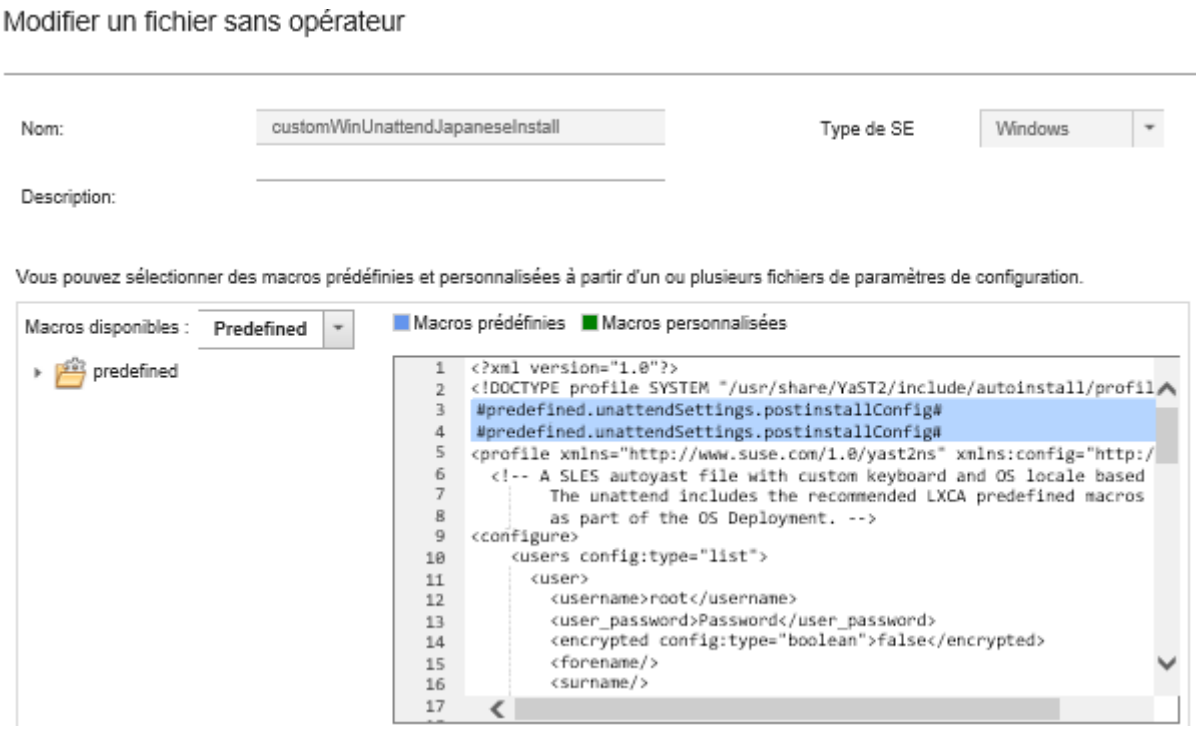
Procédez comme suit pour ajouter macros à un fichier sans opérateur.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Gérer les images de SE** pour afficher la page Déployer un système d'exploitation : déployer des images de SE.

Etape 2. Cliquez sur l'onglet **Fichiers sans opérateur**.

Etape 3. Sélectionnez le fichier sans opérateur que vous souhaitez modifier.

Etape 4. Cliquez sur l'icône **Éditer** ( ) pour afficher la boîte de dialogue Modifier un fichier sans opérateur.



Etape 5. Ajoutez les macros prédéfinis recommandées, par exemple :

1. Placez le curseur dans le fichier sans opérateur à n'importe quel endroit après la ligne 1 (après la balise <xml>).
2. Développez la liste **Prédéfinir → unattendSettings** dans la liste des macros disponibles.
3. Cliquez sur **preinstallConfig** et **postinstallConfig** pour ajouter les macros prédéfinies requises au fichier sans opérateur.

   Le code suivant est ajouté au fichier :

   #predefined.unattendSettings.preinstallConfig#
   #predefined.unattendSettings.postinstallConfig#

Etape 6. Ajoutez des macros prédéfinies ou personnalisées supplémentaires en plaçant le curseur à l'emplacement approprié dans le fichier sans opérateur, puis en cliquant sur la macro dans la liste.

Etape 7. Cliquez sur **Enregistrer**.

Association d'un fichier sans opérateur à un fichier de paramètres de configuration

Vous pouvez associer des paramètres de configuration (liaison) à un fichier sans opérateur, puis ajouter les macros personnalisées associées dans le fichier sans opérateur.

À propos de cette tâche

Vous pouvez ajouter des macros prédéfinies à un fichier sans opérateur sans associer un fichier de configuration des paramètres.

Vous ne pouvez pas modifier les fichiers de paramètres de configuration qui sont associés à des fichiers sans opérateur. Toutefois, vous pouvez copier un fichier associé puis modifier la copie.

Procédure

Procédez comme suit pour associer un fichier sans opérateur à un fichier de paramètres de configuration.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Distribution → Gérer les images de SE** pour afficher la page Déployer un système d'exploitation : déployer des images de SE.

Etape 2. Cliquez sur l'onglet **Fichiers sans opérateur**.

Etape 3. Sélectionnez le fichier sans opérateur personnalisé.

Etape 4. Cliquez sur l'icône **Associer un fichier de configuration** () pour afficher la boîte de dialogue Associer un fichier sans opérateur.

Etape 5. Sélectionnez un fichier de paramètres de configuration à associer au fichier sans opérateur.

Etape 6. Ajoutez des macros prédéfinies et personnalisées dans le fichier sans opérateur en plaçant le curseur dans l'éditeur à l'emplacement où vous souhaitez ajouter la macro, puis en cliquant sur la macro dans la liste des macros disponibles (voir Injection de macros prédéfinies et de macros personnalisées dans un fichier sans opérateur).

Vous pouvez injecter des macros dans le fichier sans opérateur à l'aide du nom unique de l'objet. Pour les objets nom imbriqués, séparez chaque objet à l'aide d'un point (par exemple, `server_specific_settings.server.locale`). Notez que vous n'incluez pas le nom supérieur.

Etape 7. Cliquez sur **Associer** pour lier les fichiers.

Importation de scripts d'installation personnalisés

Vous pouvez importer des scripts d'installation dans le référentiel d'images SE. Ces fichiers peuvent ensuite être utilisés pour personnaliser des images Linux et Windows.

À propos de cette tâche

Actuellement, seuls les scripts de post-installation sont pris en charge.

Le tableau suivant répertorie les types de fichiers des scripts d'installation pris en charge par Lenovo XClarity Administrator pour chaque système d'exploitation. Notez que certaines versions du système opération ne prennent pas en charge tous les types de fichier pris en charge par XClarity Administrator(par exemple, des versions RHEL peuvent ne pas inclure Perl dans le profil minimal et, par conséquent, les scripts Perl ne s'exécuteront pas). Assurez-vous que vous utilisez le type de fichier approprié pour les versions de système d'exploitation que vous voulez déployer.

Système d'exploitation	Types de fichier pris en charge	Informations complémentaires
Linux CentOS	Non pris en charge	
Microsoft® Windows® Azure Stack HCI	Non pris en charge	
Microsoft Windows Hyper-V Server	Non pris en charge	

Système d'exploitation	Types de fichier pris en charge	Informations complémentaires
Microsoft® Windows® Server	Fichier de commande (.cmd), PowerShell (.ps1)	Le chemin d'accès aux fichiers et données personnalisés par défaut est `C:\lxca`. Pour plus d'informations sur les scripts d'installation, voir Site Web d'ajout d'un script personnalisé à la configuration Windows
Red Hat® Enterprise Linux (RHEL) Server	Bash (.sh), Perl (.pm ou .pl), Python (.py)	Le chemin d'accès aux fichiers et données personnalisés par défaut est `/home/lxca`. Pour plus d'informations sur les scripts d'installation, voir RHEL : Page Web des scripts de post-installation
Rocky Linux	Bash (.sh), Perl (.pm ou .pl), Python (.py)	Le chemin d'accès aux fichiers et données personnalisés par défaut est `/home/lxca`. Pour plus d'informations sur les scripts d'installation, voir RHEL : Page Web des scripts de post-installation
SUSE® Linux Enterprise Server (SLES)	Bash (.sh), Perl (.pm ou .pl), Python (.py)	Le chemin d'accès aux fichiers et données personnalisés par défaut est `/home/lxca`. Pour plus d'informations sur les scripts d'installation, voir SUSE : Page Web des scripts utilisateur personnalisés
Ubuntu	Non pris en charge	
VMware vSphere® Hypervisor (ESXi) avec personnalisation Lenovo	Bash (.sh), Python (.py)	Le chemin d'accès aux fichiers et données personnalisés par défaut est `/home/lxca`. Pour plus d'informations sur les scripts d'installation, voir VMware : Page Web de scripts d'installation et de mise à niveau

Remarque : Le référentiel des images SE peut stocker un nombre illimité de fichiers prédéfinis et personnalisés, si l'espace disponible est suffisant pour stocker les fichiers.

Une fois les données collectées pendant le déploiement SE, XClarity Administrator crée une instance des paramètres du fichier de configuration (qui inclut les paramètres personnalisés dans le fichier sélectionné et un sous-ensemble de paramètres prédéfinis) sur le système hôte qui peut être utilisé par le script de post-installation.

Vous pouvez injecter des macros prédéfinies et personnalisées (paramètres de configuration) dans le script de post-installation à l'aide du nom unique de l'objet. Les valeurs prédéfinies sont basées de manière dynamique basé sur les instances de XClarity Administrator. Les macros personnalisées sont basées de manière dynamique sur la saisie de l'utilisateur qui est spécifiée pendant le déploiement du système d'exploitation.

Remarques :

- Placez le nom de macro entre des symboles dièse (#).
- Pour les objets imbriqués, séparez chaque nom objet à l'aide d'un point (par exemple, **#server_settings.server0.locale#**).

- Pour les macros personnalisées, n'incluez pas le nom d'objet le plus important. Pour les macros prédéfinies, ajoutez au nom de la macro le préfixe « prédéfini ».
- Lorsqu'un objet est créé à partir d'un modèle, le nom est ajouté avec un numéro unique, en commençant par 0 (par exemple, **server0** et **server1**).
- Vous pouvez également voir le nom de chaque macro à partir de la boîte de dialogue Déployer des images SE sous les onglets Paramètres personnalisés en passant le curseur sur l'icône Aide ( ) en regard de chaque paramètre personnalisé.
- Pour obtenir la liste des macros prédéfinies, voir Macros prédéfinies. Pour plus d'informations sur les paramètres de configuration et macros personnalisés, voir Macros personnalisées.

Les macros prédéfinies recommandées dans le fichier sans opérateur indiquent l'état de déploiement de système d'exploitation final et l'état lors du téléchargement et de l'exécution de scripts de post-installation. Vous pouvez modifier le script de post-installation afin d'inclure un rapport d'état personnalisé, selon le système d'exploitation cible. Pour plus d'informations, voir Ajout de rapport d'état personnalisé aux scripts d'installation.

Procédure

Pour importer des scripts d'installation dans le référentiel d'images SE, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Gérer les images de SE** pour afficher la page Déployer un système d'exploitation : déployer des images de SE.

Etape 2. Cliquez sur l'onglet **Scripts d'installation**.

Etape 3. Cliquez sur l'icône **Importer fichier** ( ). La boîte de dialogue Importation de script d'installation s'affiche.

Etape 4. Cliquez sur l'onglet **Importation locale** pour télécharger des fichiers à partir du système local ou cliquez sur l'onglet **Importation à distance** pour télécharger des fichiers à partir d'un serveur de fichiers distant.

Remarque : Pour télécharger un fichier à partir d'un serveur de fichiers distant, vous devez d'abord créer un profil de serveur de fichiers distant en cliquant sur l'icône **Configurer le serveur de fichiers** ( ). Pour plus d'informations, voir Configuration d'un serveur de fichiers distant .

Etape 5. Si vous choisissez d'utiliser un serveur de fichiers distant, sélectionnez-le dans la liste **Serveur de fichiers distant**.

Etape 6. Sélectionnez le type de système d'exploitation.

Etape 7. Entrez le nom du fichier du script d'installation, ou cliquez sur **Parcourir** pour rechercher le fichier que vous souhaitez importer.

Etape 8. **Facultatif :** Entrez une description pour le script d'installation.

Astuce : Utilisez les zones **Description** pour différencier les fichiers personnalisés portant le même nom.

Etape 9. **Facultatif :** Sélectionnez un type de total de contrôle pour vérifier que le fichier en cours de téléchargement n'est pas endommagé et copiez et collez la valeur de total de contrôle dans la zone de texte fournie.

Si vous sélectionnez un type de total de contrôle, vous devez indiquer une valeur de total de contrôle pour vérifier l'intégrité et la sécurité du fichier téléchargé. La valeur doit venir de la source sécurisée d'une organisation fiable. Si le fichier téléchargé correspond à la valeur de total de contrôle, le déploiement peut être poursuivi en toute sécurité. Sinon, vous devez télécharger à nouveau le fichier ou vérifier la valeur de total de contrôle.

Trois types de total de contrôle sont pris en charge :
- **MD5**
- **SHA1**
- **SHA256**

Etape 10. Cliquez sur **Importer**.

Astuce : Le fichier est téléchargé via une connexion réseau sécurisée. Par conséquent, la fiabilité et les performances du réseau ont une incidence sur le temps nécessaire à l'importation du fichier.

Si vous fermez l'onglet ou la fenêtre de navigateur Web dans lesquels le fichier est téléchargé en local avant la fin du téléchargement, l'importation échoue.

Après avoir terminé

Les scripts d'installation sont répertoriés sous l'onglet **Scripts d'installation** de la page Gérer les images de SE.

Depuis cette page, vous pouvez effectuer les actions suivantes.

- Créez un profil de serveur de fichiers distant en cliquant sur l'icône **Configurer le serveur de fichiers** ( ).
- Retirez les scripts d'installation sélectionnés en cliquant sur l'icône **Supprimer** ( ).

Pour plus d'informations sur l'ajout d'un script d'installation dans un profil d'image SE personnalisé, voir Création d'un profil d'image SE personnalisé.

Ajout de rapport d'état personnalisé aux scripts d'installation

Les macros prédéfinies recommandées dans le fichier sans opérateur indiquent l'état de déploiement de système d'exploitation final et l'état lors du téléchargement et de l'exécution de scripts de post-installation. Vous pouvez inclure un rapport d'état personnalisé dans les scripts de post-installation.

Linux

Pour Linux, vous pouvez utiliser la commande `curl` suivante pour indiquer l'état.

```
curl -X PUT -globoff #predefined.otherSettings.statusSettings.urlStatus#
-H "Content-Type: application/json" -d '{"deployStatus":{"id":"<status_ID>"}}'
-cert #predefined.otherSettings.statusSettings.certLocation#/cert.pem
-key #predefined.otherSettings.statusSettings.certLocation#/key.pem
-cacert #predefined.otherSettings.statusSettings.certLocation#/ca-bundle.crt
```

Où <*status_ID*> peut être l'une des valeurs suivantes.
- **44**. Le déploiement de la charge de travail a réussi
- **45**. Le déploiement de la charge de travail s'exécute avec un avertissement

- **46**. Le déploiement de la charge de travail a échoué
- **47**. Message de déploiement de charge de travail
- **48**. Erreur de script de post-installation personnalisé

Notez que la commande `curl` utilise des macros prédéfinies pour l'URL HTTPS utilisée par Lenovo XClarity Administrator pour la production de rapports d'état (**predefined.otherSettings.statusSettings.urlStatus**) et pour le dossier contenant les certificats qui sont nécessaires pour accéder au service Web urlStatus depuis le SE hôte au premier amorçage (**predefined.otherSettings.statusSettings.certLocation**). L'exemple suivant indique qu'une erreur s'est produite dans le script de post-installation.

L’exemple suivant indique qu’une erreur s’est produite dans le script de post-installation.

```
curl -X PUT -globoff #predefined.otherSettings.statusSettings.urlStatus#
-H "Content-Type: application/json" -d '{"deployStatus":{"id":"48"}}'
-cert #predefined.otherSettings.statusSettings.certLocation#/cert.pem
-key #predefined.otherSettings.statusSettings.certLocation#/key.pem
-cacert #predefined.otherSettings.statusSettings.certLocation#/ca-bundle.crt
```

Windows

Pour Windows, vous pouvez importer le script `LXCA.psm1`, puis appeler les commandes suivantes pour indiquer l'état.

- **initializeRestClient**

  Initialise le client REST. Utilisez la syntaxe suivante pour exécuter cette commande. Cette commande est requise avant l'exécution des commandes de génération de rapports.

  ```
  initializeRestClient
  ```

- **testLXCAConnection**

  Vérifie que XClarity Administrator peut se connecter au serveur hôte. Utilisez la syntaxe suivante pour exécuter cette commande. Cette commande est facultative mais elle est recommandée dans le script d'installation avant l’exécution des commandes de génération de rapports.

  ```
  testLXCAConnection –masterIP "#predefined.otherSettings.lxcaIp#"
  ```

- **reportWorkloadDeploymentSucceeded**

  Indique un message d'achèvement à consigner dans le journal des travaux de XClarity Administrator. Utilisez la syntaxe suivante pour exécuter cette commande.

  Astuce : Si la macro **#predefined.unattendSettings.reportWorkloadNotComplete#** est incluse dans un fichier sans opérateur personnalisé ou un script de post-installation, incluez la commande **reportWorkloadDeploymentSucceeded** dans le script de post-installation afin d'indiquer une opération réussie. Dans le cas contraire, XClarity Administrator indique automatiquement un état d'achèvement une fois tous les scripts de post-installation exécutés.

  ```
  reportWorkloadDeploymentSucceeded -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#"
  ```

- **reportWorkloadDeploymentRunningWithWarning**

  Indique un message d'avertissement à consigner dans le journal des travaux de XClarity Administrator. Utilisez la syntaxe suivante pour exécuter cette commande.

  ```
  reportWorkloadDeploymentRunningWithWarning -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" –WarningMessage "<message_text>"
  ```

- **reportWorkloadDeploymentFailed**

  Indique un message d'échec à consigner dans le journal des travaux de XClarity Administrator. Utilisez la syntaxe suivante pour exécuter cette commande.

  ```
  reportWorkloadDeploymentFailed -masterIP "#predefined.otherSettings.lxcaIp#"
  ```

```
-UUID "#predefined.hostPlatforms.uuid#" -ErrorMessage "<message_text>"
```

- **reportCustomPostInstallScriptError**

  Indique un message d'erreur de script de post-installation à consigner dans le journal des travaux de XClarity Administrator. Utilisez la syntaxe suivante pour exécuter cette commande.

  ```
  reportCustomPostInstallScriptError -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" -Message "<message_text>"
  ```

- **reportWorkloadDeploymentMessage**

  Indique un message général à consigner dans le journal des travaux de XClarity Administrator sans que cela n'ait d'incidence sur l'état du déploiement. Utilisez la syntaxe suivante pour exécuter cette commande.

  ```
  reportWorkloadDeploymentMessage -masterIP "#predefined.otherSettings.lxcaIp#"
  -UUID "#predefined.hostPlatforms.uuid#" -Message "<message_text>"
  ```

Où <*message_text*> est le message que vous souhaitez renvoyer à XClarity Administratorpour chaque condition d'état.

Notez que ces commandes utilisent des macros prédéfinies pour l'adresse IP de l'instance de XClarity Administrator (**#predefined.otherSettings.lxcaIp#**) et pour l'UUID du serveur hôte sur lequel le système d'exploitation doit être déployé (**#predefined.hostPlatforms.uuid#**).

L'exemple suivant est un script d'installation PowerShell qui installe Java et signale une erreur en cas d'échec de l'installation

```
import-module C:\windows\system32\WindowsPowerShell\v1.0\Modules\LXCA\LXCA.psm1

initializeRestClient

testLXCAConnection –masterIP "#predefined.otherSettings.lxcaIp#"

Write-Output "Reporting status to Lenovo XClarity Administator..."
   reportWorkloadDeploymentMessage -masterIP "#predefined.otherSettings.lxcaIp#"
   -UUID "#predefined.hostPlatforms.uuid#" -Message "Installing Java"

Write-Output "Install Java...."
   Invoke-Command -ScriptBlock {#predefined.otherSettings.deployDataAndSoftwareLocation#\jre-8u151-windows-x64.exe
   [INSTALLCFG=#predefined.otherSettings.deployDataAndSoftwareLocation#\java_configfile.cfg] /s}

if ($LastExitCode -ne 0) {
   reportWorkloadDeploymentFailed -masterIP "#predefined.otherSettings.lxcaIp#"
      -UUID "#predefined.hostPlatforms.uuid#" -ErrorMessage "Java could not be installed"
}

Write-Output "Completed install of Java for Administrator user."
```

Importation de logiciels personnalisés

Vous pouvez importer des logiciels dans le référentiel d'images SE. Ces fichiers peuvent ensuite être utilisés pour personnaliser des images Linux et Windows

À propos de cette tâche

Les fichiers de logiciels personnalisés sont installés une fois le déploiement du système d'exploitation terminé et les scripts d'installation exécutés.

Les types de fichier suivants sont pris en charge pour les logiciels personnalisés.

Système d'exploitation	Types de fichier pris en charge	Informations complémentaires
Linux CentOS	Non pris en charge	
Microsoft® Windows® Azure Stack HCI	Non pris en charge	
Microsoft Windows Hyper-V Server	Non pris en charge	
Microsoft Windows® Server	Un fichier .zip contenant le contenu du logiciel.	Le chemin d'accès aux fichiers et données personnalisés par défaut est `C:\lxca`.
Red Hat® Enterprise Linux (RHEL) Server	Un fichier .tar.gz contenant le contenu du logiciel	Le chemin d'accès aux fichiers et données personnalisés par défaut est `/home/lxca`.
SUSE® Linux Enterprise Server (SLES)	Un fichier .tar.gz contenant le contenu du logiciel	Le chemin d'accès aux fichiers et données personnalisés par défaut est `/home/lxca`.
Rocky Linux	Un fichier .tar.gz contenant le contenu du logiciel	Le chemin d'accès aux fichiers et données personnalisés par défaut est `/home/lxca`.
Ubuntu	Non pris en charge	
VMware vSphere® Hypervisor (ESXi) avec personnalisation Lenovo	Un fichier .tar.gz contenant le contenu du logiciel	Le chemin d'accès aux fichiers et données personnalisés par défaut est `/home/lxca`.

Remarque : Le référentiel des images SE peut stocker un nombre illimité de fichiers prédéfinis et personnalisés, si l'espace disponible est suffisant pour stocker les fichiers.

Procédure

Pour importer des logiciels dans le référentiel d'images SE, procédez comme suit.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Distribution → Gérer les images de SE** pour afficher la page Déployer un système d'exploitation : déployer des images de SE.

Etape 2. Cliquez sur l'onglet **Logiciels**.

Etape 3. Cliquez sur l'icône **Importer fichier** ( ). La boîte de dialogue Importation de script d'installation s'affiche.

Etape 4. Cliquez sur l'onglet **Importation locale** pour télécharger des fichiers à partir du système local ou cliquez sur l'onglet **Importation à distance** pour télécharger des fichiers à partir d'un serveur de fichiers distant.

Remarque : Pour télécharger un fichier à partir d'un serveur de fichiers distant, vous devez d'abord créer un profil de serveur de fichiers distant en cliquant sur l'icône **Configurer le serveur de fichiers** (). Pour plus d'informations, voir Configuration d'un serveur de fichiers distant .

Etape 5. Si vous choisissez d'utiliser un serveur de fichiers distant, sélectionnez-le dans la liste **Serveur de fichiers distant**.

Etape 6. Sélectionnez le type de système d'exploitation.

Etape 7. Entrez le nom de fichier du fichier de logiciel, ou cliquez sur **Parcourir** pour rechercher le fichier que vous souhaitez importer.

Etape 8. **Facultatif :** Entrez une description du fichier de logiciel.

Astuce : Utilisez les zones **Description** pour différencier les fichiers personnalisés portant le même nom.

Etape 9. **Facultatif :** Sélectionnez un type de total de contrôle pour vérifier que le fichier en cours de téléchargement n'est pas endommagé et copiez et collez la valeur de total de contrôle dans la zone de texte fournie.

Si vous sélectionnez un type de total de contrôle, vous devez indiquer une valeur de total de contrôle pour vérifier l'intégrité et la sécurité du fichier téléchargé. La valeur doit venir de la source sécurisée d'une organisation fiable. Si le fichier téléchargé correspond à la valeur de total de contrôle, le déploiement peut être poursuivi en toute sécurité. Sinon, vous devez télécharger à nouveau le fichier ou vérifier la valeur de total de contrôle.

Trois types de total de contrôle sont pris en charge :
- **MD5**
- **SHA1**
- **SHA256**

Etape 10. Cliquez sur **Importer**.

Astuce : Le fichier est téléchargé via une connexion réseau sécurisée. Par conséquent, la fiabilité et les performances du réseau ont une incidence sur le temps nécessaire à l'importation du fichier.

Si vous fermez l'onglet ou la fenêtre de navigateur Web dans lesquels le fichier est téléchargé en local avant la fin du téléchargement, l'importation échoue.

Après avoir terminé

Les scripts d'installation sont répertoriés sous l'onglet **Logiciels** de la page Gérer les images de SE.

Depuis cette page, vous pouvez effectuer les actions suivantes.

- Créez un profil de serveur de fichiers distant en cliquant sur l'icône **Configurer le serveur de fichiers** ().
- Retirez des fichiers de logiciels sélectionnés en cliquant sur l'icône **Supprimer** ().

Pour plus d'informations sur l'ajout d'un fichier de logiciel dans un profil d'image SE personnalisé, voir Création d'un profil d'image SE personnalisé.

Création d'un profil d'image SE personnalisé

Vous pouvez ajouter des pilotes de périphérique personnalisés, des fichiers d'amorçage (Windows uniquement), des paramètres de configuration, des fichiers sans opérateur, des scripts d'installation et des logiciels à un profil d'image SE prédéfini existant dans le référentiel d'images SE. Lorsque vous ajoutez des fichiers à une image SE, Lenovo XClarity Administrator crée un profil personnalisé pour cette image SE. Le profil personnalisé comporte les fichiers personnalisés et des options d'installation.

Avant de commencer

Les fichiers personnalisés que vous voulez ajouter doivent exister dans le référentiel des images SE (voir Importation de fichiers d'amorçage, Importation de pilotes de périphérique, Importation de paramètres de configuration personnalisés, Importation de fichiers sans opérateur personnalisés, Importation de scripts d'installation personnalisés et Importation de logiciels personnalisés).

Procédure

Pour personnaliser une image SE, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Gérer les images de SE** pour afficher la page Déployer un système d'exploitation : déployer des images de SE.

Etape 2. Cliquez sur l'onglet **Images SE**.

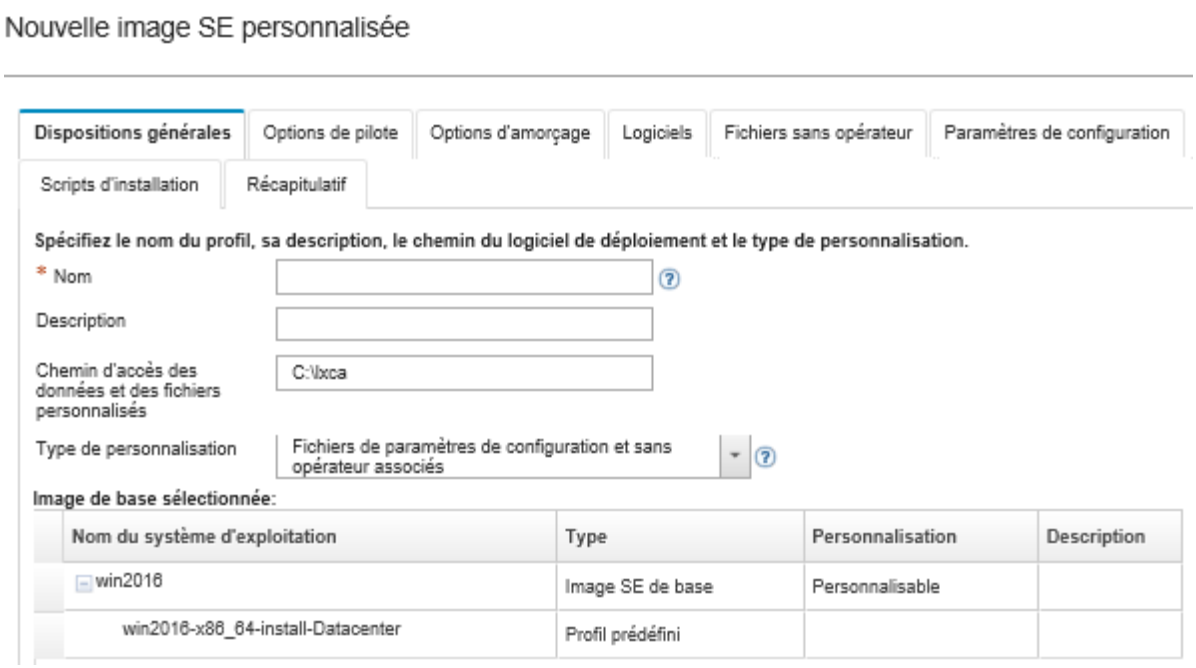
Etape 3. Sélectionnez le profil d'image SE prédéfini que vous souhaitez personnaliser.

La colonne **Personnalisation** identifie les images SE à personnaliser. Cliquez sur l'icône **Aide** ( ) pour obtenir plus d'informations sur la personnalisation d'une image SE spécifique.

- **Personnalisable**. L'image SE prend en charge la personnalisation mais n'est pas personnalisée.
- **Non personnalisable**. L'image SE ne prend pas en charge la personnalisation.

Remarque : Vous pouvez importer des images SE de base supplémentaires (au format .iso) à partir d'un système local ou distant en cliquant sur l'icône **Importer fichier** ( ).

Etape 4. Cliquez sur l'icône **Créer un profil personnalisé** ( ). La boîte de dialogue Nouvelle image SE personnalisée s'affiche.



Etape 5. Sous l'onglet **Général**, spécifiez un nom, une description, le chemin d'accès aux fichiers personnalisés et aux données de déploiement sur l'hôte de déploiement, ainsi que le type de personnalisation du nouveau profil d'image SE personnalisé.

Le type de personnalisation peut être l'un des suivants :
- **Fichiers sans opérateur seulement**
- **Fichiers de configuration seulement**
- **Fichiers de configuration et sans opérateur non associés**
- **Fichiers de configuration et sans opérateur associés**
- **Aucun**

Etape 6. Cliquez sur **Suivant**.

Etape 7. Sous l'onglet **Pilotes de périphérique**, sélectionnez le pilote de périphérique que vous souhaitez ajouter au profil d'image SE Linux.

Pour obtenir la liste des formats pris en charge, voir Importation de pilotes de périphérique.

Le fichier sélectionné est appliqué une fois que vous avez terminé l'exécution de l'assistant de configuration.

Remarque : Vous pouvez importer des pilotes de périphérique supplémentaires à partir d'un système local ou distant en cliquant sur l'icône **Importer fichier** ( ).

Etape 8. Cliquez sur **Suivant**.

Etape 9. (Windows uniquement) Sous l'onglet **Options d'amorçage**, sélectionnez les fichiers d'amorçage que vous souhaitez ajouter au profil d'image SE Windows.

Pour obtenir la liste des formats pris en charge, voir Importation de fichiers d'amorçage.

Le fichier sélectionné est appliqué une fois que vous avez terminé l'exécution de l'assistant de configuration.

Etape 10. Cliquez sur **Suivant**.

Etape 11. Sous l'onglet **Paramètres de configuration** (le cas échéant), sélectionnez un ou plusieurs fichiers de configuration personnalisés à ajouter au profil d'image SE. Vous pouvez sélectionner un seul fichier.

Etape 12. Cliquez sur **Suivant**.

Etape 13. Sous l'onglet **Fichiers sans opérateur** :

a. Sélectionnez le fichier sans opérateur que vous souhaitez ajouter au profil d'image SE.

Pour obtenir la liste des formats pris en charge, voir Importation de fichiers sans opérateur personnalisés.

Le fichier sélectionné est appliqué une fois que vous avez terminé l'exécution de l'assistant de configuration.

b. Sélectionnez un fichier de configuration à associer au fichier sans opérateur dans la colonne **Associer un fichier de configuration**

c. Sélectionnez si vous le souhaitez des macros personnalisés qui sont disponibles dans le fichier de configuration sélectionné ou ajoutez des macros personnalisées au format .xml.

Etape 14. Cliquez sur **Suivant**.

Etape 15. Sous l'onglet **Scripts d'installation** (le as échéant), sélectionnez les scripts d'installation que vous souhaitez ajouter au profil d'image SE Windows. Vous pouvez sélectionner au plus un script de post-installation.

Pour obtenir la liste des formats pris en charge, voir Importation de scripts d'installation personnalisés.

Le fichier sélectionné est appliqué une fois que vous avez terminé l'exécution de l'assistant de configuration.

Remarque : Vous pouvez importer des scripts d'installation supplémentaires à partir d'un système local ou distant en cliquant sur l'icône **Importer fichier** ().

Etape 16. Cliquez sur **Suivant**.

Etape 17. Sous l'onglet **Logiciels**, sélectionnez les logiciels que vous souhaitez ajouter au profil d'image SE Linux.

Pour obtenir la liste des formats pris en charge, voir Importation de logiciels personnalisés.

Le fichier sélectionné est appliqué une fois que vous avez terminé l'exécution de l'assistant de configuration.

Remarque : Vous pouvez importer des logiciels supplémentaires à partir d'un système local ou distant en cliquant sur l'icône **Importer fichier** ().

Etape 18. Cliquez sur **Suivant**.

Etape 19. Passez en revue les paramètres sur l'onglet **Récapitulatif** et cliquez sur **Personnaliser** pour créer le profil d'image SE personnalisé.

Après avoir terminé

Le profil d'image SE personnalisé est répertorié sous le système d'exploitation de base sur l'onglet **Images SE** de la page Gérer les images de SE.

Depuis cette page, vous pouvez effectuer les actions suivantes :

- Importer un profil d'image SE personnalisé et l'appliquer à une image SE de base en cliquant sur **Importer/exporter le profil → Exporter une image de profil personnalisé** (voir Importation d'un profil d'image SE personnalisé).
- Exporter un profil d'image SE personnalisé sélectionné en cliquant sur **Importer/exporter le profil → Exporter une image de profil personnalisé**.
- Modifier un profil d'image SE personnalisé sélectionné en cliquant sur l'icône **Éditer** ( ).
- Retirer un profil d'image SE personnalisé sélectionné en cliquant sur l'icône **Supprimer** ( ).

Configuration des paramètres de déploiement SE

Les paramètres globaux sont utilisés en tant que paramètres de valeurs par défaut lorsque des systèmes d'exploitation sont déployés.

À propos de cette tâche

La page Paramètres globaux vous permet de configurer les paramètres suivants :

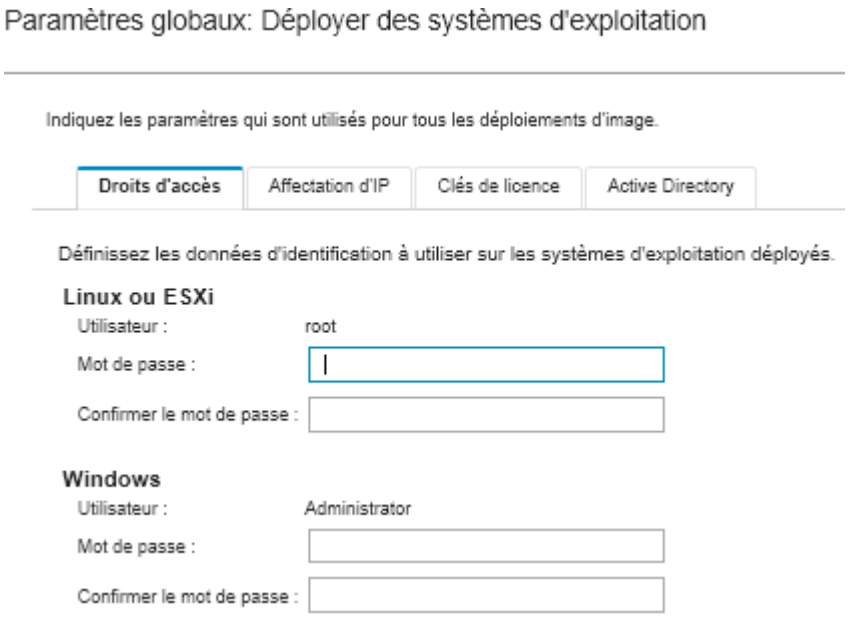
- Le mot de passe du compte utilisateur administrateur à utiliser pour le déploiement des systèmes d'exploitation
- La méthode à utiliser pour affecter des adresses IP aux serveurs
- Les clés de licence à utiliser lors de l'activation des systèmes d'exploitation installés
- Associer éventuellement un domaine Active Directory dans le cadre du déploiement de système d'exploitation Windows

Procédure

Pour configurer les paramètres globaux à utiliser pour tous les serveurs, procédez comme suit.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Distribution → Déployer des images de SE** pour afficher la page Déployer des images de SE.

Etape 2. Cliquez sur l'icône **Paramètres globaux** ( ) pour afficher la boîte de dialogue Paramètres globaux : Déployer des systèmes d'exploitation.



Etape 3. Sur l'onglet **Données d'identification**, entrez le mot de passe du compte administrateur à utiliser pour se connecter au système d'exploitation.

Etape 4. Sur l'onglet **Affectation d'IP**, sélectionnez les options suivantes.

a. **Facultatif :** Sélectionnez **Utiliser les réseaux VLAN** pour autoriser la configuration des paramètres VLAN dans la boîte de dialogue Paramètres réseau (voir Configuration des paramètres réseau pour les serveurs gérés).

Remarques : Remarques :

- Le marquage VLAN n'est pas pris en charge pour les déploiements du système d'exploitation Linux.
- Le marquage VLAN n'est pas pris en charge pour les déploiements du système d'exploitation sur les appareils ThinkServer.
- Le mode VLAN est pris en charge uniquement pour les serveurs qui ont des adresses MAC dans leur inventaire. Si AUTO est la seule adresse MAC disponible pour un serveur, les réseaux VLAN ne peuvent pas être utilisés pour déployer des systèmes d'exploitation sur ce serveur.

b. Sélectionnez la méthode permettant d'affecter des adresses IP lors de la configuration du système d'exploitation déployé :

Remarque : L'interface réseau XClarity Administrator qui est utilisée pour la gestion doit être configuré pour la connexion au contrôleur de gestion de la carte mère à l'aide de la même méthode d'adresse IP que vous choisissez dans la boîte de dialogue Paramètres globaux : Déployer des systèmes d'exploitation. Par exemple, si XClarity Administrator est configuré pour utiliser eth0 pour la gestion et si vous choisissez d'utiliser des adresses IPv6 statiques affectées manuellement lors de la configuration du SE déployé, l'interface eth0 doit être configurée avec une adresse IPv6 qui dispose d'une connectivité au contrôleur de gestion de la carte mère.

- **Affecter manuellement une adresse IPv4 statique**. Si vous choisissez d'affecter des adresses IPv4 statiques, prenez soin de configurer l'adresse IPv4 statique, l'adresse de passerelle et le masque de sous-réseau pour le serveur avant de déployer le système d'exploitation (voir Configuration des paramètres réseau pour les serveurs gérés).
- **Utiliser le protocole DHCP (Dynamic Host Configuration Protocol) pour affecter les adresses**. Si vous disposez déjà d'une infrastructure DHCPv4 dans votre réseau, vous pouvez utiliser cette infrastructure pour affecter des adresses IP aux serveurs.

  Remarque : DHCP IPv6 n'est pas pris en charge pour le déploiement des systèmes d'exploitation.
- **Affecter manuellement une adresse IPv6 statique**. Si vous choisissez d'affecter des adresses IPv6 statiques, prenez soin de configurer l'adresse IPv6 statique, l'adresse de passerelle et le masque de sous-réseau pour le serveur avant de déployer le système d'exploitation (voir Configuration des paramètres réseau pour les serveurs gérés).

Etape 5. **Facultatif :** Sur l'onglet **Clés de licence**, spécifiez les clés de licence de volume globales à utiliser lors de l'activation des systèmes d'exploitation Windows installés.

Lorsque vous spécifiez des clés de licence de volume globales sur cet onglet, vous pouvez sélectionner les clés de licence spécifiées pour tous les profils d'image SE Windows à partir de la page Déployer des images de SE.

Astuce : XClarity Administrator prend en charge des clés de licence de volume globales pour les installations Windows et des clés de licence de détail individuelles pour Windows et VMware ESXi. Vous pouvez spécifier des clés de licence de détail individuelles dans le cadre de la procédure de déploiement (voir Déploiement d'une image du système d'exploitation).

Etape 6. **Facultatif :** Sur l'onglet **Active Directory**, configurez les paramètres Active Directory pour les déploiements de système d'exploitation Windows. Pour plus d'informations sur l'intégration à Active Directory, voir Intégration à Windows Active Directory.

Etape 7. Cliquez sur **OK** pour fermer la boîte de dialogue.

Configuration des paramètres réseau pour les serveurs gérés

Les paramètres réseau sont des options de configuration spécifiques à chaque serveur. Vous devez configurer les paramètres réseau pour un serveur géré avant de pouvoir déployer un système d'exploitation sur ce serveur.

À propos de cette tâche

Si vous utiliser DHCP pour affecter dynamiquement les adresses IP, vous devez configurer les adresses MAC.

Si vous utilisez des adresses IP statiques, vous devez configurer les paramètres réseau suivants pour un serveur spécifique, avant de pouvoir déployer un système d'exploitation sur ce serveur. Une fois ces paramètres configurés, l'état de déploiement du serveur est modifié à « Prêt. » (Notez que certaines zones ne sont pas disponibles pour les adresses IPv6 statiques.)

- Nom d'hôte

  Le nom d'hôte doit également respecter les règles suivantes :
  - Le nom d'hôte de chaque serveur géré doit être unique.
  - Le nom d'hôte peut contenir des chaînes (étiquettes) qui sont séparées par un point (.).
  - Chaque étiquette peut contenir des lettres ASCII, des chiffres et des tirets (-). Toutefois, la chaîne ne peut ni commencer ni se terminer par un tiret, et ne peut pas contenir uniquement des chiffres.
  - La première étiquettes doit contenir de 2 à 15 caractères. Les étiquettes suivantes doivent contenir de 2 à 63 caractères.
  - La longueur totale du nom d'hôte ne doit pas dépasser 255 caractères.
- Adresse MAC du port sur l'hôte sur lequel le système d'exploitation doit être installé.

  L'adresse MAC est définie à AUTO par défaut. Ce paramètre détecte automatiquement les ports Ethernet qui peuvent être configurés et utilisés pour le déploiement. La première adresse MAC (port) qui est détectée est utilisée par défaut. Si la connectivité est détectée sur un adresse MAC différente, l'hôte XClarity Administrator est automatiquement redémarré pour utiliser l'adresse MAC nouvellement détectée pour le déploiement.

  Vous pouvez déterminer l'état du port d'adresse MAC utilisé pour le déploiement SE en accédant au menu déroulant **Adresse MAC** de la boîte de dialogue Paramètres réseau. Si plusieurs ports sont activés ou si tous les ports sont arrêtés, AUTO est utilisé par défaut.

  Remarques :

  - Les ports réseau virtuels ne sont pas pris en charge. N'utilisez pas un port réseau physique pour simuler plusieurs ports réseau virtuels.
  - Lorsque le paramètre réseau du serveur est défini sur AUTO, XClarity Administrator peut détecter automatiquement les ports réseau dans les emplacements 1 à 16. Au moins un port des emplacements 1 à 16 doit disposer d'une connexion à XClarity Administrator.
  - Si vous souhaitez utiliser un port réseau dans l'emplacement 17 ou supérieur pour l'adresse MAC, vous ne pouvez pas utiliser AUTO. Au lieu de cela, vous devez définir le paramètre réseau du serveur sur l'adresse MAC du port spécifique que vous souhaitez utiliser.
  - Toutes les adresses MAC hôtes ne sont pas affichées pour les serveurs ThinkServer. Dans la plupart des cas, les adresses MAC pour les cartes Ethernet AnyFabric sont listées dans la boîte de dialogue

Éditer les paramètres réseau. Les adresses MAC d'autres cartes Ethernet (tels que LAN-on-motherboard) ne sont pas listées. Dans le cas où les adresses MAC ne sont pas disponibles pour une carte, utilisez la méthode AUTO pour les déploiements non VLAN.

- Adresse IP et masque de sous-réseau
- Passerelle IP
- Jusqu'à deux serveurs DNS (Domain Name System)
- Vitesse d'unité MTU (unité de transmission maximale)
- ID VLAN, si le mode IP VLAN est activé

Si vous choisissez d'utiliser les réseaux VLAN, vous pouvez affecter un ID VLAN à la carte réseau qui est en cours de configuration.

Procédure

Procédez comme suit afin de configurer les paramètres réseau pour un ou plusieurs serveurs.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Déployer des images SE** pour afficher la page Déployer un système d'exploitation : déployer des images SE.

Etape 2. Sélectionnez un ou plusieurs serveurs à configurer. Vous pouvez configurer jusqu'à 28 serveurs à la fois.

Etape 3. Cliquez sur **Modifier la sélection → Paramètres réseau** pour afficher la page Éditer les paramètres réseau.

Etape 4. Remplissez les zones du tableau pour chaque serveur.

Conseil : afin d'éviter de remplir chaque ligne, vous pouvez mettre toutes les lignes à jour dans le tableau pour certaines zones :

a. Cliques sur **Modifier toutes les lignes → Nom d'hôte** pour définir les noms d'hôtes pour l'ensemble des serveurs, à l'aide d'un schéma de désignation prédéfini ou personnalisé.

b. Cliquez sur **Modifier toutes les lignes → Adresse IP** pour affecter une plage d'adresses IP, un masque de sous-réseau et une passerelle. L'adresse IP est affectée à chaque serveur, en commençant par la première adresse IP et en terminant par la dernière adresse IP affichée. Le masque de sous-réseau et l'adresse IP de passerelle sont appliqués à chaque serveur.

c. Cliquez sur **Modifier toutes les lignes → Domain Name System (DNS)** pour définir les serveurs DNS devant être utilisés par le système d'exploitation pour la recherche DNS. Si le réseau définit automatiquement les serveurs DNS, ou si vous ne voulez pas définir de serveurs DNS, sélectionnez **Aucun**.

d. Cliquez sur **Modifier toutes les lignes → Unité MTU (unité de transmission maximale)** afin de définir la MTU devant être utilisée sur la carte Ethernet configurée sur les systèmes d'exploitation déployés.

e. Cliquez sur **Modifier toutes les lignes → ID VLAN** afin de définir un ID VLAN spécifique pour le marquage VLAN du système d'exploitation.

Vous pouvez indiquer une valeur allant de 1 à 4 095. La valeur par défaut est 1, ce qui signifie que le mode VLAN n'est pas utilisé.

Cette option n'est disponible que lorsque la fonction Utiliser les réseaux VLAN est activée sur la boîte de dialogue Paramètres globaux (voir Configuration des paramètres de déploiement SE).

Important :

- Indiquez un ID VLAN uniquement lorsqu'un marquage VLAN est requis pour fonctionner sur le réseau. **L'utilisation de balises VLAN** peut affecter la routabilité de réseau entre le système d'exploitation hôte et le XClarity Administrator.
- Le châssis ou les commutateurs de la partie supérieure de l'armoire doivent être configurés indépendamment afin de traiter les paquets marqués VLAN. Assurez-vous que XClarity Administrator et le réseau de données sont configurés pour traiter correctement ces paquets.
- Le mode VLAN est pris en charge uniquement pour les serveurs qui ont des adresses MAC dans leur inventaire. Si AUTO est la seule adresse MAC disponible pour un serveur, les réseaux VLAN ne peuvent pas être utilisés pour déployer des systèmes d'exploitation sur ce serveur.
- Le marquage VLAN n'est pas pris en charge pour les déploiements de système d'exploitation Linux ; toutefois, si vous souhaitez déployer avec VLAN sur certains serveurs et déployer également sur d'autres serveurs sans VLAN en même temps, vous pouvez forcer le déploiement en mode VLAN en définissant l'ID VLAN sur 1.

Etape 5. Cliquez sur **OK** pour enregistrer les paramètres. Les paramètres sont enregistrés et persistants uniquement dans le cache de stockage local de votre navigateur web.

Résultats

Chaque serveur configuré présente désormais un état de déploiement **Prêt** sur la page Déployer un système d'exploitation : déployer des images de SE.

Choix de l'emplacement de stockage pour les serveurs gérés

Choisissez l'emplacement de stockage préféré où vous souhaitez déployer l'image du système d'exploitation pour un ou plusieurs serveurs.

Avant de commencer

Passez en revue les questions liées au stockage et au démarrage avant de choisir un emplacement de stockage (voir Remarques sur le déploiement de systèmes d'exploitation).

Vous pouvez déployer un système d'exploitation sur les types de stockage suivants :

- **Unité de disque locale**

  Seuls les disques connectés à un contrôleur RAID ou à un adaptateur de bus hôte SAS/SATA sont pris en charge.

  Lenovo XClarity Administrator installe l'image du système d'exploitation sur le disque RAID local répertorié en premier sur le serveur géré.

  Si la configuration RAID sur le serveur n'est pas correctement configurée, ou si elle est inactive, le disque local peut ne pas être visible pour Lenovo XClarity Administrator. Pour résoudre le problème, activez la configuration RAID à l'aide des modèles de configuration (voir Définition d'un stockage local)ou à l'aide du logiciel de gestion RAID sur le serveur.

  Remarques :

  – Si un lecteur M.2 est également présent, le lecteur de disque local doit être configuré pour un RAID matériel.

  – Si un adaptateur SATA est activé, le mode SATA *ne doit pas* être paramétré sur « IDE ».

- Pour les serveurs ThinkServer, des systèmes d'exploitation peuvent être déployés uniquement sur le disque local. Le stockage SAN et les hyperviseurs imbriqués ne sont pas pris en charge.
- Pour les serveurs ThinkServer, la configuration est disponible uniquement dans le logiciel de gestion RAID sur le serveur.

Pour obtenir un exemple de scénario de déploiement de VMware ESXi 5.5 sur une unité de disque installée en local, voir Déploiement d'ESXi sur un disque dur local.

- **(ESXi uniquement) Hyperviseur imbriqué (adaptateur de support USB ou SD)**

  Cet emplacement s'applique uniquement lorsqu'une image VMware ESXi est déployée sur les serveurs gérés.

  L'hyperviseur imbriqué peut être l'un des dispositifs suivants :

  - Clé USB de licence IBM (PN 41Y8298) ou clé USB de licence Lenovo montée sur un port spécifique sur l'un des serveurs suivants :
    - Flex System x222
    - Flex System x240
    - Flex System x440
    - Flex System x480
    - Flex System x880
    - System x3850 X6
    - System x3950 X6
  - Adaptateur de support SD installé sur les serveurs suivants :
    - Flex System x240 M5
    - System x3500 M5
    - System x3550 M5
    - System x3650 M5

    En outre, l'unité doit être configurée comme suit :
    - Les unités appropriées sur l'adaptateur de support doivent être définies.
    - Le mode de l'adaptateur de support SD doit être défini sur **Opérationnel**.
    - Le propriétaire doit être défini sur Système ou Système uniquement.
    - L'accès doit être défini sur Lecture/Écriture.
    - Un numéro d'unité logique de 0 doit être attribué à l'unité.

    Important : Si l'adaptateur de support SD n'est pas correctement configuré, le déploiement du système d'exploitation sur l'adaptateur de support SD Lenovo XClarity Administrator n'aboutira pas.

    Vous pouvez définir le mode de l'adaptateur de support SD sur **Configuration** et configurer l'adaptateur de support grâce à l'interface CLI du contrôleur de gestion à l'aide de la commande `sdraid`. Pour plus d'informations sur la définition du mode de l'adaptateur de support SD et la configuration de l'adaptateur à partir de l'interface CLI, voir Documentation en ligne d'Integrated Management Module II.

  Si deux clés d'hyperviseur sont installées sur le serveur géré, le programme d'installation de VMware sélectionne la première clé répertoriée pour le déploiement.

  Remarque : Si vous essayez de déployer Microsoft Windows sur un serveur géré qui possède une clé d'hyperviseur, des problèmes peuvent survenir même si vous ne sélectionnez pas la clé d'hyperviseur imbriqué. Si des erreurs de déploiement Windows se produisent, retirez la clé d'hyperviseur imbriqué du serveur géré et essayez de redéployer Microsoft Windows sur ce serveur.

- **unité M.2**

  Lenovo XClarity Administrator installe l'image du système d'exploitation sur la première unité M.2 qui est configurée sur le serveur de gestion.

  Le stockage M.2 est pris en charge uniquement sur les serveurs ThinkSystem.

Attention : Si un appareil géré possède à la fois des unités locales (SATA, SAS ou SSD) qui ne sont pas configurées pour le RAID matériel et des unités M.2, vous devez désactiver les unités locales pour utiliser les unités M.2, ou désactiver les unités M.2 pour utiliser les unités locales. Vous pouvez désactiver les contrôleurs de stockage intégrés et les mémoires mortes en option du stockage hérité et UEFI à l'aide des modèles de configuration en sélectionnant Désactiver le disque local dans l'onglet Stockage local de l'assistant ou en créant un Modèle de configuration à partir d'un serveur existant, puis désactiver les appareils M.2 dans le modèle UEFI étendu.

- **Stockage SAN**

  Lenovo XClarity Administrator installe l'image du système d'exploitation sur la cible d'amorçage SAN qui est configurée sur le serveur géré.

  Les protocoles suivants sont pris en charge.
  - Fibre Channel
  - Fibre Channel over Ethernet
  - SAN iSCSI (avec uniquement un adaptateur Emulex VFA5.2 2x10 GbE SFP+ et FCoE/iSCSI SW ou un adaptateur Emulex VFA5.2 ML2 2x10 GbE SFP+ et des adaptateurs FCoE/iSCSI SW)

  Sur les serveurs rack gérés, vous pouvez uniquement déployer Windows ou RHEL sur un stockage SAN. Vérifiez que la cible d'amorçage SAN est configurée sur les serveurs gérés. Vous pouvez également configurer la cible d'amorçage SAN FC à l'aide d'un modèle de serveur (voir Définition d'options d'amorçage)

  Lors du déploiement de VMware ESXi :

  - Les disques durs locaux doivent être désactivés ou retirés du serveur. Vous pouvez désactiver les disques durs locaux à l'aide de modèles de serveur (voir Définition d'un stockage local).
  - Si plusieurs volumes SAN sont disponibles, seul le premier volume est utilisé pour le déploiement.

  Vérifiez que le volume de SE sur lequel vous effectuez l'installation est le seul volume visible pour le système d'exploitation.

  Pour obtenir un exemple de scénario de déploiement de VMware ESXi 5.5 sur des volumes SAN connectés à des serveurs, voir Déploiement d'ESXi sur un stockage SAN.

Remarque : Chaque serveur doit disposer d'un adaptateur RAID matériel ou d'un adaptateur de bus hôte SAS/SATA installé et configuré. Le RAID logiciel généralement présent sur l'adaptateur de stockage Intel SATA embarqué ou sur le stockage qui est configuré comme JBOD n'est pas pris en charge. Toutefois si un adaptateur RAID matériel n'est pas présent, le fait de paramétrer l'adaptateur SATA en **mode AHCI SATA** activé pour le déploiement de système d'exploitation ou de configurer des disques corrects non configurés en mode JBOD peut fonctionner dans certains cas. Pour plus d'informations, voir Le programme d'installation du système d'exploitation ne trouve pas le disque sur lequel vous voulez effectuer l'installation XClarity Administrator dans la documentation en ligne de XClarity Administrator.

Procédure

Pour choisir l'emplacement de stockage pour un ou plusieurs serveurs gérés, procédez comme suit.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Distribution → Déployer des images SE** pour afficher la page Déployer des images SE.

Etape 2. Sélectionnez les serveurs dont vous souhaitez modifier les paramètres de stockage.

Etape 3. Cliquez sur **Modifier la sélection → Emplacement de stockage** pour modifier l'ordre de priorité des emplacements de stockage pour tous les serveurs sélectionnés. Si le premier emplacement de stockage n'est pas compatible, le suivant est interrogé.

Vous pouvez définir la priorité pour les emplacements de stockage suivants :
- **Stockage des unités de disque locales**
- **Utiliser l'hyperviseur imbriqué (adaptateur de support USB ou SD) lorsqu'ESXi est sélectionné**
- **Utiliser l'unité M.2**
- **Utiliser le stockage SAN**

Etape 4. Pour chaque serveur, sélectionnez l'emplacement de stockage préféré sur lequel vous souhaitez déployer l'image du système d'exploitation dans la colonne **Stockage**. Vous pouvez faire votre choix parmi les valeurs suivantes, correspondant aux valeurs de l'étape précédente.
- **Unité de disque locale**
- **Hyperviseur intégré**
- **Unité M.2**
- **Stockage SAN**

Si vous sélectionnez **Stockage SAN**, une boîte de dialogue s'affiche pour configurer le volume SAN. Assurez-vous que le volume SAN cible est accessible pendant le déploiement.

Si l'emplacement de stockage sélectionné n'est pas compatible avec le serveur, Lenovo XClarity Administrator tente de déployer le système d'exploitation sur l'emplacement de stockage qui apparaît ensuite dans l'ordre de priorité défini lors de l'étape précédente.

Déploiement d'une image du système d'exploitation

Vous pouvez utiliser Lenovo XClarity Administrator pour déployer une image du système d'exploitation sur un maximum de 28 serveurs à la fois.

Avant de commencer

Prenez connaissance des remarques relatives au déploiement du système d'exploitation avant de tenter de déployer les systèmes d'exploitation sur vos serveurs gérés (voir Remarques sur le déploiement de systèmes d'exploitation).

Sous l'onglet **Images SE**, vérifiez que l'**État du déploiement** du système d'exploitation que vous voulez déployer est défini sur « Prêt. » Pour déployer le système d'exploitation Windows, un fichier d'amorçage WinPE est requis. Si aucun fichier WinPE correspondant n'est disponible, l'**État du déploiement** est défini

sur « Non prêt » et le système d'exploitation ne peut pas être déployé. Vous devez télécharger et importer un fichier WinPE manuellement (voir Importation de fichiers d'amorçage).

Depuis l'onglet **Gérer les images de SE**, vous pouvez filtrer la liste des images SE en cliquant sur **Afficher tout → État du déploiement**. Vous pouvez filtrer la liste de sorte à n'afficher que les serveur dont l'état est « Prêt, » « Non prêt » et « Avertissement ». Notez que si l'état de déploiement d'une image SE est défini sur « Non prêt, » le système d'exploitation n'est pas inclus dans la liste des systèmes d'exploitation déployables.

L'anglais est pris en charge par défaut. Pour spécifier des paramètres régionaux spécifiques à une langue, vous devez utiliser un fichier de configuration personnalisé et un fichier sans opérateur. Pour plus d'informations, voir Déploiement de SLES 12 SP3 avec des paramètres régionaux configurable et des serveurs NTP, Déploiement de Windows 2016 pour le japonais.

Le déploiement de système d'exploitation sur une unité de stockage non RAID n'est pas pris en charge.

Attention : Si un système d'exploitation est installé sur le serveur, le déploiement d'un profil d'image SE remplacera le système d'exploitation installé.

Pour les serveurs équipés de XCC2 où System Guard est activé et où l'action est définie sur **Empêcher l'amorçage SE**, assurez-vous que System Guard est conforme sur l'appareil. Si System Guard n'est pas conforme, les appareils ne peuvent pas mener à bien le processus d'amorçage, ce qui entraîne l'échec du déploiement du système d'exploitation. Pour provisionner ces appareils, répondez manuellement à l'invite d'amorçage de System Guard afin d'autoriser l'amorçage normal des appareils.

Procédure

Pour déployer une image SE sur un ou plusieurs serveurs gérés, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Déployer des images SE** pour afficher la page Déployer un système d'exploitation : déployer des images SE.

Astuce : Pour les complexes évolutifs, le système d'exploitation est déployé sur la partition principale ; par conséquent, seule cette dernière est incluse dans la liste des serveurs.

Etape 2. Sélectionnez un ou plusieurs serveurs sur lesquels déployer le système d'exploitation. Vous pouvez déployer un système d'exploitation sur un maximum de 28 serveurs à la fois.

Vous pouvez trier les colonnes du tableau afin de faciliter la recherche de serveurs spécifiques. En outre, vous pouvez filtrer la liste des appareils affichés en sélectionnant une option du menu **Afficher** pour afficher uniquement la liste des appareils dans un châssis, armoire ou groupe spécifique, ou en entrant du texte (par exemple, un nom ou une adresse IP) dans la zone **Filtre**.

Astuce : Vous pouvez choisir plusieurs nœuds de traitement à partir de plusieurs châssis si vous souhaitez déployer le même système d'exploitation sur tous les nœuds de traitement.

Etape 3. Cliquez sur **Modifier la sélection → Paramètres réseau** pour configurer les paramètres réseau.

Pour plus d'informations, voir Configuration des paramètres réseau pour les serveurs gérés.

Etape 4. Pour chaque serveur, sélectionnez le profil d'image SE à déployer dans la liste déroulante de la colonne **Image à déployer**.

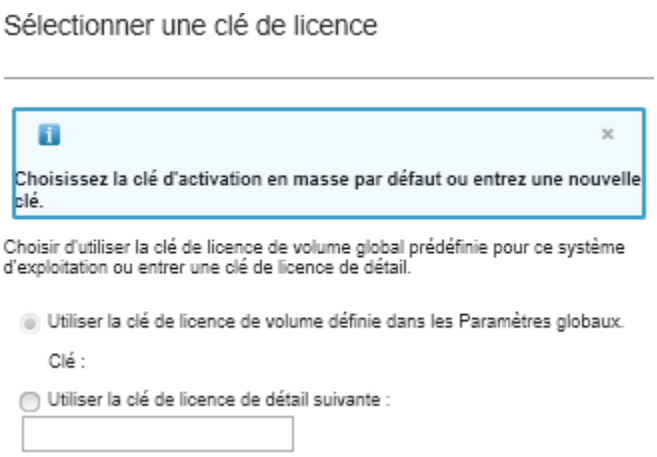
Veillez à sélectionner un profil d'image SE qui est compatible avec le serveur sélectionné. Vous pouvez déterminer la compatibilité à partir des attributs du profil listés dans la colonne **Attribut** de la page Gérer les images de SE. Pour plus d'informations sur les attributs de profil, voir Profils d'image de système d'exploitation.

Etape 5. Pour chaque serveur, cliquez sur l'icône **Clé de licence** (), puis indiquez la clé de licence à utiliser pour activer le système d'exploitation une fois qu'il est installé.

XClarity Administrator prend en charge des clés de licence de volume par défaut pour les installations Windows et des clés de licence de détail individuelles pour Windows et VMware ESXi.

Pour utiliser la clé de licence de volume globale que vous avez spécifiée dans la boîte de dialogue Paramètres globaux, sélectionnez **Utiliser la clé de licence de volume définie dans les Paramètres globaux**. Pour plus d'informations sur les clés de licence de volume globales, voir Configuration des paramètres de déploiement SE.

Pour utiliser une clé de licence de détail individuelle, sélectionnez **Utiliser la clé de licence de détail suivante** et entrez la clé dans la zone suivante.



Etape 6. **Facultatif :** Si vous avez sélectionné un système d'exploitation Windows pour un serveur, vous pouvez associer le système d'exploitation Windows à un domaine Active Directory dans le cadre du déploiement du système d'exploitation en cliquant sur l'icône **Dossier** ( ) affichée en regard de l'image du système d'exploitation, puis en sélectionnant le nom du domaine Active Directory.

Pour utiliser le domaine Active Directory par défaut que vous avez spécifié dans la boîte de dialogue Paramètres globaux, sélectionnez **Utiliser le domaine Active Directory défini dans Paramètres globaux**. Pour plus d'informations sur l'association d'un domaine Active Directory, voir Intégration à Windows Active Directory.

Pour utiliser un domaine Active Directory individuel, sélectionnez **Utiliser le domaine Active Directory suivant** et choisissez le domaine Active Directory.

Etape 7. Pour chaque serveur, sélectionnez l'emplacement de stockage préféré sur lequel vous souhaitez déployer l'image du système d'exploitation dans la colonne **Stockage**.
- **Unité de disque locale**
- **Hyperviseur intégré**
- **Unité M.2**
- **Stockage SAN**

Si l'emplacement de stockage sélectionné n'est pas compatible avec le serveur, XClarity Administrator tente de déployer le système d'exploitation sur l'emplacement de stockage qui apparaît ensuite dans l'ordre de priorité.

Remarque : Pour les serveurs ThinkServer, seule l'option **Disque local** est disponible.

Pour plus d'informations sur la configuration de l'emplacement de stockage, voir Choix de l'emplacement de stockage pour les serveurs gérés.

Remarque : Pour faire en sorte que les déploiements de système d'exploitation aboutissent, déconnectez toutes les unités de stockage du serveur géré, à l'exception de l'unité de stockage qui a été choisie pour le déploiement du système d'exploitation.

Etape 8. Vérifiez que l'état de déploiement de tous les serveurs sélectionnés est Prêt.

Important : Assurez-vous que l'état de déploiement de tous les serveurs sélectionnés est Prêt. Si un serveur est à l'état Non Prêt, vous ne pouvez pas déployer une image du système d'exploitation sur ce serveur. Cliquez sur le lien **Non prêt** pour obtenir des informations qui vous permettront de résoudre le problème. Si les paramètres réseau ne sont pas valides, cliquez sur **Modifier la sélection → Paramètres réseau** pour configurer les paramètres réseau.

Etape 9. Cliquez sur l'icône **Déployer des images** () pour lancer le déploiement du système d'exploitation.

Si les paramètres de configuration personnalisés ont été ajoutés au profil d'image SE, l'onglet **Paramètres personnalisés** s'affiche dans la boîte de dialogue Déployer l'image SE. Indiquez des paramètres personnalisés, des paramètres serveurs communs et des paramètres spécifiques à un serveur, puis cliquez sur **Suivant** pour continuer le déploiement SE. Notez que le déploiement SE ne se poursuivra pas si aucune entrée n'est spécifiée pour les paramètres de configuration personnalisés requis.

Après avoir terminé

Vous pouvez surveiller l'état du processus de déploiement en consultant le journal des travaux. Dans le menu XClarity Administrator, cliquez sur **Surveillance → Travaux**. Pour plus d'informations sur le journal des travaux, voir Surveillance des travaux.

Vous pouvez également configurer une session de contrôle à distance via le contrôleur de gestion de la carte mère du serveur afin de regarder l'installation à mesure qu'elle progresse. Pour plus d'informations sur le contrôle à distance, voir Utilisation du contrôle à distance pour gérer des serveurs Converged, Flex System, NeXtScale et System x.

Les informations de déploiement sont sauvegardées pour le système d'exploitation. Vous pouvez afficher les informations de déploiement en cliquant sur **Distribution → Gérer l'accès SE**, puis en pointant sur le nom du serveur.

Intégration à Windows Active Directory

Lorsque vous déployez une image Windows à l'aide de Lenovo XClarity Administrator, vous pouvez rejoindre un domaine Active Directory dans le cadre du déploiement du système d'exploitation.

Avant de commencer

Pour connecter un domaine Active Directory dans le cadre d'un déploiement d'image Windows, vous devez configurer le serveur de gestion et le serveur Windows qui exécutent le contrôleur de domaine Active Directory affecté. Pour effectuer cette configuration, vous avez besoin de l'accès suivant :

- Un compte administrateur disposant des droits pour authentifier et rejoindre le domaine de serveurs Active Directory. Ce compte doit disposer de privilèges similaires à ceux du groupe d'administrateurs de domaine par défaut, et vous pouvez utiliser un compte dans ce groupe pour cette configuration.
- Accès à un Domain Name System (DNS) qui se résout sur le serveur Active Directory qui exécute le contrôleur de domaine. Ce DNS doit être spécifié dans l'option **Paramètres réseau → DNS** pour le serveur dans lequel vous déployez le système d'exploitation.
- L'administrateur du serveur Active Directory doit créer le nom d'ordinateur requis sur le serveur de domaine avant le déploiement du système d'exploitation. La tentative de connexion ne crée pas de nom d'ordinateur. Si aucun nom n'est spécifié, la connexion échoue.
- L'administrateur du serveur Active Directory doit indiquer le nom d'hôte du serveur sur lequel l'image est déployée en tant que nom d'ordinateur sous l'unité organisationnelle cible en cliquant sur la zone **Paramètres réseau → Nom d'hôte**.

  Le nom d'hôte (nom d'ordinateur) spécifié doit être unique. Spécifier un nom qui est déjà utilisé par une autre installation de Windows a pour effet de faire échouer la connexion.

Vous pouvez joindre le domaine Active Directory en utilisant l'une des méthodes suivantes :

- **Utiliser un domaine Active Directory**

  Vous pouvez choisir d'utiliser un domaine Active Directory spécifique d'une liste de domaines prédéfinis. Procédez comme suit pour définir un domaine Active Directory dans XClarity Administrator. Si vous souhaitez utiliser plusieurs domaines, reprenez ces étapes pour chaque nom de domaine.

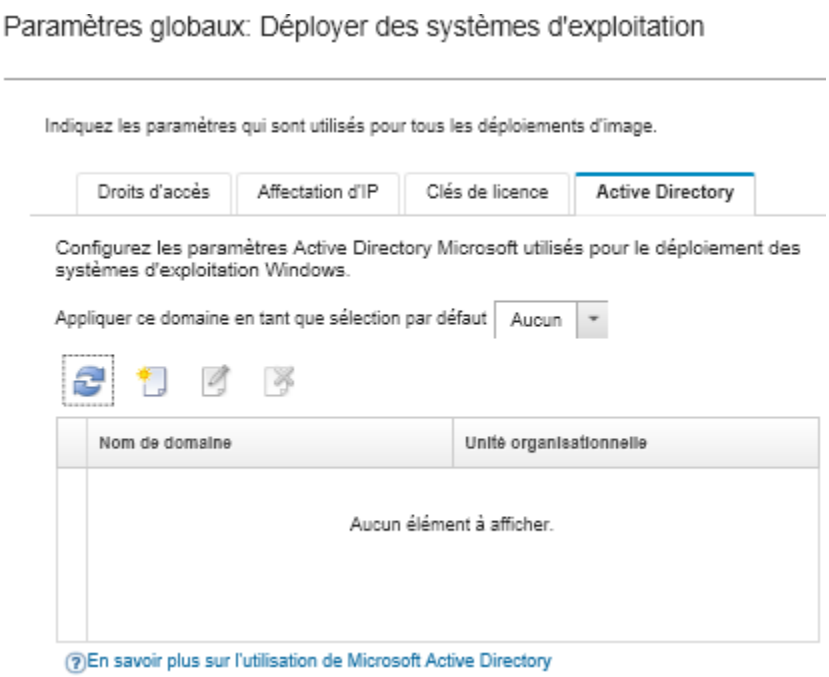
  1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Déployer des images SE** pour afficher la page Déployer des images SE.
  2. Cliquez sur l'icône **Paramètres globaux** ( ) pour afficher la boîte de dialogue Paramètres globaux : Déployer des systèmes d'exploitation.
  3. Cliquez sur l'onglet **Active Directory**.
  4. Cliquez sur l'icône **Créer** ( ) pour afficher la boîte de dialogue Ajouter un nouveau domaine Active Directory.
  5. Indiquez le nom de domaine et l'unité organisationnelle.

     Le déploiement du système d'exploitation prend en charge la connexion d'un domaine et la création d'unités organisationnelles imbriquées dans un domaine. Si vous spécifiez des unités organisationnelles, il n'est pas nécessaire de spécifier le OU dans le cadre de la connexion explicite. Active Directory peut déterminer le OU correct à l'aide du nom de domaine et du nom d'ordinateur.
  6. Cliquez sur **OK**.

- **Utiliser le domaine Active Directory par défaut**

  Vous pouvez choisir d'utiliser le domaine Active Directory par défaut qui est défini dans les paramètres globaux. Procédez comme suit pour définir le domaine Active Directory par défaut dans XClarity Administrator.

  1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Déployer des images SE** pour afficher la page Déployer des images SE.
  2. Cliquez sur l'icône **Paramètres globaux** ( ) pour afficher la boîte de dialogue Paramètres globaux : Déployer des systèmes d'exploitation.
  3. Cliquez sur l'onglet **Active Directory**.



4. Dans le menu déroulant **Appliquer ce domaine en tant que sélection par défaut**, sélectionnez le domaine Active Directory à utiliser par défaut pour chaque déploiement Windows.
5. Cliquez sur **OK**.

- **Utiliser des donnes Blob de métadonnées**

  Vous pouvez utiliser des métadonnées d'ordinateur Active Directory (au format de données Blob codé en Base-64) pour rejoindre le domaine Active Directory d'un serveur. Pour générer les données Blob de métadonnées, procédez comme suit.

  1. Utilisez un compte administrateur pour vous connecter à l'ordinateur. L'ordinateur doit faire partie du domaine Active Directory que vous rejoignez.
  2. Cliquez sur **Démarrer → Programmes → Accessoires**. Cliquez avec le bouton droit de la souris sur **Invite de commande**, puis sélectionnez **Exécuter en tant qu'administrateur**.
  3. Accédez au répertoire C:\windows\system32.
  4. Exécutez la commande `djoin` en utilisant le format suivant pour rejoindre le domaine hors ligne :
     `djoin /provision /domain <AD_domain_name> /machine <hostname> /savefile blob`

     où :

     – *<AD_domain_name>* est le nom du domaine Active Directory.
     – *<hostname>* est le nom d'hôte du serveur sur lequel l'image est déployée en tant que nom d'ordinateur sous l'unité organisationnelle cible en cliquant sur la zone **Paramètres réseau → Nom d'hôte**.

     Cette commande un fichier nommé `blob` qui contient les données Blob de métadonnées. Le contenu de ce fichier est utilisé par le processus de déploiement du système d'exploitation pour indiquer les détails permettant de rejoindre Active Directory ; vous devez donc conserver ces données à proximité.

     Les données Blob de métadonnées sont des données sensibles.

Pour obtenir des informations détaillées sur le déploiement d'une image de système d'exploitation, voir Déploiement d'une image du système d'exploitation.

Procédure

Pour connecter un domaine Active Directory, procédez comme suit.

Etape 1. Importez l'image du système d'exploitation Windows dans le Référentiel d'images SE (voir Importation d'images du système d'exploitation).

Etape 2. Sélectionnez un ou plusieurs serveurs sur lesquels déployer le système d'exploitation. Vous pouvez déployer un système d'exploitation sur un maximum de 28 serveurs à la fois.

Astuce : Vous pouvez choisir plusieurs nœuds de traitement à partir de plusieurs châssis si vous souhaitez déployer le même système d'exploitation sur tous les nœuds de traitement.

Etape 3. Cliquez sur **Modifier la sélection → Paramètres réseau** pour configurer les paramètres réseau.

a. Cliquez sur **Modifier toutes les lignes → Domain Name System (DNS)**, et spécifiez au moins un DNS qui se résout dans le domaine Active Directory.

b. Pour chaque serveur, spécifiez un nom d'hôte correspondant à un nom d'ordinateur existant dans le domaine et l'unité organisationnelle que vous rejoignez.

Pour plus d'informations sur la configuration des paramètres réseau, voir Configuration des paramètres réseau pour les serveurs gérés.

Etape 4. Pour chaque serveur, sélectionnez l'image du système d'exploitation Windows à déployer dans la colonne **Image à déployer**. Une icône de dossier et de clés de licence est affiché en regard du nom de l'image.

Etape 5. Pour chaque serveur, cliquez sur l'icône **Clé de licence** (), puis indiquez la clé de licence à utiliser pour activer le système d'exploitation une fois qu'il est installé.

Etape 6. Pour chaque serveur, cliquez sur l'icône **Dossier** (), puis indiquez le domaine Active Directory. Vous pouvez choisir l'une des valeurs suivantes :

- **Utiliser le domaine Active Directory défini dans Paramètres globaux** pour utiliser le domaine par défaut.
- **Utiliser le domaine Active Directory suivant** pour sélectionner un domaine spécifique.
- **Utiliser des donnes Blob de métadonnées** pour indiquer le contenu du fichier Blob.

  Les données Blob de métadonnées contiennent des informations sensibles et elles ne sont pas affichées dans la zone. Ces informations sont disponibles uniquement jusqu'à la fin de l'opération de déploiement. Elles ne sont pas persistantes.

Etape 7. Pour chaque serveur, sélectionnez l'emplacement de stockage préféré sur lequel vous souhaitez déployer l'image du système d'exploitation dans la colonne **Stockage**.

- **Unité de disque locale**
- **Hyperviseur intégré**
- **Unité M.2**
- **Stockage SAN**

Si l'emplacement de stockage sélectionné n'est pas compatible avec le serveur, XClarity Administrator tente de déployer le système d'exploitation sur l'emplacement de stockage qui apparaît ensuite dans l'ordre de priorité.

Pour plus d'informations sur la configuration de l'emplacement de stockage, voir Choix de l'emplacement de stockage pour les serveurs gérés.

Remarque : Pour faire en sorte que les déploiements de système d'exploitation aboutissent, déconnectez toutes les unités de stockage du serveur géré, à l'exception de l'unité de stockage qui a été choisie pour le déploiement du système d'exploitation.

Etape 8. Vérifiez que l'état de déploiement de tous les serveurs sélectionnés est Prêt.

Si un serveur est à l'état Non Prêt, vous ne pouvez pas déployer une image du système d'exploitation sur ce serveur. Cliquez sur le lien **Non prêt** pour obtenir des informations qui vous permettront de résoudre le problème. Si les paramètres réseau ne sont pas valides, cliquez sur **Modifier la sélection → Paramètres réseau** pour configurer les paramètres réseau.

Etape 9. Cliquez sur l'icône **Déployer des images** () pour lancer le déploiement du système d'exploitation.

La boîte de dialogue Confirmation de déploiement vous invite à saisir les données d'identification à utiliser sur le serveur Active Directory et à rejoindre le domaine. Pour des raisons de sécurité, ces données d'identification ne sont pas enregistrées dans XClarity Administrator. Vous devez soumettre les données d'identification pour chaque déploiement Windows qui rejoint le domaine.

Vous pouvez surveiller l'état du processus de déploiement en consultant le journal des travaux. Dans le menu XClarity Administrator, cliquez sur **Surveillance → Travaux**. Pour plus d'informations sur le journal des travaux, voir Surveillance des travaux.

Résultats

Lorsque le déploiement du système d'exploitation est terminé, ouvrez un navigateur Web sur l'adresse IP que vous avez spécifiée sur la page Éditer les paramètres réseau, puis connectez-vous pour continuer le processus de configuration.

Scénarios de déploiement SE

Utilisez ces scénarios pour vous aider à personnaliser et à déployer des systèmes d'exploitation sur des serveurs gérés.

Déploiement RHEL avec des pilotes de périphérique personnalisés

Ce scénario installe le système d'exploitation Red Hat Enterprise Linux (RHEL) et des pilotes de périphérique supplémentaires qui ne sont pas disponibles dans le système d'exploitation de base. Un profil personnalisé comprenant les pilotes de périphérique supplémentaires est utilisé. Ce profil personnalisé peut ensuite être sélectionné sur la page Déployer des images de SE.

Avant de commencer

Lorsque vous déployez des systèmes d'exploitation à l'aide de Lenovo XClarity Administrator, le système d'exploitation doit inclure les pilotes de périphérique Ethernet, Fibre Channel et d'adaptateur de stockage appropriés pour votre matériel. Si un pilote de périphérique n'est pas inclus dans le système d'exploitation, l'adaptateur n'est pas pris en charge lors du déploiement du système d'exploitation. Dans XClarity Administrator v1.2.0 et ultérieure, vous pouvez personnaliser un système d'exploitation en ajoutant des pilotes de périphérique.

Vous pouvez obtenir des pilotes de périphérique auprès de Page Web du référentiel YUM Lenovo, du fournisseur (par exemple, Red Hat) ou par le biais d'un pilote de périphérique personnalisé que vous générez vous-même. Pour certains pilotes de périphérique Windows, vous pouvez générer un pilote de périphérique personnalisé en extrayant le pilote de périphérique de l'exécutable d'installation sur votre système local et en créant un fichier d'archive .zip.

Remarque : Les pilotes de périphérique RHEL doivent se trouver dans .iso ou .rpm.

Procédure

Pour déployer RHEL avec des pilotes de périphérique personnalisés, procédez comme suit.

Etape 1. Téléchargez le système d'exploitation RHEL de base à partir du site Web Red Hat sur le système local, puis importez l'image dans le référentiel d'images SE. Pour plus d'informations, voir Importation d'images du système d'exploitation.

1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Gérer les images de SE** pour afficher la page Déployer un système d'exploitation : déployer des images de SE.
2. Cliquez sur l'onglet **Images SE**.
3. Cliquez sur l'icône **Importer** ( ).
4. Cliquez sur **Importation locale**.
5. Cliquez sur **Parcourir** pour rechercher et sélectionner l'image RHEL à importer (par exemple, `RHEL-<ver>-<date>-Server-x86_64-dvd1.iso`).
6. Cliquez sur **Importer** pour charger l'image dans le référentiel des images SE.
7. Attendez la fin de l'importation. Cette opération peut prendre un certain temps.

Etape 2. Téléchargez les pilotes de périphérique personnalisés sur le système local et importez les fichiers dans le référentiel d'images SE. Pour plus d'informations, voir Importation de pilotes de périphérique.

1. Cliquez sur l'onglet **Pilotes de périphérique**.
2. Cliquez sur l'icône **Importer** ( ).
3. Cliquez sur **Importation locale**.
4. Sélectionnez `RHEL` comme système d'exploitation.
5. Sélectionnez la version du système d'exploitation.
6. Sélectionnez le type d'appareil.
7. Cliquez sur **Parcourir** pour rechercher et sélectionner le pilote de périphérique à importer (par exemple, `kmod-i40e-2.0.12-1.el7.x86_64.rpm`).
8. Cliquez sur **Importer** pour charger le fichier dans le référentiel des images SE.

Etape 3. Créez un profil d'image SE personnalisé qui inclut les pilotes de périphérique personnalisés. Pour plus d'informations, voir Création d'un profil d'image SE personnalisé.

1. Cliquez sur l'onglet **Images SE**.
2. Sélectionnez un profil d'image SE à personnaliser (par exemple, `Virtualization`).
3. Cliquez sur l'icône **Créer** ( ) pour afficher la boîte de dialogue Créer un profil personnalisé.
4. Sur l'onglet **Général** :
   a. Entrez un nom pour le profil (par exemple, `Custom RHEL with device drivers`).
   b. Utilisez la valeur par défaut pour la zone **Chemin d'accès des données et des fichiers personnalisés**.
   c. Sélectionnez **Aucun** comme type de personnalisation.

d. Cliquez sur **Suivant**.

5. Sous l'onglet **Options de pilote**, sélectionnez les pilotes de périphérique personnalisés à inclure dans le profil, puis cliquez sur **Suivant**. Les pilotes d'appareil fournis par Windows sont inclus par défaut.
6. Sous l'onglet **Software**, cliquez sur **Suivant**.
7. Cliquez sur **Personnaliser** pour créer le profil d'image SE personnalisé.

Etape 4. Déployez le profil d'image SE personnalisé sur les serveurs cible. Pour plus d'informations, voir Déploiement d'une image du système d'exploitation.

1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Déployer des images SE** pour afficher la page Déployer un système d'exploitation : déployer des images SE.
2. Pour chacun des serveurs cible :
   a. Sélectionnez le serveur.
   b. Cliquez sur **Modifier la sélection → Paramètres réseau**, puis indiquez le nom d'hôte, l'adresse IP, les paramètres DNS, MTU et VLAN pour le serveur.

      Astuce : Les paramètres VLAN sont disponibles uniquement lorsque le mode VLAN est défini dans **Paramètres globaux → Affectation d'IP → Utiliser les réseaux VLAN**.
   c. Sélectionnez le profil d'image SE personnalisé (par exemple, *<base_OS>*|*<timestamp>*_`Custom RHEL with device drivers`) dans la liste déroulante de la colonne **Image à déployer**.

      Remarque : Vérifiez que tous les serveurs cible utilisent le même profil personnalisé.
   d. (Facultatif) Cliquez sur l'icône **Clé de licence** ( ) et indiquez la clé de licence à utiliser pour activer le système d'exploitation une fois qu'il est installé.
   e. Sélectionnez l'emplacement de stockage préféré sur lequel vous souhaitez déployer l'image du système d'exploitation dans la colonne **Stockage**.

      Remarque : Pour faire en sorte que les déploiements de système d'exploitation aboutissent, déconnectez toutes les unités de stockage du serveur géré, à l'exception de l'unité de stockage qui a été choisie pour le déploiement du système d'exploitation.
   f. Vérifiez que l'état de déploiement du serveur sélectionné est **Prêt**.
3. Sélectionnez tous les serveurs cible, puis cliquez sur l'icône **Déployer l'image** ( ) pour lancer le déploiement du système d'exploitation.
4. Sous l'onglet **Récapitulatif**, passez les paramètres en revue.
5. Cliquez sur **Déployer** pour déployer le système d'exploitation.

Déploiement de RHEL et d'une application PHP Hello World à l'aide d'un fichier sans opérateur personnalisé

Ce scénario installe le système d'exploitation RHEL ainsi que des logiciels personnalisés (Apache HTTP, PHP et une application de PHP hello world). Un profil d'image SE personnalisé est utilisé et il contient le fichier sans opérateur personnalisé qui enregistre le système d'exploitation auprès du service de souscription RHEL Lenovo interne de sorte qu'il puisse utiliser les référentiels yum ; installes les modules Apache et PHP, configure le pare-feu afin d'autoriser Les connexions Apache, crée une application PHP Hello World et copies dans le répertoire de serveur web Apache et configure les fichiers de configuration Apache pour la prise en charge de PHP.

Avant de commencer

Vous pouvez déployer RHEL avec des logiciels personnalisés de plusieurs manières différentes. Cet exemple utilise un fichier sans opérateur personnalisé que vous incluez dans le profil d'image SE personnalisé. Vous pouvez également utiliser le script de post-installation qui installe un logiciel personnalisé que vous importez dans le référentiel et incluez dans le profil d'image SE personnalisé. Pour installer des logiciels à l'aide d'un script de post-installation, voir Déploiement de RHEL et d'une application PHP Hello World utilisant un logiciel personnalisé et un script de post-installation.

Ce scénario utilise les modèles de fichier suivants.

- RHEL_installSoftware_customUnattend.cfg Ce fichier sans opérateur personnalisé utilise des valeurs dans des macros prédéfinies et personnalisées et installe et configure les logiciels personnalisés.

Procédure

Pour déployer RHEL avec des logiciels personnalisés à l'aide d'un fichier sans opérateur personnalisé, procédez comme suit.

Etape 1. Téléchargez le système d'exploitation RHEL de base à partir du site Web Red Hat sur le système local, puis importez l'image dans le référentiel d'images SE. Pour plus d'informations, voir Importation d'images du système d'exploitation.

1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Gérer les images de SE** pour afficher la page Déployer un système d'exploitation : déployer des images de SE.
2. Cliquez sur l'onglet **Images SE**.
3. Cliquez sur l'icône **Importer** ().
4. Cliquez sur **Importation locale**.
5. Cliquez sur **Parcourir** pour rechercher et sélectionner l'image RHEL à importer (par exemple, `RHEL-<ver>-<date>-Server-x86_64-dvd1.iso`).
6. Cliquez sur **Importer** pour charger l'image dans le référentiel des images SE.
7. Attendez la fin de l'importation. Cette opération peut prendre un certain temps.

Etape 2. Modifiez le fichier sans opérateur RHEL (kickstart) pour enregistrer les systèmes d'exploitation avec vote service d'abonnement satellite RHEL, installez les modules HTTP (Apache) et PHP, puis créez une simple application PHP Hello World, ajoutez les macros prédéfinies requises et d'autres macros prédéfinies si nécessaire, comme l'adresse IP, la passerelle, les paramètres DNS et nom d'hôte, puis importez le fichier personnalisé dans le répertoire d'images SE. Pour plus d'informations, voir Importation de fichiers sans opérateur personnalisés.

Ajoutez les commandes permettant d'enregistrer l'hôte auprès de votre satellite RHEL, par exemple :

```
rpm -Uvh http://<YOUR_SATELLITE_SERVER_IP>/pub/katello-ca-consumer-latest.noarch.rpm
subscription-manager register --org="<YOUR_ORGANIZATION>" --activationkey="RHEL_Base" --force
subscription-manager repos --enable rhel-7-server-rpms
```

Important : Dans l'exemple de fichier sans opérateur, indiquez l'adresse IP de votre serveur satellite et de votre organisation en fonction de la configuration de votre service de souscription.

Ajoutez les commandes permettant de mettre à jour l'hôte et d'installer et de configurer des modules apache et php, par exemple :

```
%packages
@base
@core
@fonts
@gnome-desktop
@internet-browser
```

```
@multimedia
@x11
@print-client
-gnome-initial-setup

#Add the Apache and PHP packages
httpd
mod_ssl
openssl
php
php-mysql
php-gd
%end

yum -y update

systemctl enable httpd.service

firewall-cmd --permanent --zone=public --add-service=http
firewall-cmd --permanent --zone=public --add-service=https
firewall-cmd --reload

echo "<?PHP
echo 'Hello World !! ';
?>" | tee /var/www/html/index.php

sudo cp /etc/httpd/conf/httpd.conf /etc/httpd/conf/httpd.conf.original

sudo sed -i -e 's/^[ \t]*//' /etc/httpd/conf/httpd.conf
sudo sed -i "s|IncludeOptional|#IncludeOptional|" /etc/httpd/conf/httpd.conf
sudo sed -i "s|#ServerName www.example.com:80|ServerName localhost|" /etc/httpd/conf/httpd.conf
sudo sed -i "s|DirectoryIndex index.html|DirectoryIndex index.html index.php|" /etc/httpd/conf/httpd.conf

echo "AddType application/x-httpd-php .php" | tee -a /etc/httpd/conf/httpd.conf
```

Remarque : L'exemple de fichier sans opérateur modifie les modules par défaut installés avec le fichier kickstart. Il indique les modules Apache et PHO dans le cadre de la section %packages.

Pour ESXi et RHEL uniquement, XClarity Administrator fournit la macro **#predefined.unattendSettings.networkConfig#**, qui ajoute tous les paramètres réseau qui sont définis dans l'interface utilisateur dans le fichier sans opérateur, ainsi que la macro **#predefined.unattendSettings.storageConfig#**, qui ajoute tous les paramètres de stockage qui sont définis dans l'interface utilisateur dans le fichier sans opérateur. L'exemple de fichier sans opérateur contient déjà ces macros.

XClarity Administrator fournit également certaines macros de base, par exemple l'injection de pilotes OOB, la génération de rapports d'état, des scripts de post-installation, ainsi que des logiciels personnalisés. Toutefois, pour tirer parti de ces macros prédéfinies, vous devez spécifier les macros suivantes dans le fichier sans opérateur personnalisé. Le fichier exemple contient déjà les macros requises.

```
#predefined.unattendSettings.preinstallConfig#
#predefined.unattendSettings.postinstallConfig#
```

Le modèle de fichier contient déjà les macros nécessaires et les macros prédéfinies supplémentaires pour l'indication en mode dynamique des paramètres réseau pour le serveur cible et le fuseau horaire. Pour plus d'informations sur l'ajout de macros dans les fichiers sans opérateur, voir Injection de macros prédéfinies et de macros personnalisées dans un fichier sans opérateur.

Vous pouvez également ajouter des commandes pour envoyer des messages personnalisés aux travaux qui se connectent dans XClarity Administrator. Pour plus d'informations, voir Ajout de rapport d'état personnalisé aux scripts d'installation.

Pour importer le script d'installation personnalisé, procédez comme suit. Pour plus d'informations, voir Importation de scripts d'installation personnalisés.

Pour importer le fichier sans opérateur personnalisé, procédez comme suit.

1. Cliquez sur l'onglet **Fichiers sans opérateur**.
2. Cliquez sur l'icône **Importer** ().
3. Cliquez sur **Importation locale**.
4. Sélectionnez `RHEL` comme système d'exploitation.
5. Cliquez sur **Parcourir** pour rechercher et sélectionner le fichier à importer (par exemple, `RHEL_installSoftware_customUnattend.cfg`).
6. Cliquez sur **Importer** pour charger le fichier dans le référentiel des images SE.

Etape 3. Créez un profil d'image SE personnalisé qui inclut le logiciel personnalisé et le script de post-installation. Pour plus d'informations, voir Création d'un profil d'image SE personnalisé.

1. Cliquez sur l'onglet **Images SE**.
2. Sélectionnez un profil d'image SE à personnaliser (par exemple, `Basic`).
3. Cliquez sur l'icône **Créer** () pour afficher la boîte de dialogue Créer un profil personnalisé.
4. Sur l'onglet **Général** :
   a. Entrez un nom pour le profil (par exemple, `RHEL personnalisé avec logiciels utilisant un fichier sans opérateur`).
   b. Utilisez la valeur par défaut pour la zone **Chemin d'accès des données et des fichiers personnalisés**.
   c. Sélectionnez **Fichiers sans opérateur uniquement** comme type de personnalisation.
   d. Cliquez sur **Suivant**.
5. Sous l'onglet **Options de pilote**, cliquez sur **Suivant** . Les pilotes d'appareil fournis par Windows sont inclus par défaut.
6. Sous l'onglet **Software**, cliquez sur **Suivant**.
7. Sous l'onglet **Fichiers sans opérateur**, sélectionnez des fichiers personnalisés (par exemple, `RHEL_installSoftware_customUnattend.cfg`), puis cliquez sur **Suivant**.
8. Sous l'onglet **Scripts d'installation**, cliquez sur **Suivant**.
9. Sous l'onglet **Récapitulatif**, passez les paramètres en revue.
10. Cliquez sur **Personnaliser** pour créer le profil d'image SE personnalisé.

Etape 4. Déployez le profil d'image SE personnalisé sur les serveurs cible. Pour plus d'informations, voir Déploiement d'une image du système d'exploitation.

1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Déployer des images SE** pour afficher la page Déployer un système d'exploitation : déployer des images SE.
2. Pour chacun des serveurs cible :
   a. Sélectionnez le serveur.
   b. Cliquez sur **Modifier la sélection → Paramètres réseau**, puis indiquez le nom d'hôte, l'adresse IP, les paramètres DNS, MTU et VLAN pour le serveur.

      Astuce :

- Les paramètres VLAN sont disponibles uniquement lorsque le mode VLAN est défini dans **Paramètres globaux → Affectation d'IP → Utiliser les réseaux VLAN**.
- Les paramètres réseau que vous spécifiez dans la boîte de dialogue Paramètres réseau sont ajoutés au fichier sans opérateur au moment de l'exécution à l'aide des macros **#predefined.hostPlatforms.networkSettings.<*setting*>#**.

c. Sélectionnez le profil d'image SE personnalisé (par exemple, <*base_OS*>|<*timestamp*>_`RHEL personnalisé avec logiciels utilisant un fichier sans opérateur`) dans la liste déroulante de la colonne **Image à déployer**

Remarque : Vérifiez que tous les serveurs cible utilisent le même profil personnalisé.

d. (Facultatif) Cliquez sur l'icône **Clé de licence** ( ) et indiquez la clé de licence à utiliser pour activer le système d'exploitation une fois qu'il est installé.

e. Sélectionnez l'emplacement de stockage préféré sur lequel vous souhaitez déployer l'image du système d'exploitation dans la colonne **Stockage**.

Remarque : Pour faire en sorte que les déploiements de système d'exploitation aboutissent, déconnectez toutes les unités de stockage du serveur géré, à l'exception de l'unité de stockage qui a été choisie pour le déploiement du système d'exploitation.

f. Vérifiez que l'état de déploiement du serveur sélectionné est **Prêt**.

3. Sélectionnez tous les serveurs cible, puis cliquez sur l'icône **Déployer l'image** ( ) pour lancer le déploiement du système d'exploitation.
4. Sous l'onglet Paramètres personnalisés, cliquez sur le sous-onglet **Paramètres de configuration et sans opérateur**, puis sélectionnez le fichier sans opérateur personnalisé (par exemple, `RHEL_installSoftware_customUnattend.cfg`).

5. Sous l'onglet **Récapitulatif**, passez les paramètres en revue.
6. Cliquez sur **Déployer** pour déployer le système d'exploitation.

Déploiement de RHEL et d'une application PHP Hello World utilisant un logiciel personnalisé et un script de post-installation

Ce scénario installe le système d'exploitation RHEL ainsi que des logiciels personnalisés (Apache HTTP, PHP et une application de PHP hello world). Un profil d'image SE personnalisé est utilisé et il contient le logiciel personnalisé et un script de post-installation qui enregistre le système d'exploitation auprès du service de souscription RHEL Lenovo interne de sorte qu'il puisse utiliser les référentiels yum ; installes les modules Apache et PHP, configure le pare-feu afin d'autoriser Les connexions Apache, crée une application PHP Hello World et copies dans le répertoire de serveur web Apache et configure les fichiers de configuration Apache pour la prise en charge de PHP. Les modules logiciels personnalisés sont exportés sur l'hôte lors du déploiement, puis mis à disposition pour le script de post-installation personnalisé.

Avant de commencer

Vous pouvez déployer RHEL et une application PHP Hello World de différentes manières. Cet exemple utilise un script de post-installation qui installe un logiciel personnalisé que vous importez dans le référentiel et incluez dans le profil d'image SE personnalisé. Vous pouvez aussi utiliser un fichier sans opérateur personnalisé que vous incluez dans le profil d'image SE personnalisé. Pour l'installation du logiciel à l'aide d'un fichier sans opérateur personnalisés, voir Déploiement de RHEL et d'une application PHP Hello World à l'aide d'un fichier sans opérateur personnalisé.

Ce scénario utilise les modèles de fichiers suivants.

- httpd.conf. Il s'agit du fichier d'installation pour Apache HTTP.
- hello_world.php Il s'agit de l'application PHP Hello World.
- RHEL_installSoftware_customScript.sh Ce script de post-installation installe et configure le logiciel personnalisé.

Remarques :

- Les scripts d'installation RHEL se présentent sous l'un des formats suivants : Bash (.sh), Perl (.pm ou .pl), Python (.py)
- Les fichiers logiciels et les scripts d'installation sont installés à partir du chemin de données et de fichiers personnalisé que vous spécifiez lors du déploiement. Le chemin d'accès aux fichiers et données personnalisés par défaut est `/home/lxca`.

Procédure

Pour déployer RHEL avec un logiciel personnalisé utilisant un script de post-installation, procédez comme suit.

Etape 1. Téléchargez le système d'exploitation RHEL de base à partir du site Web Red Hat sur le système local, puis importez l'image dans le référentiel d'images SE. Pour plus d'informations, voir Importation d'images du système d'exploitation.

1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Gérer les images de SE** pour afficher la page Déployer un système d'exploitation : déployer des images de SE.
2. Cliquez sur l'onglet **Images SE**.
3. Cliquez sur l'icône **Importer** ().
4. Cliquez sur **Importation locale**.
5. Cliquez sur **Parcourir** pour rechercher et sélectionner l'image RHEL à importer (par exemple, `RHEL-<ver>-<date>-Server-x86_64-dvd1.iso`).
6. Cliquez sur **Importer** pour charger l'image dans le référentiel des images SE.
7. Attendez la fin de l'importation. Cette opération peut prendre un certain temps.

Etape 2. Téléchargez le logiciel personnalisé sur le système local et importez les fichiers dans le référentiel d'images SE. Pour plus d'informations, voir Importation de logiciels personnalisés.

Conseil : Pour importer des logiciels personnalisés dans XClarity Administrator, les fichiers doivent être contenus dans un fichier tar.gz. Dans cet exemple, comprimez les fichiers logiciels en exemple `httpd.conf` et `index.php` dans un fichier tar.gz nommé `RHEL_installSoftware_customsw.tar.gz` avant de continuer

1. Cliquez sur l'onglet **Logiciels**.
2. Cliquez sur l'icône **Importer** ().
3. Cliquez sur **Importation locale**.
4. Sélectionnez `RHEL` comme système d'exploitation.
5. Cliquez sur **Parcourir** pour rechercher et sélectionner le fichier à importer (par exemple, `RHEL_installSoftware_customsw.tar.gz`).
6. Cliquez sur **Importer** pour charger le fichier dans le référentiel des images SE.

Etape 3. Créez un script de post-installation personnalisé et importez le fichier dans le référentiel d'images SE.

Ajout de commandes permettant d'enregistrer l'hôte auprès du satellite RHEL, par exemple :

```
rpm -Uvh http://satellite.labs.lenovo.com/pub/katello-ca-consumer-latest.noarch.rpm
subscription-manager register --org="Default_Organization" --activationkey="RHEL_Base" --force
subscription-manager repos --enable rhel-7-server-rpms A
```

Ajout d'une commande permettant de mettre à jour l'hôte et d'installer et de configurer des modules apache et php, par exemple :

```
yum -y update
yum -y install httpd mod_ssl openssl php php-mysql php-gd

systemctl enable httpd.service

firewall-cmd --permanent --zone=public --add-service=http
firewall-cmd --permanent --zone=public --add-service=https
firewall-cmd --reload
```

Ajout de commandes permettant d'ajouter notre application PHP à serversatellite web, par exemple :

```
cp #predefined.otherSettings.deployDataAndSoftwareLocation#/lxca/index.php /var/www/html/index.php
```

Ajout de commandes permettant de configurer Apache HTTP, par exemple :

```
cp /etc/httpd/conf/httpd.conf /etc/httpd/conf/httpd.conf.original
cp #predefined.otherSettings.deployDataAndSoftwareLocation#/httpd.conf /etc/httpd/conf/httpd.conf
```

Notez que ces commandes utilisent des macro prédéfinies pour le chemin d'accès aux fichiers de données et logiciels extraits (**predefined.otherSettings.deployDataAndSoftwareLocation**).

Vous pouvez également ajouter des commandes pour envoyer des messages personnalisés aux travaux qui se connectent dans XClarity Administrator. Pour plus d'informations, voir Ajout de rapport d'état personnalisé aux scripts d'installation.

Pour importer le script d'installation personnalisé, procédez comme suit. Pour plus d'informations, voir Importation de scripts d'installation personnalisés.

1. Cliquez sur l'onglet **Scripts d'installation**.
2. Cliquez sur l'icône **Importer** ().

3. Cliquez sur **Importation locale**.
4. Sélectionnez `RHEL` comme système d'exploitation.
5. Cliquez sur **Parcourir** pour rechercher et sélectionner le script de post-installation à importer (par exemple, `RHEL_installSoftware_customScript.sh`).
6. Cliquez sur **Importer** pour charger le fichier dans le référentiel des images SE.

Etape 4. Créez un profil d'image SE personnalisé qui inclut le logiciel personnalisé et le script de post-installation. Pour plus d'informations, voir Création d'un profil d'image SE personnalisé.

1. Cliquez sur l'onglet **Images SE**.
2. Sélectionnez un profil d'image SE à personnaliser (par exemple, `Basic`).
3. Cliquez sur l'icône **Créer** () pour afficher la boîte de dialogue Créer un profil personnalisé.
4. Sur l'onglet **Général** :
   a. Entrez un nom pour le profil (par exemple, `RHEL personnalisé avec logiciels utilisant un script de post-installation`).
   b. Utilisez la valeur par défaut pour la zone **Chemin d'accès des données et des fichiers personnalisés**.
   c. Sélectionnez **Aucun** comme type de personnalisation.
   d. Cliquez sur **Suivant**.
5. Sous l'onglet **Options de pilote**, cliquez sur **Suivant** . Les pilotes d'appareil fournis par Windows sont inclus par défaut.
6. Sous l'onglet **Logiciels**, sélectionnez les fichiers d'installation des logiciels (par exemple, `httpd.conf` et `index.php`), puis cliquez sur **Suivant**.
7. Sous l'onglet **Scripts d'installation**, sélectionnez les scripts d'installation (par exemple, `RHEL_installSoftware_customScript.sh`), puis cliquez sur **Suivant**.
8. Sous l'onglet **Récapitulatif**, passez les paramètres en revue.
9. Cliquez sur **Personnaliser** pour créer le profil d'image SE personnalisé.

Etape 5. Déployez le profil d'image SE personnalisé sur les serveurs cible. Pour plus d'informations, voir Déploiement d'une image du système d'exploitation.

1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Déployer des images SE** pour afficher la page Déployer un système d'exploitation : déployer des images SE.
2. Pour chacun des serveurs cible :
   a. Sélectionnez le serveur.
   b. Cliquez sur **Modifier la sélection → Paramètres réseau**, puis indiquez le nom d'hôte, l'adresse IP, les paramètres DNS, MTU et VLAN pour le serveur.

      Astuce : Les paramètres VLAN sont disponibles uniquement lorsque le mode VLAN est défini dans **Paramètres globaux → Affectation d'IP → Utiliser les réseaux VLAN**.
   c. Sélectionnez le profil d'image SE personnalisé (par exemple, *<base_OS>*|*<timestamp>*_`RHEL personnalisé avec logiciels utilisant un script de post-installation`) dans la liste déroulante de la colonne **Image à déployer**.

      Remarque : Vérifiez que tous les serveurs cible utilisent le même profil personnalisé.
   d. Sélectionnez l'emplacement de stockage préféré sur lequel vous souhaitez déployer l'image du système d'exploitation dans la colonne **Stockage**.

      Remarque : Pour faire en sorte que les déploiements de système d'exploitation aboutissent, déconnectez toutes les unités de stockage du serveur géré, à l'exception de l'unité de stockage qui a été choisie pour le déploiement du système d'exploitation.

e. Vérifiez que l'état de déploiement du serveur sélectionné est **Prêt**.

3. Sélectionnez tous les serveurs cible, puis cliquez sur l'icône **Déployer l'image** () pour lancer le déploiement du système d'exploitation.
4. Sous l'onglet **Récapitulatif**, passez les paramètres en revue.
5. Cliquez sur **Déployer** pour déployer le système d'exploitation.

Déploiement de SLES 12 SP3 avec des modules personnalisés et un fuseau horaire

Ce scénario installe le système d'exploitation SLES 12 SP3 (en anglais) et plusieurs modules SLES en option. Il demande également de définir le fuseau horaire. Un profil personnalisé d'image SE y est utilisé. Il comprend un fichier de configuration personnalisé et un fichier sans opérateur. Ce profil personnalisé peut être sélectionné sur la page Déployer des images de SE. Ensuite, vous pouvez sélectionner les modules SLE que vous souhaitez déployer et spécifier le fuseau horaire, sous l'onglet **Paramètres personnalisés**. Les valeurs sélectionnées sont remplacées dans les macros personnalisées du fichier sans opérateur personnalisé et le programme d'installation autoyast SLES utilise ces valeurs dans le fichier sans opérateur pour configurer le système d'exploitation.

Avant de commencer

Ce scénario utilise les modèles de fichiers suivants.

- SLES_installPackages_customConfig.json. Ce fichier de configuration invite à définir le fuseau horaire et les modules SLES en option (Linux, Apache, MySQL, module logiciel PHP, module de serveur de messagerie SLES et module de serveur de fichiers SLES) à installer.
- SLES_installPackages_customUnattend.xml Ce fichier sans opérateur utilise les valeurs des macros prédéfinies et personnalisées qui sont définies dans le fichier de configuration.

Procédure

Pour déployer SLES 12 SP3 sur des serveurs à l'aide d'un profil d'image SE personnalisé, procédez comme suit.

Etape 1. Téléchargez le système d'exploitation SLES de base à partir du site web SUSE sur le système local, puis importez l'image dans le référentiel d'images SE. Pour plus d'informations, voir Importation d'images du système d'exploitation.

1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Gérer les images de SE** pour afficher la page Déployer un système d'exploitation : déployer des images de SE.
2. Cliquez sur l'onglet **Images SE**.
3. Cliquez sur l'icône **Importer** ().
4. Cliquez sur **Importation locale**.
5. Cliquez sur **Parcourir** pour rechercher et sélectionner l'image SLES 12 SP3 à importer (par exemple, `SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso`).
6. Cliquez sur **Importer** pour charger l'image dans le référentiel des images SE.
7. Attendez la fin de l'importation. Cette opération peut prendre un certain temps.

Etape 2. Créer un fichier de paramètres de configuration personnalisé et importez-le dans le référentiel d'images SE.

Le fichier de paramètres de configuration est un fichier JSON qui décrit les données à collecter dynamiquement pendant le processus de déploiement SE. Dans le cadre de ce scénario, nous souhaitons spécifier les modules SLES en option qui peuvent être installés (notamment SLES

Linux, Apache, MySQL, module logiciel PHP, module de serveur de messagerie SLES et module de serveur de fichiers SLES) et un fuseau horaire à utiliser pour chaque déploiement SE. Pour plus d'informations sur la création d'un fichier de paramètres de configuration, voir Macros personnalisées.

Pour importer le fichier de paramètres de configuration, procédez comme suit. Pour plus d'informations, voir Importation de paramètres de configuration personnalisés.

1. Cliquez sur l'onglet **Fichiers de configuration**.
2. Cliquez sur l'icône **Importer** ().
3. Cliquez sur **Importation locale**.
4. Sélectionnez `SLES` comme système d'exploitation.
5. Cliquez sur **Parcourir** pour rechercher et sélectionner le fichier de paramètres de configuration à importer (par exemple, `SLES_installPackages_customConfig.json`).
6. Cliquez sur **Importer** pour charger le fichier dans le référentiel des images SE.

   Remarque : Lorsque vous importez un fichier de paramètres de configuration personnalisé, XClarity Administratorgénère des macros personnalisées pour chaque paramètre du fichier. Vous pouvez ajouter ces macros au fichier sans opérateur. Pendant le déploiement SE, les macros sont remplacées par des valeurs réelles.

Etape 3. Modifiez le fichier sans opérateur SLES pour spécifier des valeurs dynamiques pour les modules SLES en option et le fuseau horaire, puis importez le fichier personnalisé dans le référentiel d'images SE. Pour plus d'informations, voir Importation de fichiers sans opérateur personnalisés.

Dans la section **<general>**, ajoutez les informations de fuseau horaire, par exemple :

```
<timezone>
   <hwclock></hwclock>
   <timezone></timezone>
</timezone>
```

Dans la section **<patterns>**, ajoutez trois balises de modèle. Ces balises seront utilisées pour les macros personnalisées pour les paramètres de module SLES en option, par exemple :

```
<patterns config:type="list">
   <pattern>32bit</pattern>
   <pattern>Basis-Devel</pattern>
   <pattern>Minimal</pattern>
   <pattern>WBEM</pattern>
   <pattern>apparmor</pattern>
   <pattern>base</pattern>
   <pattern>documentation</pattern>
   <pattern>fips</pattern>
   <pattern>gateway_server</pattern>
   <pattern>ofed</pattern>
   <pattern>printing</pattern>
   <pattern>sap_server</pattern>
   <pattern>x11</pattern>
   <pattern></pattern>
   <pattern></pattern>
   <pattern></pattern>
</patterns>
```

Remarques :

- Ces balises sont dans l'exemple de fichier sans opérateur.
- Lorsque vous utilisez un fichier sans opérateur personnalisé, XClarity Administrator n'offre pas la plupart des fonctionnalités normales dont vous bénéficiez lorsque vous utilisez un fichier sans

opérateur prédéfini. Par exemple, les cibles **<DiskConfiguration>**, **<ImageInstall>**, **<ProductKey>** et **<UserAccounts>** pour l'administrateur, **<Interfaces>** pour les réseaux et la liste **<package>** pour les fonctionnalités d'installation doivent être spécifiées dans le fichier sans opérateur personnalisé qui est en cours de téléchargement.

Pour importer le fichier sans opérateur personnalisé, procédez comme suit.

1. Cliquez sur l'onglet **Fichiers sans opérateur**.
2. Cliquez sur l'icône **Importer** ().
3. Cliquez sur **Importation locale**.
4. Sélectionnez `SLES` comme système d'exploitation.
5. Cliquez sur **Parcourir** pour rechercher et sélectionner le fichier sans opérateur à importer (par exemple, `SLES_installPackages_customUnattend.xml`).
6. Cliquez sur **Importer** pour charger le fichier dans le référentiel des images SE.

   Remarque : Un avertissement indiquant que des macros prédéfinies dans le fichier sans opérateur sont manquantes s'affiche. Vous pouvez ignorer cet avertissement pour l'instant. Vous allez ajouter des macros prédéfinis à l'étape suivante
7. Cliquez sur **Fermer** dans la boîte de dialogue d'avertissement pour ouvrir la boîte de dialogue Modifier un fichier sans opérateur.

Etape 4. Associez le fichier sans opérateur personnalisé avec le fichier de paramètres de configuration personnalisé, et ajoutez les macros prédéfinies et personnalisées (de paramètres) requises au fichier sans opérateur à partir du fichier de paramètres de configuration. Pour plus d'informations, voir Association d'un fichier sans opérateur à un fichier de paramètres de configuration, Injection de macros prédéfinies et de macros personnalisées dans un fichier sans opérateur.

Astuce : Vous pouvez éventuellement associer le fichier sans opérateur personnalisé au fichier de paramètres de configuration personnalisé et ajouter des macros lors de l'importation du fichier sans opérateur

1. Dans la boîte de dialogue Modifier un fichier sans opérateur, sélectionnez le fichier de paramètres de configuration à associer au fichier sans opérateur dans la liste déroulante **Associer un fichier de configuration** (par exemple, `SLES_installPackages_customConfig`).
2. Ajoutez les macros prédéfinies requises au fichier sans opérateur.
   a. Sélectionnez **Prédéfinies** à partir de la liste déroulante **Macros disponibles**.
   b. Placez le curseur dans le fichier sans opérateur à n'importe quel endroit après la ligne 1 (après la balise **<xml>**).
   c. Développez la liste **predefined → unattendSettings** dans la liste des macros prédéfinies disponibles.
   d. Cliquez sur les macros **preinstallConfig** et **postinstallConfig** pour ajouter les macros au fichier sans opérateur.

   Par exemple :

   ```
   #predefined.unattendSettings.preinstallConfig#
   #predefined.unattendSettings.postinstallConfig#
   <profile xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://www.suse.com/1.0/configns">
   ```
3. Ajoutez la macro personnalisée pour spécifier le fuseau horaire.
   a. Sélectionnez **Personnalisée** à partir de la liste déroulante **Macros disponibles**.
   b. Placez le curseur après la balise **<hwclock>**, puis cliquez sur **fuseau horaire** pour ajouter la macro de fuseau horaire.

c. Placez le curseur après la balise **<timezone>**, puis cliquez sur **fuseau horaire** pour ajouter la macro de fuseau horaire.

Par exemple :

```
<timezone>
   <hwclock>#timezone#</hwclock>
   <timezone>#timezone#</timezone>
</timezone>
```

4. Ajoutez la macro personnalisée pour spécifier les modules SLES en option.
   a. Développez la liste **paramètres du serveur → nœud** dans la liste des macros personnalisées disponibles.
   b. Placez le curseur dans l'une des balises **<pattern>** vides, puis cliquez sur **fileserver**.
   c. Placez le curseur dans l'une des balises **<pattern>** vides, puis cliquez sur **lampserver**.
   d. Placez le curseur dans l'une des balises **<pattern>** vides, puis cliquez sur **mailserver**.

   Par exemple :

```
<patterns config:type="list">
   <pattern>32bit</pattern>
   <pattern>Basis-Devel</pattern>
   <pattern>Minimal</pattern>
   <pattern>WBEM</pattern>
   <pattern>apparmor</pattern>
   <pattern>base</pattern>
   <pattern>documentation</pattern>
   <pattern>fips</pattern>
   <pattern>gateway_server</pattern>
   <pattern>ofed</pattern>
   <pattern>printing</pattern>
   <pattern>sap_server</pattern>
   <pattern>x11</pattern>
   <pattern>#server-settings.node.fileserver#</pattern>
   <pattern>#server-settings.node.lampserver#</pattern>
   <pattern>#server-settings.node.mailserver#</pattern>
</patterns>
```

5. Cliquez sur **Enregistrer** pour lier les fichiers ensemble et enregistrer les modifications apportées au fichier sans opérateur.

Etape 5. Créez un profil d'image SE personnalisé qui inclut les paramètres de configuration personnalisés et les fichiers sans opérateur. Pour plus d'informations, voir Création d'un profil d'image SE personnalisé.

1. Cliquez sur l'onglet **Images SE**.
2. Sélectionnez un profil d'image SE à personnaliser (par exemple, `Basic`).
3. Cliquez sur l'icône **Créer** ( ) pour afficher la boîte de dialogue Créer un profil personnalisé.
4. Sur l'onglet **Général** :
   a. Entrez un nom pour le profil (par exemple, `SLES personnalisé avec modules en option`).
   b. Utilisez la valeur par défaut pour la zone **Chemin d'accès des données et des fichiers personnalisés**.
   c. Sélectionnez **Fichiers de paramètres configuration et sans opérateur associés** comme type de personnalisation.
   d. Cliquez sur **Suivant**.
5. Sous l'onglet **Options de pilote**, cliquez sur **Suivant** . Les pilotes d'appareil fournis par Windows sont inclus par défaut.
6. Sous l'onglet **Software**, cliquez sur **Suivant**.

7. Sous l'onglet **Fichiers sans opérateur**, sélectionnez le fichier sans opérateur personnalisé (par exemple, `SLES_installPackages_customUnattend.xml`), puis cliquez sur **Suivant**.

   Le fichier de paramètres de configuration associé est sélectionné automatiquement.
8. Sous l'onglet **Scripts d'installation**, cliquez sur **Suivant**.
9. Sous l'onglet **Récapitulatif**, passez les paramètres en revue.
10. Cliquez sur **Personnaliser** pour créer le profil d'image SE personnalisé.

Etape 6. Déployez le profil d'image SE personnalisé sur les serveurs cible. Pour plus d'informations, voir Déploiement d'une image du système d'exploitation.

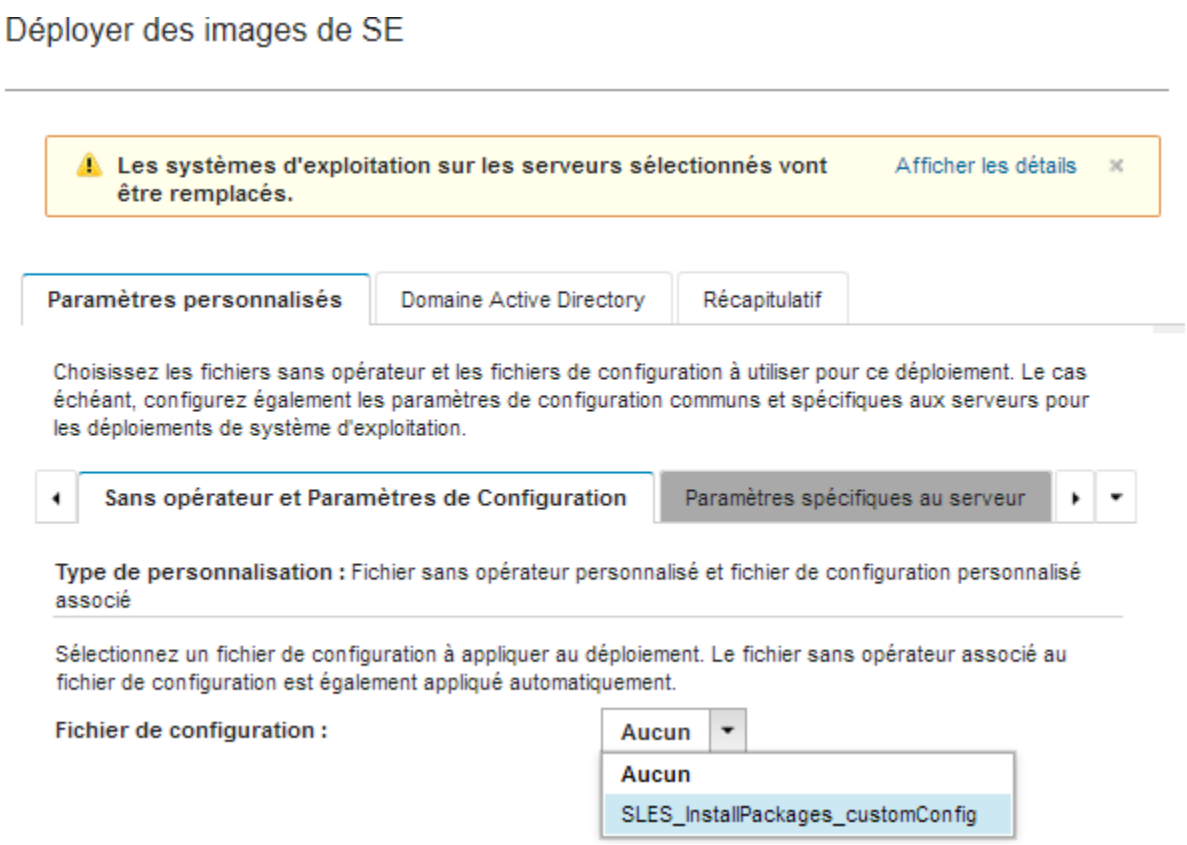
1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Déployer des images SE** pour afficher la page Déployer un système d'exploitation : déployer des images SE.
2. Pour chacun des serveurs cible :
   a. Sélectionnez le serveur.
   b. Cliquez sur **Modifier la sélection → Paramètres réseau**, puis indiquez le nom d'hôte, l'adresse IP, les paramètres DNS, MTU et VLAN pour le serveur.

      Astuce : Les paramètres VLAN sont disponibles uniquement lorsque le mode VLAN est défini dans **Paramètres globaux → Affectation d'IP → Utiliser les réseaux VLAN**.
   c. Sélectionnez le profil d'image SE personnalisé (par exemple, *<base_OS>*|*<timestamp>*_`SLES personnalisé avec modules en option`) dans la liste déroulante de la colonne **Image à déployer**.

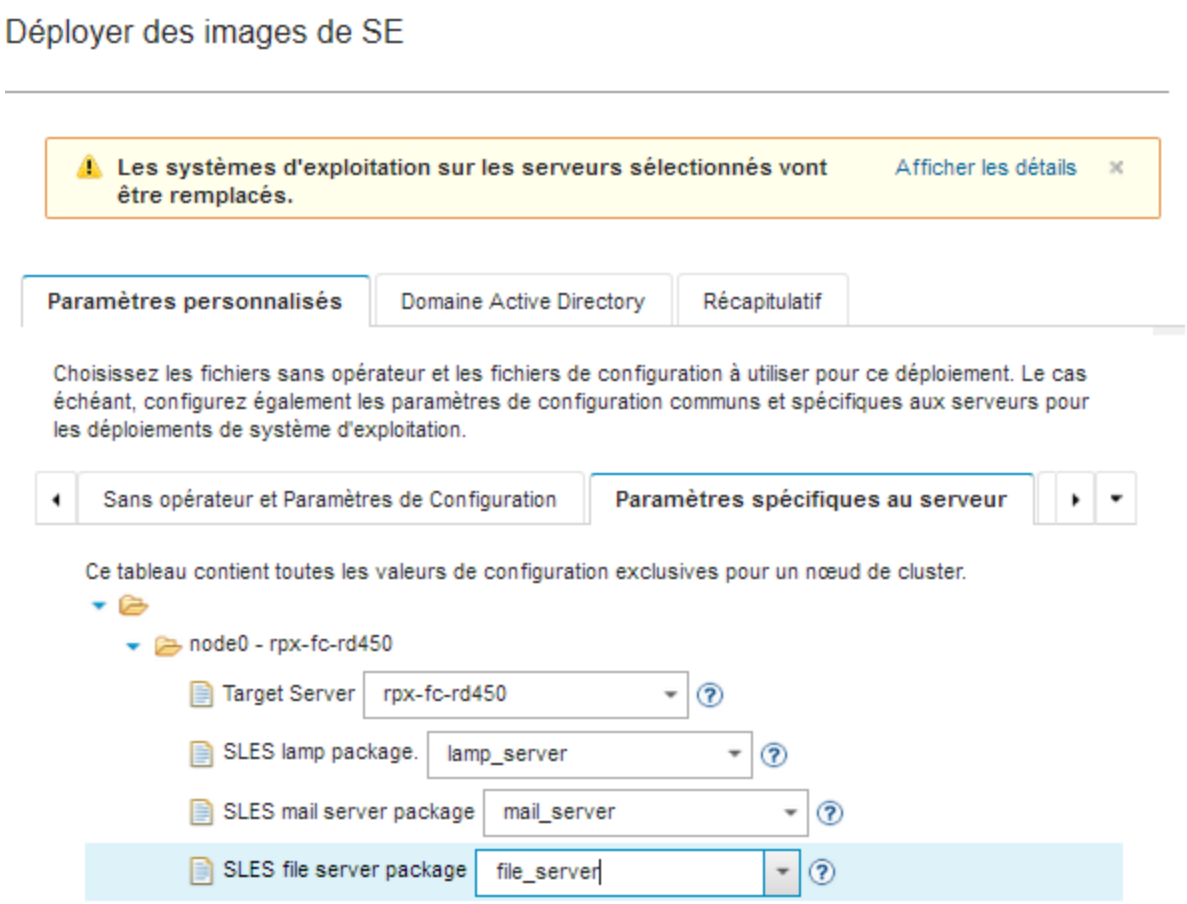
      Remarque : Vérifiez que tous les serveurs cible utilisent le même profil personnalisé.
   d. Sélectionnez l'emplacement de stockage préféré sur lequel vous souhaitez déployer l'image du système d'exploitation dans la colonne **Stockage**.

      Remarque : Pour faire en sorte que les déploiements de système d'exploitation aboutissent, déconnectez toutes les unités de stockage du serveur géré, à l'exception de l'unité de stockage qui a été choisie pour le déploiement du système d'exploitation.
   e. Vérifiez que l'état de déploiement du serveur sélectionné est **Prêt**.
3. Sélectionnez tous les serveurs cible, puis cliquez sur l'icône **Déployer l'image** () pour lancer le déploiement du système d'exploitation.
4. Sous l'onglet **Paramètres personnalisés**, cliquez sur le sous-onglet **Paramètres de configuration et sans opérateur**, puis sélectionnez le fichier de paramètres de configuration personnalisé (par exemple, `SLES_installPackages_customConfig`).

   Remarque : Le fichier sans opérateur personnalisé associé est sélectionné automatiquement.



5. Sous le sous-onglet **Paramètres spécifiques au serveur**, sélectionnez le serveur cible et les modules SLES en option que vous souhaitez déployer.



6. Sous le sous-onglet **Paramètres globaux**, sélectionnez le fuseau horaire à définir pour tous les serveurs cible.

7. Sous l'onglet **Récapitulatif**, passez les paramètres en revue.
8. Cliquez sur **Déployer** pour déployer le système d'exploitation.

Déploiement de SLES 12 SP3 avec des logiciels personnalisés

Ce scénario installe le système d'exploitation SLES 12 SP3 avec des logiciels personnalisés (Java et Eclipse IDE). Un profil personnalisé comprenant les logiciels personnalisés et les scripts post-installation d'installation et de configuration des logiciels personnalisés. Les modules logiciels personnalisés sont copiés sur l'hôte lors du déploiement, puis mis à disposition pour le script de post-installation personnalisé.

Avant de commencer

Ce scénario utilise les modèles de fichiers suivants.

- jre-8u151-linux-x64.tar.gz. Il s'agit du fichier d'installation pour Java pour Eclipse.
- eclipse-4.6.3-3.1.x86_64.tar.gz Il s'agit du fichier d'installation pour un environnement de développement Eclipse.
- SLES_installSoftware_customScript.sh Ce script de post-installation crée un utilisateur pour le lancement d'Eclipse, puis il installe l'environnement de développement Eclipse et Java.

Remarques :

- Les scripts d'installation SLES se présentent sous l'un des formats suivants : Bash (.sh), Perl (.pm ou .pl), Python (.py)
- Les fichiers logiciels et les scripts d'installation sont installés à partir du chemin de données et de fichiers personnalisé que vous spécifiez lors du déploiement. Le chemin d'accès aux fichiers et données personnalisés par défaut est `/home/lxca`.
- Pour SLES 12 SP3, l'environnement de développement Eclipse requiert le compilateur GCC, lequel est inclus dans le profil de base prédéfini. Ce scénario crée un profil d'image SE personnalisé à l'aide du profil de base prédéfini comme base. Si vous choisissez d'utiliser un autre profil, vous devez vous assurer que le profil contient le compilateur GCC.

Procédure

Pour déployer SLES 12 SP3 avec des logiciels personnalisés, procédez comme suit.

Etape 1. Téléchargez le système d'exploitation SLES 12 SP3 de base à partir du site web SUSE sur le système local, puis importez l'image dans le référentiel d'images SE. Pour plus d'informations, voir Importation d'images du système d'exploitation.

1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Gérer les images de SE** pour afficher la page Déployer un système d'exploitation : déployer des images de SE.
2. Cliquez sur l'onglet **Images SE**.
3. Cliquez sur l'icône **Importer** ( ).
4. Cliquez sur **Importation locale**.
5. Cliquez sur **Parcourir** pour rechercher et sélectionner l'image SLES 12 SP3 à importer (par exemple, `SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso`).
6. Cliquez sur **Importer** pour charger l'image dans le référentiel des images SE.
7. Attendez la fin de l'importation. Cette opération peut prendre un certain temps.

Etape 2. Téléchargez le logiciel personnalisé sur le système local et importez les fichiers dans le référentiel d'images SE. Pour plus d'informations, voir Importation de logiciels personnalisés.

1. Cliquez sur l'onglet **Logiciels**.
2. Cliquez sur l'icône **Importer** ( ).
3. Cliquez sur **Importation locale**.

4. Sélectionnez SLES comme système d'exploitation.
5. Cliquez sur **Parcourir** pour rechercher et sélectionner le fichier logiciel à importer (par exemple, jre-8u151-linux-x64.tar.gz).
6. Cliquez sur **Importer** pour charger le fichier dans le référentiel des images SE.
7. Cliquez de nouveau sur l'icône **Importer** ().
8. Cliquez sur **Importation locale**.
9. Sélectionnez SLES comme système d'exploitation.
10. Cliquez sur **Parcourir** pour rechercher et sélectionner le fichier-logiciel à importer (par exemple, eclipse-4.6.3-3.1.x86_64.tar.gz).
11. Cliquez sur **Importer** pour charger le fichier dans le référentiel des images SE.

Etape 3. Créez un script de post-installation personnalisé et importez le fichier dans le référentiel d'images SE.

Ajoutez les commandes permettant de créer un utilisateur pour lancer Eclipse dans ce fichier, par exemple :

```
echo "Create a user called lenovo..."
egrep "lenovo" /etc/passwd >/dev/null
pass=$(perl -e 'print crypt($ARGV[0], "password")' "Passw0rd")
useradd -m -p $pass lenovo
[ $? -eq 0 ] &amp;amp;&amp;amp; echo "User has been created." || curl -X PUT
--globoff #predefined.otherSettings.statusSettings.urlStatus# -H "Content-Type: application/json"
-d '{"deployStatus":{"id":"46","parameters":["'"Could not create lenovo user"'"]}}'
--cert #predefined.otherSettings.statusSettings.certLocation#/cert.pem
--key #predefined.otherSettings.statusSettings.certLocation#/key.pem
--cacert #predefined.otherSettings.statusSettings.certLocation#/ca-bundle.crt
```

Ajoutez les commandes pour installer le logiciel, par exemple :

```
#Install Java for eclipse
echo "Installing Java JRE 8...."
rpm -ivh #predefined.otherSettings.deployDataAndSoftwareLocation#/jre-8u151-linux-x64.rpm

#Install eclipse
echo "Installing Eclipse IDE..."
rpm -ivh #predefined.otherSettings.deployDataAndSoftwareLocation#/eclipse-4.6.3-3.1.x86_64.rpm
```

Notez que ces commandes utilisent des macros prédéfinies pour l'URL HTTPS utilisée par XClarity Administrator pour la production de rapports d'état (**predefined.otherSettings.statusSettings.urlStatus**), pour le dossier contenant les certificats qui sont nécessaires pour accéder au service Web urlStatus depuis le SE hôte au premier amorçage (**predefined.otherSettings.statusSettings.certLocation**), ainsi que pour les chemin d'accès aux fichiers de données et de logiciels extraits (**predefined.otherSettings.deployDataAndSoftwareLocation**).

Vous pouvez également ajouter des commandes pour envoyer des messages personnalisés aux travaux qui se connectent dans XClarity Administrator, comme illustré dans le modèle de fichier. Pour plus d'informations, voir Ajout de rapport d'état personnalisé aux scripts d'installation.

Pour importer le script d'installation personnalisé, procédez comme suit. Pour plus d'informations, voir Importation de scripts d'installation personnalisés.

1. Cliquez sur l'onglet **Scripts d'installation**.
2. Cliquez sur l'icône **Importer** ().
3. Cliquez sur **Importation locale**.
4. Sélectionnez SLES comme système d'exploitation.

5. Cliquez sur **Parcourir** pour rechercher et sélectionner le script de post-installation à importer (par exemple, `SLES_installSoftware_customScript.sh`).
6. Cliquez sur **Importer** pour charger le fichier dans le référentiel des images SE.

Etape 4. Créez un profil d'image SE personnalisé qui inclut le logiciel personnalisé et le script de post-installation. Pour plus d'informations, voir Création d'un profil d'image SE personnalisé.

1. Cliquez sur l'onglet **Images SE**.
2. Sélectionnez un profil d'image SE à personnaliser (par exemple, `Basic`).
3. Cliquez sur l'icône **Créer** ( ) pour afficher la boîte de dialogue Créer un profil personnalisé.
4. Sur l'onglet **Général** :
   a. Entrez un nom pour le profil (par exemple, `SLES personnalisé avec logiciels`).
   b. Utilisez la valeur par défaut pour la zone **Chemin d'accès des données et des fichiers personnalisés**.
   c. Sélectionnez **Aucun** comme type de personnalisation.
   d. Cliquez sur **Suivant**.
5. Sous l'onglet **Options de pilote**, cliquez sur **Suivant** . Les pilotes d'appareil fournis par Windows sont inclus par défaut.
6. Sous l'onglet **Logiciels**, sélectionnez les fichiers d'installation des logiciels (par exemple `jre-8u151-linux-x64.tar.gz` et `eclipse-4.6.3-3.1.x86_64.tar.gz`), puis cliquez sur **Suivant**.
7. Sous l'onglet **Scripts d'installation**, sélectionnez les scripts d'installation (par exemple, `SLES_installSoftware_customScript.sh`), puis cliquez sur **Suivant**.
8. Sous l'onglet **Récapitulatif**, passez les paramètres en revue.
9. Cliquez sur **Personnaliser** pour créer le profil d'image SE personnalisé.

Etape 5. Déployez le profil d'image SE personnalisé sur les serveurs cible. Pour plus d'informations, voir Déploiement d'une image du système d'exploitation.

1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Déployer des images SE** pour afficher la page Déployer un système d'exploitation : déployer des images SE.
2. Pour chacun des serveurs cible :
   a. Sélectionnez le serveur.
   b. Cliquez sur **Modifier la sélection → Paramètres réseau**, puis indiquez le nom d'hôte, l'adresse IP, les paramètres DNS, MTU et VLAN pour le serveur.

      Astuce : Les paramètres VLAN sont disponibles uniquement lorsque le mode VLAN est défini dans **Paramètres globaux → Affectation d'IP → Utiliser les réseaux VLAN**.
   c. Sélectionnez le profil d'image SE personnalisé (par exemple, *<base_OS>*|*<timestamp>*_`SLES personnalisé avec logiciel`) dans la liste déroulante de la colonne **Image à déployer**

      Remarque : Vérifiez que tous les serveurs cible utilisent le même profil personnalisé.
   d. Sélectionnez l'emplacement de stockage préféré sur lequel vous souhaitez déployer l'image du système d'exploitation dans la colonne **Stockage**.

      Remarque : Pour faire en sorte que les déploiements de système d'exploitation aboutissent, déconnectez toutes les unités de stockage du serveur géré, à l'exception de l'unité de stockage qui a été choisie pour le déploiement du système d'exploitation.
   e. Vérifiez que l'état de déploiement du serveur sélectionné est **Prêt**.
3. Sélectionnez tous les serveurs cible, puis cliquez sur l'icône **Déployer l'image** ( ) pour lancer le déploiement du système d'exploitation.

4. Sous l'onglet **Récapitulatif**, passez les paramètres en revue.
5. Cliquez sur **Déployer** pour déployer le système d'exploitation.

Déploiement de SLES 12 SP3 avec des paramètres régionaux configurable et des serveurs NTP

Ce scénario installe le système d'exploitation SLES 12 SP3 en activant l'anglais, le brésilien ou le japonais pour le clavier et les paramètres régionaux du système d'exploitation. Il configure également l'adresse IP pour jusqu'à trois serveurs NTP. Un profil d'image SE personnalisé est utilisé. Il comprend un fichier sans opérateur (avec des macros prédéfinies et des macros personnalisées) et un fichier de paramètres de configuration permettant de sélectionner les paramètres régionaux et les paramètres du serveur NTP. Ce profil personnalisé peut être sélectionné sur la page Déployer des images de SE. Ensuite, les paramètres régionaux et les paramètres du serveur NTP peuvent être sélectionnés sous l'onglet **Paramètres personnalisés**. Les valeurs spécifiées sont remplacées dans les macros personnalisées contenues dans le fichier sans opérateur personnalisé et le programme d'installation autoyast SLES utilise ces valeurs dans le fichier sans opérateur pour configurer le système d'exploitation.

Avant de commencer

Ce scénario utilise les modèles de fichiers suivants.

- SLES_locale_customConfig.json. Ce fichier de configuration personnalisé demande la langue d'installation des paramètres régionaux du SE et du clavier pour SLES et le serveur NTP.
- SLES_locale_customUnattend.xml. Ce fichier sans opérateur personnalisé utilise les valeurs des macros personnalisées qui sont définies dans le fichier de configuration.

Procédure

Pour déployer SLES 12 SP3 à l'aide d'un profil d'image SE personnalisé, procédez comme suit.

Etape 1. Téléchargez le système d'exploitation SLES de base à partir du site web SUSE sur le système local, puis importez l'image dans le référentiel d'images SE. Pour plus d'informations, voir Importation d'images du système d'exploitation.

1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Gérer les images de SE** pour afficher la page Déployer un système d'exploitation : déployer des images de SE.
2. Cliquez sur l'onglet **Images SE**.
3. Cliquez sur l'icône **Importer** ().
4. Cliquez sur **Importation locale**.
5. Cliquez sur **Parcourir** pour rechercher et sélectionner l'image SLES 12 SP3 à importer (par exemple, `SLE-12-SP3-Server-DVD-x86_64-GM-DVD1.iso`).
6. Cliquez sur **Importer** pour charger l'image dans le référentiel des images SE.
7. Attendez la fin de l'importation.

Etape 2. Créer un fichier de paramètres de configuration personnalisé et importez-le dans le référentiel d'images SE.

Le fichier de paramètres de configuration est un fichier JSON qui décrit les données à collecter dynamiquement pendant le processus de déploiement SE. Dans le cadre de ce scénario, nous souhaitons spécifier les paramètres régionaux du système d'exploitation (en_US, ja_JP, pt_BR), les paramètres régionaux du clavier (anglais-US, japonais ou portugais-BR) et jusqu'à trois adresses IP de serveur NTP à utiliser pour chaque déploiement SE. Pour plus d'informations sur la création d'un fichier de paramètres de configuration, voir Macros personnalisées.

Pour importer le fichier de paramètres de configuration, procédez comme suit. Pour plus d'informations, voir Importation de paramètres de configuration personnalisés.

1. Cliquez sur l'onglet **Fichiers de configuration**.
2. Cliquez sur l'icône **Importer** ().
3. Cliquez sur **Importation locale**.
4. Sélectionnez `SLES` comme système d'exploitation.
5. Cliquez sur **Parcourir** pour rechercher et sélectionner le fichier de paramètres de configuration à importer (par exemple, `SLES_locale_customConfig.json`).
6. Cliquez sur **Importer** pour charger le fichier dans le référentiel des images SE.

   Remarque : Lorsque vous importez un fichier de paramètres de configuration personnalisé, XClarity Administratorgénère des macros personnalisées pour chaque paramètre du fichier. Vous pouvez ajouter ces macros au fichier sans opérateur. Pendant le déploiement SE, les macros sont remplacées par des valeurs réelles.

Etape 3. Modifiez le fichier sans opérateur SLES pour spécifier des valeurs dynamiques pour les paramètres régionaux du système d'exploitation, les paramètres régionaux du clavier et les adresses IP du serveur NTP, puis importez le fichier personnalisé dans le référentiel d'images SE. Pour plus d'informations, voir Importation de fichiers sans opérateur personnalisés.

Juste après la balise <profile>, ajoutez les informations relatives au serveur NTP et au réseau. L'exemple suivant contient des balises pour deux serveurs NTP. Les adresses IP seront ajoutées en tant que macros à une étape ultérieure.

```
<ntp-client>
   <configure_dhcp config:type="boolean">false</configure_dhcp>
   <peers config:type="list">
      <peer>
         <address></address>
         <initial_sync config:type="boolean">true</initial_sync>
         <options></options>
         <type>server</type>
      </peer>
      <peer>
         <address></address>
         <initial_sync config:type="boolean">true</initial_sync>
         <options></options>
         <type>server</type>
      </peer>
   </peers>
   <start_at_boot config:type="boolean">true</start_at_boot>
   <start_in_chroot config:type="boolean">true</start_in_chroot>
</ntp-client>
```

Dans la section <general>, ajoutez les informations des paramètres régionaux du SE et du clavier, comme illustré dans l'exemple suivant. Les paramètres régionaux de clavier et de système d'exploitation seront ajoutés en tant que macros à une étape ultérieure.

```
<keyboard>
   <keymap></keymap>
</keyboard>
<language></language>
```

Remarque : Lorsque vous utilisez un fichier sans opérateur personnalisé, XClarity Administrator n'offre pas la plupart des fonctionnalités normales dont vous bénéficiez lorsque vous utilisez un fichier sans opérateur prédéfini. Par exemple, les cibles **<DiskConfiguration>**, **<ImageInstall>**, **<ProductKey>** et **<UserAccounts>** pour l'administrateur, **<Interfaces>** pour les réseaux et la

liste **<package>** pour les fonctionnalités d'installation doivent être spécifiées dans le fichier sans opérateur personnalisé qui est en cours de téléchargement.

Pour importer le fichier sans opérateur personnalisé, procédez comme suit.

1. Cliquez sur l'onglet **Fichiers sans opérateur**.
2. Cliquez sur l'icône **Importer** ().
3. Cliquez sur **Importation locale**.
4. Sélectionnez `SLES` comme système d'exploitation.
5. Cliquez sur **Parcourir** pour rechercher et sélectionner le fichier sans opérateur à importer (par exemple, `SLES_locale_customUnattend.xml`).
6. Cliquez sur **Importer** pour charger le fichier dans le référentiel des images SE.

Etape 4. Associez le fichier sans opérateur personnalisé avec le fichier de paramètres de configuration personnalisé, et ajoutez les macros prédéfinies et personnalisées (de paramètres) requises au fichier sans opérateur à partir du fichier de paramètres de configuration. Pour plus d'informations, voir Association d'un fichier sans opérateur à un fichier de paramètres de configuration, Injection de macros prédéfinies et de macros personnalisées dans un fichier sans opérateur.

Astuce : Vous pouvez éventuellement associer le fichier sans opérateur personnalisé au fichier de paramètres de configuration personnalisé et ajouter des macros lors de l'importation du fichier sans opérateur.

1. À partir de l'onglet **Fichiers sans opérateur**, sélectionnez le fichier sans opérateur personnalisé (par exemple, `SLES_locale_customUnattend.xml`).
2. Cliquez sur l'icône **Associer un fichier de configuration** () pour afficher la boîte de dialogue Associer un fichier sans opérateur.
3. Sélectionnez le fichier de paramètres de configuration à associer au fichier sans opérateur (par exemple, `SLES_locale_customConfig`).
4. Ajoutez les macros prédéfinies requises au fichier sans opérateur.
   a. Sélectionnez **Prédéfinies** à partir de la liste déroulante **Macros disponibles**.
   b. Placez le curseur dans le fichier sans opérateur à n'importe quel endroit après la ligne 1 (après la balise **<xml>**).
   c. Développez la liste **predefined → unattendSettings** dans la liste des macros prédéfinies disponibles.
   d. Cliquez sur les macros **preinstallConfig** et **postinstallConfig** pour ajouter les macros.

   Par exemple :

```
<?xml version="1.0"?>
<!DOCTYPE profile SYSTEM "/usr/share/YaST2/include/autoinstall/profile.dtd">
   #predefined.unattendSettings.preinstallConfig#
   #predefined.unattendSettings.postinstallConfig#
<profile xmlns="http://www.suse.com/1.0/yast2ns" xmlns:config="http://www.suse.com/1.0/configns">
```

5. Ajoutez la macro personnalisée pour spécifier les paramètres régionaux du système d'exploitation.
   a. Sélectionnez **Personnalisée** à partir de la liste déroulante **Macros disponibles**.
   b. Placez le curseur après la balise **<language>**.
   c. Développez **Paramètres du serveur → Nœud** dans la liste des macros personnalisées disponibles, puis cliquez sur **Paramètres régionaux** pour ajouter la macro des paramètres régionaux du système d'exploitation.

   Par exemple :

```
<language>#server-settings.node.locale#</language>
```

6. Ajoutez la macro personnalisée pour spécifier les paramètres régionaux du clavier.
   a. Placez le curseur après la balise **<keymap>**.
   b. Développez **Paramètres du serveur → Nœud** dans la liste des macros personnalisées disponibles, puis cliquez sur **keyboardLocale** pour ajouter la macro des paramètres régionaux du clavier.

   Par exemple :

```
<keyboard>
   <keymap>#server-settings.node.keyboardLocale#</keymap>
</keyboard>
```

7. Ajoutez la macro personnalisée pour spécifier les adresses IP du serveur NTP.

   Dans ce scénario, le fichier de paramètres de configuration personnalisé utilise un modèle pour indiquer de zéro à trois serveurs NTP. Lors de l'utilisation de modèles dans le fichier de paramètres de configuration, les macros qui sont associées à un modèle ne sont pas affichées dans la boîte de dialogue Associer un fichier sans opérateur. Au lieu de cela, vous devez modifier manuellement le fichier sans opérateur et ajouter les macros et les balises appropriées.

   Par exemple, pour inclure trois serveurs NTP, vous devez ajouter les balises et les macros suivantes dans le fichier sans opérateur. Ces balises et macros existent déjà dans l'exemple de fichier sans opérateur de ce scénario.

```
<ntp-client>
   <configure_dhcp config:type="boolean">false</configure_dhcp>
   <peers config:type="list">
      <peer>
         <address>#server-settings.ntpserver1#</address>
         <initial_sync config:type="boolean">true</initial_sync>
         <options></options>
         <type>server</type>
      </peer>
      <peer>
         <address>#server-settings.ntpserver2#</address>
         <initial_sync config:type="boolean">true</initial_sync>
         <options></options>
         <type>server</type>
      </peer>
      <peer>
         <address>#server-settings.ntpserver3#</address>
         <initial_sync config:type="boolean">true</initial_sync>
         <options></options>
         <type>server</type>
      </peer>
   </peers>
   <start_at_boot config:type="boolean">true</start_at_boot>
    <start_in_chroot config:type="boolean">true</start_in_chroot>
</ntp-client>
```

8. Cliquez sur **Associer** pour lier les fichiers ensemble et enregistrer les modifications apportées au fichier sans opérateur.

Etape 5. Créez un profil d'image SE personnalisé qui inclut les paramètres de configuration personnalisés et les fichiers sans opérateur. Pour plus d'informations, voir Création d'un profil d'image SE personnalisé.

1. Cliquez sur l'onglet **Images SE**.
2. Sélectionnez un profil d'image SE à personnaliser (par exemple, `Basic`).

3. Cliquez sur l'icône **Créer** ( ) pour afficher la boîte de dialogue Créer un profil personnalisé.
4. Sur l'onglet **Général** :
   a. Entrez un nom pour le profil (par exemple, `SLES personnalisé pour paramètres régionaux SE et clavier et serveur NTP`).
   b. Utilisez la valeur par défaut pour la zone **Chemin d'accès des données et des fichiers personnalisés**.
   c. Sélectionnez **Fichiers de paramètres configuration et sans opérateur associés** comme type de personnalisation.
   d. Cliquez sur **Suivant**.
5. Sous l'onglet **Options de pilote**, cliquez sur **Suivant** . Les pilotes d'appareil fournis par Windows sont inclus par défaut.
6. Sous l'onglet **Software**, cliquez sur **Suivant**.
7. Sous l'onglet **Fichiers sans opérateur**, sélectionnez le fichier sans opérateur personnalisé (par exemple, `SLES_locale_customUnattend.xml`), puis cliquez sur **Suivant**.

   Le fichier de paramètres de configuration associé est sélectionné automatiquement.
8. Sous l'onglet **Scripts d'installation**, cliquez sur **Suivant**.
9. Sous l'onglet **Récapitulatif**, passez les paramètres en revue.
10. Cliquez sur **Personnaliser** pour créer le profil d'image SE personnalisé.

Etape 6. Déployez le profil d'image SE personnalisé sur le serveur cible. Pour plus d'informations, voir Déploiement d'une image du système d'exploitation.

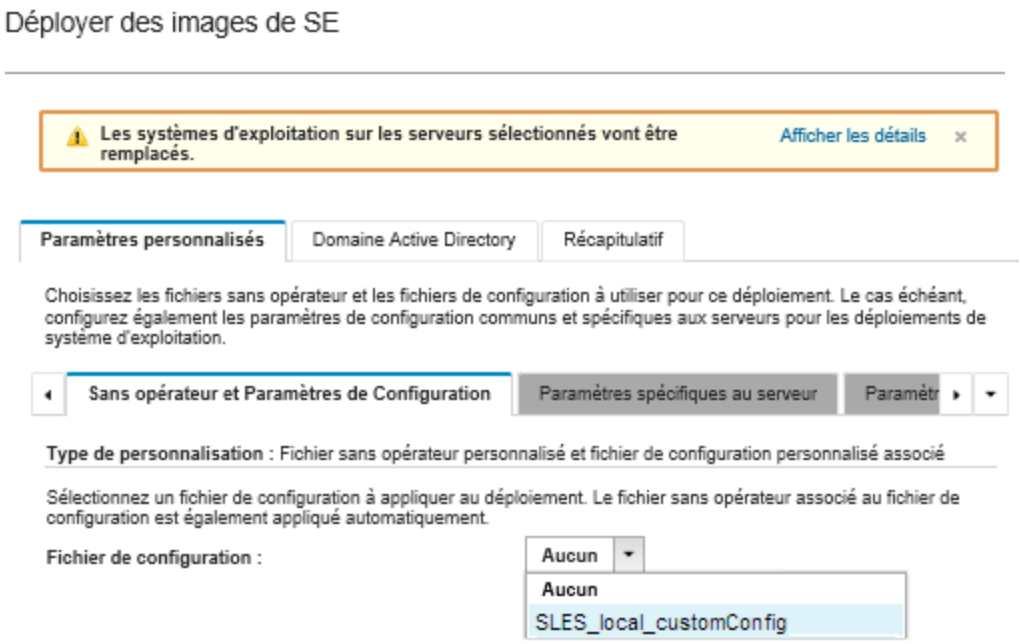
1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Déployer des images SE** pour afficher la page Déployer un système d'exploitation : déployer des images SE.
2. Pour chacun des serveurs cible :
   a. Sélectionnez le serveur.
   b. Cliquez sur **Modifier la sélection → Paramètres réseau**, puis indiquez le nom d'hôte, l'adresse IP, les paramètres DNS, MTU et VLAN pour le serveur.

      Astuce : Les paramètres VLAN sont disponibles uniquement lorsque le mode VLAN est défini dans **Paramètres globaux → Affectation d'IP → Utiliser les réseaux VLAN**.
   c. Sélectionnez le profil d'image SE personnalisé (par exemple, *<base_OS>*|*<timestamp>*_`SLES personnalisé pour paramètres régionaux SE et clavier et serveur NTP`) dans la liste déroulante de la colonne **Image à déployer**

      Remarque : Vérifiez que tous les serveurs cible utilisent le même profil personnalisé.
   d. Sélectionnez l'emplacement de stockage préféré sur lequel vous souhaitez déployer l'image du système d'exploitation dans la colonne **Stockage**.

      Remarque : Pour faire en sorte que les déploiements de système d'exploitation aboutissent, déconnectez toutes les unités de stockage du serveur géré, à l'exception de l'unité de stockage qui a été choisie pour le déploiement du système d'exploitation.
   e. Vérifiez que l'état de déploiement du serveur sélectionné est **Prêt**.
3. Sélectionnez tous les serveurs cible, puis cliquez sur l'icône **Déployer l'image** ( ) pour lancer le déploiement du système d'exploitation.
4. Sous l'onglet **Paramètres personnalisés**, cliquez sur le sous-onglet **Paramètres de configuration et sans opérateur**, puis sélectionnez le fichier de paramètres de configuration personnalisé (par exemple, `SLES_locale_customConfig`).

Remarque : Le fichier sans opérateur personnalisé associé est sélectionné automatiquement.



5. Sous le sous-onglet **Paramètres spécifiques au serveur**, sélectionnez le serveur cible, les paramètres régionaux du système d'exploitation et les paramètres régionaux du clavier.
6. Sous le sous-onglet **Paramètres globaux**, cliquez sur **Ajouter** pour définir l'adresse IP de jusqu'à trois serveurs NTP.
7. Sous l'onglet **Récapitulatif**, passez les paramètres en revue.
8. Cliquez sur **Déployer** pour déployer le système d'exploitation.

Déploiement de VMware ESXi v6.7 avec personnalisation Lenovo sur un disque local à l'aide d'une adresse IP statique

Ce scénario installe le système d'exploitation VMware ESXi v6.7 avec personnalisation Lenovo sur le disque local à l'aide de l'adresse IP statique du serveur hôte. Un profil d'image SE personnalisé comprenant un fichier sans opérateur avec des macros prédéfinies. Ce profil personnalisé peut être sélectionné sur la page Déployer des images de SE. Les valeurs connues sont remplacées par les macros prédéfinies dans le fichier sans opérateur personnalisé et le programme d'installation VMware ESXi kickstart utilise ces valeurs dans le fichier sans opérateur pour configurer le système d'exploitation.

Avant de commencer

Ce scénario utilise les modèles de fichiers suivants.

- ESXi_staticIP_customUnattend.cfg. Ce fichier sans opérateur personnalisé utilise les valeurs de macros prédéfinies.

Procédure

Pour déployer VMware ESXi v6.7 à l'aide d'un profil d'image SE personnalisé, procédez comme suit.

Etape 1. Téléchargez le système d'exploitation VMware vSphere® Hypervisor (ESXi) avec personnalisation Lenovo à partir du Support VMware - Site Web de téléchargement site Web Red Hat sur le système local, puis importez l'image dans le référentiel d'images SE. Pour plus d'informations, voir Importation d'images du système d'exploitation.

1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Gérer les images de SE** pour afficher la page Déployer un système d'exploitation : déployer des images de SE.
2. Cliquez sur l'onglet **Images SE**.
3. Cliquez sur l'icône **Importer** ().
4. Cliquez sur **Importation locale**.
5. Cliquez sur **Parcourir** pour rechercher et sélectionner l'image ESXi à importer (par exemple, `ESXi6.7-7535516-RC-Lenovo_20180126_Async.iso`).
6. Cliquez sur **Importer** pour charger l'image dans le référentiel des images SE.
7. Attendez la fin de l'importation.

Etape 2. Modifiez le fichier sans opérateur ESXi (kickstart) pour ajouter les macros prédéfinies et d'autres macros prédéfinies le cas échéant, comme l'adresse IP, la passerelle, les paramètres de nom DNS et de nom d'hôte, puis importez le fichier personnalisé dans le référentiel d'images SE. Pour plus d'informations, voir Importation de fichiers sans opérateur personnalisés.

Pour ESXi et RHEL uniquement, XClarity Administrator fournit la macro **#predefined.unattendSettings.networkConfig#**, laquelle ajoute tous les paramètres réseau qui sont définis dans l'interface graphique du fichier sans opérateur. Étant donné que cet exemple indique un paramètre (**--addvmportgroup**) qui n'est pas défini dans l'interface utilisateur, la macro **#predefinedunattendSettings.storageConfig#** n'est pas utilisée dans l'exemple de fichier sans opérateur. Au lieu de cela, les paramètres réseau sont ajoutées individuellement dans le fichier et les macros **#predefined.hostPlatforms.networkSettings.**<*setting*>**#** sont utilisées.

Pour ESXi et RHEL uniquement, XClarity Administrator fournit également la macro **#predefined.unattendSettings.storageConfig#**, laquelle ajoute tous les paramètres de stockage qui sont définis dans l'interface graphique du fichier sans opérateur. Étant donné que cet exemple indique des paramètres (**--novmfsondisk** et **–ignoressd**) qui ne sont pas définis dans l'interface utilisateur, la macro **#predefinedunattendSettings.storageConfig#** n'est pas utilisée dans l'exemple de fichier sans opérateur. Au lieu de cela, les paramètres de stockage sont ajoutées individuellement et **--firstdisk=local** est codé en dur dans le fichier.

Remarque : XClarity Administrator fournit certaines macros de base, par exemple l'injection de pilotes OOB, la génération de rapports d'état, des scripts de post-installation et des logiciels personnalisés. Toutefois, pour tirer parti de ces macros prédéfinies, vous devez spécifier les macros suivantes dans le fichier sans opérateur personnalisé. Le fichier exemple contient déjà les macros requises. Notez que comme la section %firstboot est incluse, l'ordre de ces macros prédéfinies a de l'importance. Pour plus d'informations, voir Importation de fichiers sans opérateur personnalisés.

```
#predefined.unattendSettings.preinstallConfig#
#predefined.unattendSettings.postinstallConfig#
```

Le modèle de fichier contient déjà les macros nécessaires et les macros prédéfinies supplémentaires pour l'indication en mode dynamique des paramètres réseau pour le serveur cible. Pour plus d'informations sur l'ajout de macros dans les fichiers sans opérateur, voir Injection de macros prédéfinies et de macros personnalisées dans un fichier sans opérateur.

Pour plus d'informations sur les macros prédéfinies disponibles, voir Macros prédéfinies.

Pour importer le fichier sans opérateur personnalisé, procédez comme suit.

1. Cliquez sur l'onglet **Fichiers sans opérateur**.
2. Cliquez sur l'icône **Importer** ().
3. Cliquez sur **Importation locale**.

4. Sélectionnez `ESXi` comme système d'exploitation.
5. Cliquez sur **Parcourir** pour rechercher et sélectionner le fichier sans opérateur à importer (par exemple, `ESXi_staticIP_customUnattend.cfg`).
6. Cliquez sur **Importer** pour charger le fichier dans le référentiel des images SE.

Etape 3. Créez un profil d'image SE personnalisé qui inclut le fichier personnalisé. Pour plus d'informations, voir Création d'un profil d'image SE personnalisé.

1. Cliquez sur l'onglet **Images SE**.
2. Sélectionnez un profil d'image SE à personnaliser (par exemple, `Virtualization`).
3. Cliquez sur l'icône **Créer** ( ) pour afficher la boîte de dialogue Créer un profil personnalisé.
4. Sur l'onglet **Général** :
   a. Entrez un nom pour le profil (par exemple, `ESXi personnalisé avec IP statique`).
   b. Utilisez la valeur par défaut pour la zone **Chemin d'accès des données et des fichiers personnalisés**.
   c. Sélectionnez **Fichiers sans opérateur uniquement** comme type de personnalisation.
   d. Cliquez sur **Suivant**.
5. Sous l'onglet **Fichiers sans opérateur**, sélectionnez le fichier sans opérateur personnalisé (par exemple, `ESXi_staticIP_customUnattend.cfg`), puis cliquez sur **Suivant**.
6. Sous l'onglet **Récapitulatif**, passez les paramètres en revue.
7. Cliquez sur **Personnaliser** pour créer le profil d'image SE personnalisé.

Etape 4. Déployez le profil d'image SE personnalisé sur le serveur cible. Pour plus d'informations, voir Déploiement d'une image du système d'exploitation.

1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Déployer des images SE** pour afficher la page Déployer un système d'exploitation : déployer des images SE.
2. Pour chacun des serveurs cible :
   a. Sélectionnez le serveur.
   b. Cliquez sur **Modifier la sélection → Paramètres réseau**, puis indiquez le nom d'hôte, l'adresse IP, les paramètres DNS, MTU et VLAN pour le serveur.

      Astuce :

      - Les paramètres VLAN sont disponibles uniquement lorsque le mode VLAN est défini dans **Paramètres globaux → Affectation d'IP → Utiliser les réseaux VLAN**.
      - Les paramètres réseau que vous spécifiez dans la boîte de dialogue Paramètres réseau sont ajoutés au fichier sans opérateur au moment de l'exécution à l'aide des macros **#predefined.hostPlatforms.networkSettings.**<*setting*>**#**.

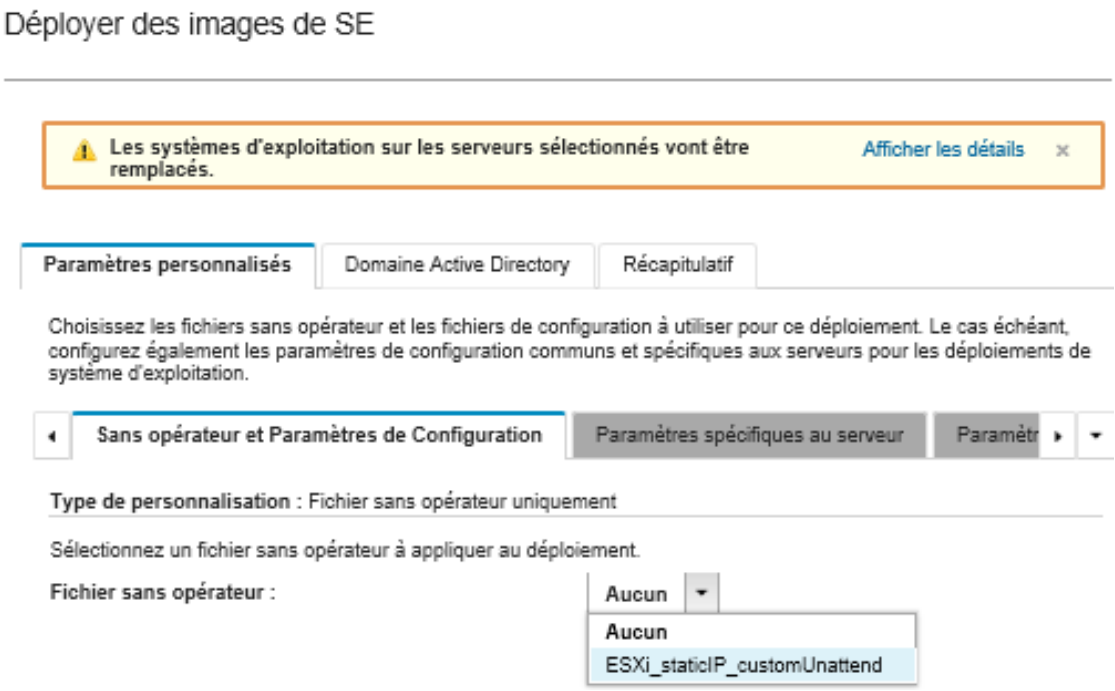
   c. Sélectionnez le profil d'image SE personnalisé (par exemple, <*base_OS*>|<*timestamp*>_ `ESXi personnalisé avec IP statique`) dans la liste déroulante de la colonne **Image à déployer**.

      Remarque : Vérifiez que tous les serveurs cible utilisent le même profil personnalisé.

   d. (Facultatif) Cliquez sur l'icône **Clé de licence** ( ) et indiquez la clé de licence à utiliser pour activer le système d'exploitation une fois qu'il est installé.
   e. Vérifiez que l'état de déploiement du serveur sélectionné est **Prêt**.

Remarque : Étant donné que **--firstdisk = local** est indiqué dans le fichier sans opérateur, vous n'avez pas besoin d'indiquer l'emplacement de stockage préféré dans la colonne **Stockage**. Le paramètre de l'interface utilisateur est ignoré.

3. Sélectionnez tous les serveurs cible, puis cliquez sur l'icône **Déployer l'image** ( ) pour lancer le déploiement du système d'exploitation.
4. Sous l'onglet **Paramètres personnalisés**, cliquez sur le sous-onglet **Paramètres de configuration et sans opérateur**, puis sélectionnez le fichier sans opérateur personnalisé (par exemple, `ESXi_staticIP_customUnattend.cfg`).



5. Sous l'onglet **Récapitulatif**, passez les paramètres en revue.
6. Cliquez sur **Déployer** pour déployer le système d'exploitation.

Déploiement de VMware ESXi v6.7 avec personnalisation Lenovo, des paramètres régionaux configurables et les données d'identification d'un second utilisateur

Ce scénario installe VMware ESXi v6.7 avec un système d'exploitation de personnalisation Lenovo, une langue configurable activée pour les paramètres régionaux du clavier et les données d'identification d'un second utilisateur ESXi. Cet exemple utilise également les paramètres réseau et de stockage de base qui sont définis dans l'interface utilisateur. Un profil d'image SE est utilisé. Il comprend un fichier sans opérateur (avec des macros prédéfinies et des macros personnalisées) et un fichier de paramètres de configuration permettant de sélectionner le mot de passe. Ce profil personnalisé peut être sélectionné sur la page Déployer des images de SE. Ensuite, le mot de passe peut être spécifié sous l'onglet **Paramètres personnalisés**. La valeur spécifiée est remplacée par la macro personnalisée du fichier sans opérateur personnalisé et le programme d'installation ESXi utilise ces valeurs dans le fichier sans opérateur pour configurer le système d'exploitation.

Avant de commencer

Ce scénario utilise les modèles de fichiers suivants.

- ESXi_locale_customConfig.json. Ce fichier de configuration personnalisé invite à entrer les paramètres régionaux de clavier et les données d'identification du second utilisateur ESXi.
- ESXi_locale_customUnattend.cfg. Ce fichier sans opérateur personnalisé utilise les valeurs de macros prédéfinies et de macros personnalisées qui sont définies dans le fichier de configuration.

Procédure

Pour déployer VMware ESXi v6.7 à l'aide d'un profil d'image SE personnalisé, procédez comme suit.

Etape 1. Téléchargez le système d'exploitation VMware vSphere® Hypervisor (ESXi) avec personnalisation Lenovo à partir du Support VMware - Site Web de téléchargement site Web Red Hat sur le système local, puis importez l'image dans le référentiel d'images SE. Pour plus d'informations, voir Importation d'images du système d'exploitation.

1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Gérer les images de SE** pour afficher la page Déployer un système d'exploitation : déployer des images de SE.
2. Cliquez sur l'onglet **Images SE**.
3. Cliquez sur l'icône **Importer** ().
4. Cliquez sur **Importation locale**.
5. Cliquez sur **Parcourir** pour rechercher et sélectionner l'image ESXi à importer (par exemple, `ESXi6.7-7535516-RC-Lenovo_20180126_Async.iso`).
6. Cliquez sur **Importer** pour charger l'image dans le référentiel des images SE.
7. Attendez la fin de l'importation.

Etape 2. Créer un fichier de paramètres de configuration personnalisé et importez-le dans le référentiel d'images SE.

Le fichier de paramètres de configuration est un fichier JSON qui décrit les données à collecter dynamiquement pendant le processus de déploiement SE. Dans ce scénario, nous souhaitons choisir les paramètres régionaux de clavier ainsi que l'ID utilisateur et le mot de passe utilisateur ESXi d'un second utilisateur pour chaque déploiement SE. Pour plus d'informations sur la création d'un fichier de paramètres de configuration, voir Macros personnalisées.

Pour importer le fichier de paramètres de configuration, procédez comme suit. Pour plus d'informations, voir Importation de paramètres de configuration personnalisés.

1. Cliquez sur l'onglet **Fichiers de configuration**.
2. Cliquez sur l'icône **Importer** ().
3. Cliquez sur **Importation locale**.
4. Sélectionnez `ESXi` comme système d'exploitation.
5. Cliquez sur **Parcourir** pour rechercher et sélectionner le fichier de paramètres de configuration à importer (par exemple, `ESXi_locale_customConfig.json`).
6. Cliquez sur **Importer** pour charger le fichier dans le référentiel des images SE.

   Remarque : Lorsque vous importez un fichier de paramètres de configuration personnalisé, XClarity Administratorgénère des macros personnalisées pour chaque paramètre du fichier. Vous pouvez ajouter ces macros au fichier sans opérateur. Pendant le déploiement SE, les macros sont remplacées par des valeurs réelles.

Etape 3. Modifiez le fichier sans opérateur ESXi (kickstart) pour spécifier les paramètres régionaux du système d'exploitation, les paramètres régionaux du clavier et les données d'identification utilisateur pour le second utilisateur ESXi, puis importez le fichier personnalisé dans le référentiel d'images SE. Pour plus d'informations, voir Importation de fichiers sans opérateur personnalisés.

Ajoutez des commandes pour définir les paramètres régionaux du clavier, par exemple :

```
# Set the keyboard locale
keyboard ''
```

Ajoutez des commandes pour créer un second utilisateur ESXi. Dans l'exemple suivant, *<user_id>* et *<password>* sont remplacés par des macros personnalisés à l'étape suivante.

```
#Create second user
/usr/lib/vmware/auth/bin/adduser -D -h /tmp <user_id>
echo <password> | /usr/lib/vmware/auth/bin/passwd <user_id> --stdin
/bin/vim-cmd vimsvc/auth/entity_permission_add vim.Folder:ha-folder-root <user_id> false Admin true
```

Pour importer le fichier sans opérateur personnalisé, procédez comme suit.

1. Cliquez sur l'onglet **Fichiers sans opérateur**.
2. Cliquez sur l'icône **Importer** ().
3. Cliquez sur **Importation locale**.
4. Sélectionnez `ESXi` comme système d'exploitation.
5. Cliquez sur **Parcourir** pour rechercher et sélectionner le fichier sans opérateur à importer (par exemple, `ESXi_locale_customUnattend.cfg`).
6. Cliquez sur **Importer** pour charger le fichier dans le référentiel des images SE.

Etape 4. Associez le fichier sans opérateur personnalisé avec le fichier de paramètres de configuration personnalisé, et ajoutez les macros prédéfinies et personnalisées (de paramètres) requises au fichier sans opérateur à partir du fichier de paramètres de configuration. Pour plus d'informations, voir Association d'un fichier sans opérateur à un fichier de paramètres de configuration, Injection de macros prédéfinies et de macros personnalisées dans un fichier sans opérateur.

Astuce :

- Vous pouvez éventuellement associer le fichier sans opérateur personnalisé au fichier de paramètres de configuration personnalisé et ajouter des macros lors de l'importation du fichier sans opérateur
- XClarity Administrator fournit certaines macros de base, par exemple l'injection de pilotes OOB, la génération de rapports d'état, des scripts de post-installation et des logiciels personnalisés. Toutefois, pour tirer parti de ces macros prédéfinies, vous devez spécifier les macros suivantes dans le fichier sans opérateur personnalisé. Le fichier exemple contient déjà les macros requises. Notez que comme la section %firstboot est incluse, l'ordre de ces macros prédéfinies a de l'importance. Pour plus d'informations, voir Importation de fichiers sans opérateur personnalisés.
  ```
  #predefined.unattendSettings.preinstallConfig#
  #predefined.unattendSettings.postinstallConfig#
  ```
- XClarity Administrator offre également des macros qui injectent des paramètres réseau et d'emplacement de stockage qui sont définis dans l'interface utilisateur. Ces macros sont utiles uniquement lorsque des paramètres de base sont nécessaires pour le déploiement. Le fichier exemple contient déjà les macros requises.
  ```
  #predefined.unattendSettings.networkConfig#
  #predefined.unattendSettings.storageConfig#
  ```

Pour plus d'informations sur l'ajout de macros dans les fichiers sans opérateur, voir Injection de macros prédéfinies et de macros personnalisées dans un fichier sans opérateur. Pour plus d'informations sur les macros prédéfinies disponibles, voir Macros prédéfinies.

Pour ajouter le fichier sans opérateur personnalisé au fichier de paramètres de configuration personnalisé, procédez comme suit.

1. À partir de l'onglet **Fichiers sans opérateur**, sélectionnez le fichier sans opérateur personnalisé (par exemple, `ESXi_locale_customUnattend.cfg`).
2. Cliquez sur l'icône **Associer un fichier de configuration** () pour afficher la boîte de dialogue Associer un fichier sans opérateur.

3. Sélectionnez le fichier de paramètres de configuration à associer au fichier sans opérateur (par exemple, `ESXi_locale_customConfig`).
4. Sélectionnez **Personnalisée** à partir de la liste déroulante **Macros disponibles**.
5. Ajoutez la macro personnalisée pour spécifier les paramètres régionaux de clavier, en plaçant le curseur entre guillemets après le clavier, puis en cliquant sur **keyboard_locale**.

   Par exemple :

   ```
   # Set the keyboard locale
   keyboard '#keyboard_locale#'
   ```

6. Ajoutez la macro personnalisée pour spécifier le second ID de l'utilisateur en plaçant le curseur à l'adresse de chaque emplacement souhaité pour ajouter l'ID utilisateur, puis en cliquant sur **second_user_id**. Dans l'exemple de fichier, remplacez chaque occurrence de <*user_id*> par la macro personnalisée.

   Par exemple :

   ```
   #Create second user
   /usr/lib/vmware/auth/bin/adduser -D -h /tmp #second_user_id#
   echo <password> | /usr/lib/vmware/auth/bin/passwd #second_user_id# --stdin
   /bin/vim-cmd vimsvc/auth/entity_permission_add vim.Folder:ha-folder-root #second_user_id# false Admin true
   ```

7. Ajoutez la macro personnalisée pour spécifier le mot de passe du second utilisateur en plaçant le curseur à l'emplacement souhaité pour ajouter le mot de passe, puis en cliquant sur **second_user_password**. Dans l'exemple de fichier, remplacez <*password*> par la macro personnalisée.

   Par exemple :

   ```
   #Create second user
   /usr/lib/vmware/auth/bin/adduser -D -h /tmp #second_user_id#
   echo #second_user_password# | /usr/lib/vmware/auth/bin/passwd #second_user_id# --stdin
   /bin/vim-cmd vimsvc/auth/entity_permission_add vim.Folder:ha-folder-root #second_user_id# false Admin true
   ```

8. Cliquez sur **Associer** pour lier les fichiers ensemble et enregistrer les modifications apportées au fichier sans opérateur.

Etape 5. Créez un profil d'image SE personnalisé qui inclut les paramètres de configuration personnalisés et les fichiers sans opérateur. Pour plus d'informations, voir Création d'un profil d'image SE personnalisé.

1. Cliquez sur l'onglet **Images SE**.
2. Sélectionnez un profil d'image SE à personnaliser (par exemple, `Virtualization`).
3. Cliquez sur l'icône **Créer** ( ) pour afficher la boîte de dialogue Créer un profil personnalisé.
4. Sur l'onglet **Général** :
   a. Entrez un nom pour le profil (par exemple, `ESXi personnalisé utilisant les paramètres régionaux personnalisés et les données d'identification d'un second utilisateur`).
   b. Utilisez la valeur par défaut pour la zone **Chemin d'accès des données et des fichiers personnalisés**.
   c. Sélectionnez **Fichiers de paramètres configuration et sans opérateur associés** comme type de personnalisation.
   d. Cliquez sur **Suivant**.
5. Sous l'onglet **Fichiers sans opérateur**, sélectionnez le fichier sans opérateur personnalisé (par exemple, `ESXi_locale_customUnattend.cfg`), puis cliquez sur **Suivant**.

   Le fichier de paramètres de configuration associé est sélectionné automatiquement.
6. Sous l'onglet **Récapitulatif**, passez les paramètres en revue.
7. Cliquez sur **Personnaliser** pour créer le profil d'image SE personnalisé.

Etape 6. Déployez le profil d'image SE personnalisé sur le serveur cible. Pour plus d'informations, voir Déploiement d'une image du système d'exploitation.

1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Déployer des images SE** pour afficher la page Déployer un système d'exploitation : déployer des images SE.
2. Pour chacun des serveurs cible :
   a. Sélectionnez le serveur.
   b. Cliquez sur **Modifier la sélection → Paramètres réseau**, puis indiquez le nom d'hôte, l'adresse IP, les paramètres DNS, MTU et VLAN pour le serveur.

      Astuce :

      - Les paramètres VLAN sont disponibles uniquement lorsque le mode VLAN est défini dans **Paramètres globaux → Affectation d'IP → Utiliser les réseaux VLAN**.
      - Les paramètres réseau que vous spécifiez dans la boîte de dialogue Paramètres réseau sont ajoutés au fichier sans opérateur au moment de l'exécution à l'aide de la macro **#predefined.hostPlatforms.networkConfig#**.

   c. Sélectionnez le profil d'image SE personnalisé (par exemple, <*base_OS*>|<*timestamp*>_`ESXi personnalisé utilisant les paramètres régionaux personnalisés et les données d'identification d'un second utilisateur`) dans la liste déroulante de la colonne **Image à déployer**.

      Remarque : Vérifiez que tous les serveurs cible utilisent le même profil personnalisé.

   d. (Facultatif) Cliquez sur l'icône **Clé de licence** () et indiquez la clé de licence à utiliser pour activer le système d'exploitation une fois qu'il est installé.
   e. Sélectionnez l'emplacement de stockage préféré sur lequel vous souhaitez déployer l'image du système d'exploitation dans la colonne **Stockage**.

      Remarques :

      - Pour faire en sorte que les déploiements de système d'exploitation aboutissent, déconnectez toutes les unités de stockage du serveur géré, à l'exception de l'unité de stockage qui a été choisie pour le déploiement du système d'exploitation.
      - Les paramètres de stockage que vous spécifiez dans la boîte de dialogue Paramètres de stockage sont ajoutés au fichier sans opérateur au moment de l'exécution à l'aide de la macro **#predefined.hostPlatforms.storageConfig#**.

   f. Vérifiez que l'état de déploiement du serveur sélectionné est **Prêt**.
3. Sélectionnez tous les serveurs cible, puis cliquez sur l'icône **Déployer l'image** () pour lancer le déploiement du système d'exploitation.
4. Sous l'onglet **Paramètres personnalisés**, cliquez sur le sous-onglet **Paramètres de configuration et sans opérateur**, puis sélectionnez le fichier de paramètres de configuration personnalisé (par exemple, `ESXi_locale_customConfig`).

   Remarque : Le fichier sans opérateur personnalisé associé est sélectionné automatiquement.

5. Sous le sous-onglet **Paramètres spécifiques au serveur**, sélectionnez les paramètre régionaux du clavier ainsi que les données d'identification du second utilisateur ESXi.
6. Sous l'onglet **Récapitulatif**, passez les paramètres en revue.
7. Cliquez sur **Déployer** pour déployer le système d'exploitation.

Déploiement de Windows 2016 avec des fonctions personnalisées

Ce scénario installe le système d'exploitation Windows 2016 et plusieurs fonctions supplémentaires. Un profil personnalisé comprenant un fichier sans opérateur personnalisé est utilisé. Ce profil personnalisé peut ensuite être sélectionné sur la page Déployer des images de SE.

Avant de commencer

Ce scénario utilise les modèles de fichiers suivants.

- Windows_installFeatures_customUnattend.xml. Ce fichier sans opérateur personnalisé installe les fonctions WindowsMediaPlayer et BitLocker, puis il utilise les macros prédéfinies pour les valeurs dynamiques.

Procédure

Pour déployer Windows 2016 avec des fonctions personnalisées, procédez comme suit.

Etape 1. Téléchargez la version japonaise du système d'exploitation Windows 2016 sur le système local, puis importez l'image dans le référentiel d'images SE. Pour plus d'informations, voir Importation d'images du système d'exploitation.

1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Gérer les images de SE** pour afficher la page Déployer un système d'exploitation : déployer des images de SE.
2. Cliquez sur l'onglet **Images SE**.
3. Cliquez sur l'icône **Importer** ( ).
4. Cliquez sur **Importation locale**.

5. Cliquez sur **Parcourir** pour rechercher et sélectionner l'image SE que vous souhaitez importer (par exemple, `ja_windows_server_2016_x64_dvd_9720230.iso`).
6. Cliquez sur **Importer** pour charger l'image dans le référentiel des images SE.
7. Attendez la fin de l'importation. Cette opération peut prendre un certain temps.

Etape 2. Téléchargez le fichier de lot pour Windows 2016 sur le système local, puis importez l'image dans le référentiel d'images SE. Pour plus d'informations, voir Importation de pilotes de périphérique.

Le fichier de lot contient les pilotes de périphérique et les fichiers d'amorçage de WinPE les plus récents que vous pouvez ajouter à vos profils d'images SE personnalisés. Ce scénario utilise un fichier d'amorçage personnalisé, de sorte que le fichier d'amorçage du lot n'est pas utilisé.

1. Cliquez sur l'onglet **Fichiers du pilote**.
2. Cliquez sur **Téléchargements → Fichiers de lots Windows** pour accéder à la page Web de Support Lenovo et télécharger le fichier de lot pour Windows 2016 sur le système local.
3. Cliquez sur l'icône **Importer** ().
4. Cliquez sur **Importation locale**.
5. Cliquez sur **Parcourir** pour rechercher et sélectionner l'image SE que vous souhaitez importer (par exemple, `bundle_win2016_20180126130051.zip`).
6. Cliquez sur **Importer** pour charger le fichier dans le référentiel des images SE.
7. Attendez la fin de l'importation. Cette opération peut prendre un certain temps.

Etape 3. Modifiez le fichier sans opérateur pour installer les fonctions supplémentaires (comme WindowsMediaPlayer et BitLocker), puis importez le fichier personnalisé dans le référentiel d'images SE.

Dans la section « servicing » du fichier sans opérateur de Windows, ajoutez les fonctions Windows à installer, par exemple

```
<servicing>
  <package action="configure">
   <assemblyIdentity name="Microsoft-Windows-Foundation-Package" version="10.0.14393.0"
            processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
            language=""></assemblyIdentity>
   <selection name="Microsoft-Hyper-V" state="true"></selection>
   <selection name="MultipathIo" state="true"></selection>
   <selection name="FailoverCluster-PowerShell" state="true"></selection>
   <selection name="FailoverCluster-FullServer" state="true"></selection>
   <selection name="FailoverCluster-CmdInterface" state="true"></selection>
   <selection name="FailoverCluster-AutomationServer" state="true"></selection>
   <selection name="FailoverCluster-AdminPak" state="true"></selection>
   <selection name="MicrosoftWindowsPowerShellRoot" state="true"></selection>
   <selection name="MicrosoftWindowsPowerShell" state="true"></selection>
   <selection name="ServerManager-Core-RSAT" state="true"></selection>
      <selection name="WindowsMediaPlayer" state="true"></selection>
      <selection name="BitLocker" state="true"></selection>
  </package>
</servicing>
```

Remarques :

- Ces balises sont dans l'exemple de fichier sans opérateur.
- Lorsque vous utilisez un fichier sans opérateur personnalisé, XClarity Administrator n'offre pas la plupart des fonctionnalités normales dont vous bénéficiez lorsque vous utilisez un fichier sans opérateur prédéfini. Par exemple, les cibles `<DiskConfiguration>`, `<ImageInstall>`, `<ProductKey>` et `<UserAccounts>` pour l'administrateur, `<Interfaces>` pour le réseau, et la liste `<package>` pour

les fonctionnalités d'installation doivent être spécifiées dans le fichier sans opérateur personnalisé qui est en cours de téléchargement.

Pour importer le fichier sans opérateur personnalisé, procédez comme suit. Pour plus d'informations, voir Importation de fichiers sans opérateur personnalisés.

1. Cliquez sur l'onglet **Fichiers sans opérateur**.
2. Cliquez sur l'icône **Importer** ().
3. Cliquez sur **Importation locale**.
4. Sélectionnez `Windows` comme système d'exploitation.
5. Cliquez sur **Parcourir** pour rechercher et sélectionner le fichier sans opérateur personnalisé (par exemple, `Windows_installFeatures_customUnattend.xml`).
6. Cliquez sur **Importer** pour charger le fichier dans le référentiel des images SE.

XClarity Administrator fournit certaines macros de base, par exemple l'injection de pilotes OOB, la génération de rapports d'état, des scripts de post-installation, ainsi que des logiciels personnalisés. Toutefois, pour tirer parti de ces macros prédéfinies, vous devez spécifier les macros suivantes dans le fichier sans opérateur personnalisé.

- `#predefined.unattendSettings.preinstallConfig#`
- `#predefined.unattendSettings.postinstallConfig#`

Le modèle de fichier contient déjà le code pour l'installation des fonctions supplémentaires, des macros requises, ainsi que des autres macros qui sont nécessaires pour la saisie dynamique. Pour plus d'informations sur l'ajout de macros dans les fichiers sans opérateur, voir Injection de macros prédéfinies et de macros personnalisées dans un fichier sans opérateur.

Pour plus d'informations sur les macros prédéfinies disponibles, voir Macros prédéfinies.

Etape 4. Créez un profil d'image SE personnalisé qui inclut le fichier sans opérateur. Pour plus d'informations, voir Création d'un profil d'image SE personnalisé.

1. Cliquez sur l'onglet **Images SE**.
2. Sélectionnez le profil à personnaliser (par exemple, `win2016-x86_64-install-Datacenter_Virtualization`).
3. Cliquez sur l'icône **Créer** () pour afficher la boîte de dialogue Créer un profil personnalisé.
4. Sur l'onglet **Général** :
   a. Entrez un nom pour le profil (par exemple, `Windows personnalisé avec des fonctions`).
   b. Utilisez la valeur par défaut pour la zone **Chemin d'accès des données et des fichiers personnalisés**.
   c. Sélectionnez **Fichiers sans opérateur uniquement** comme type de personnalisation.
   d. Cliquez sur **Suivant**.
5. Sous l'onglet **Options de pilote**, cliquez sur **Suivant** . Les pilotes d'appareil fournis par Windows sont inclus par défaut.
6. Sous l'onglet **Options d'amorçage**, cliquez sur **Suivant**. Le fichier d'amorçage WinPE prédéfini est sélectionné par défaut.
7. Sous l'onglet **Software**, cliquez sur **Suivant**.
8. Sous l'onglet **Fichiers sans opérateur**, sélectionnez des fichiers sans opérateur personnalisés (par exemple, `Windows_installFeatures_customUnattend.xml`), puis cliquez sur **Suivant**.
9. Sous l'onglet **Scripts d'installation**, cliquez sur **Suivant**.
10. Sous l'onglet **Récapitulatif**, passez les paramètres en revue.

11. Cliquez sur **Personnaliser** pour créer le profil d'image SE personnalisé.

Etape 5. Déployez le profil d'image SE personnalisé sur les serveurs cible. Pour plus d'informations, voir Déploiement d'une image du système d'exploitation.

1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Déployer des images SE** pour afficher la page Déployer un système d'exploitation : déployer des images SE.
2. Pour chacun des serveurs cible :
   a. Sélectionnez le serveur.
   b. Cliquez sur **Modifier la sélection → Paramètres réseau**, puis indiquez le nom d'hôte, l'adresse IP, le masque de sous-réseau, la passerelle, les paramètres DNS, MTU et VLAN pour le serveur.

      Astuce : Les paramètres VLAN sont disponibles uniquement lorsque le mode VLAN est défini dans **Paramètres globaux → Affectation d'IP → Utiliser les réseaux VLAN**.
   c. Sélectionnez le profil d'image SE personnalisé (par exemple, *<base_OS>*|*<timestamp>*_`Windows personnalisé avec des fonctions`) dans la liste déroulante de la colonne **Image à déployer**.

      Remarque : Vérifiez que tous les serveurs cible utilisent le même profil personnalisé.
   d. (Facultatif) Cliquez sur l'icône **Clé de licence** () et indiquez la clé de licence à utiliser pour activer le système d'exploitation une fois qu'il est installé.
   e. Sélectionnez l'emplacement de stockage préféré sur lequel vous souhaitez déployer l'image du système d'exploitation dans la colonne **Stockage**.

      Remarque : Pour faire en sorte que les déploiements de système d'exploitation aboutissent, déconnectez toutes les unités de stockage du serveur géré, à l'exception de l'unité de stockage qui a été choisie pour le déploiement du système d'exploitation
   f. Vérifiez que l'état de déploiement du serveur sélectionné est **Prêt**.
3. Sélectionnez tous les serveurs cible, puis cliquez sur l'icône **Déployer l'image** () pour lancer le déploiement du système d'exploitation.
4. Sous l'onglet **Paramètres personnalisés**, cliquez sur le sous-onglet **Paramètres de configuration et sans opérateur**, puis sélectionnez le fichier sans opérateur personnalisé (par exemple, `Windows_installFeatures_customUnattend.xml`).
5. (Facultatif) Dans l'onglet **Domaine Active Directory**, indiquez les informations pour rejoindre un domaine Active Directory dans le cadre d'un déploiement d'image Windows (voir Intégration à Windows Active Directory).
6. Sous l'onglet **Récapitulatif**, passez les paramètres en revue.
7. Cliquez sur **Déployer** pour déployer le système d'exploitation.

Déploiement de Windows 2016 avec des logiciels personnalisés

Ce scénario installe le système d'exploitation Windows 2016 avec des logiciels personnalisés (Java et Eclipse IDE). Un profil personnalisé comprenant les logiciels personnalisés et les scripts post-installation d'installation et de configuration des logiciels personnalisés. Les modules logiciels personnalisés sont copiés sur l'hôte lors du déploiement, puis mis à disposition pour le script de post-installation personnalisé.

Avant de commencer

Ce scénario utilise les modèles de fichiers suivants.

- jre-8u151-windows-x64-with-configfile.zip. Il s'agit du fichier d'installation pour Java pour Eclipse.

- eclipse-java-oxygen-1a-win32-x86_64.zip Il s'agit du fichier d'installation pour l'environnement de développement Eclipse.
- Windows_installSoftware_customScript.ps1 Ce script de post-installation crée un utilisateur pour le lancement d'Eclipse, puis il installe l'environnement de développement Eclipse et Java.

Remarques :

- Les scripts d'installation Windows se présentent sous l'un des formats suivants : Fichier de commande (. cmd), PowerShell (.ps1)
- Les fichiers logiciels et les scripts d'installation sont installés à partir du chemin de données et de fichiers personnalisé que vous spécifiez lors du déploiement. Le chemin d'accès aux fichiers et données personnalisés par défaut est `C:\lxca`.

Procédure

Pour déployer Windows 2016 avec des logiciels personnalisés, procédez comme suit.

Etape 1. Téléchargez la version japonaise du système d'exploitation Windows 2016 sur le système local, puis importez l'image dans le référentiel d'images SE. Pour plus d'informations, voir Importation d'images du système d'exploitation.

1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Gérer les images de SE** pour afficher la page Déployer un système d'exploitation : déployer des images de SE.
2. Cliquez sur l'onglet **Images SE**.
3. Cliquez sur l'icône **Importer** ( ).
4. Cliquez sur **Importation locale**.
5. Cliquez sur **Parcourir** pour rechercher et sélectionner l'image SE que vous souhaitez importer (par exemple, `ja_windows_server_2016_x64_dvd_9720230.iso`).
6. Cliquez sur **Importer** pour charger l'image dans le référentiel des images SE.
7. Attendez la fin de l'importation. Cette opération peut prendre un certain temps.

Etape 2. Téléchargez le fichier de lot pour Windows 2016 sur le système local, puis importez l'image dans le référentiel d'images SE. Pour plus d'informations, voir Importation de pilotes de périphérique.

Le fichier de lot contient les pilotes de périphérique et les fichiers d'amorçage de WinPE les plus récents que vous pouvez ajouter à vos profils d'images SE personnalisés. Ce scénario utilise un fichier d'amorçage personnalisé, de sorte que le fichier d'amorçage du lot n'est pas utilisé.

1. Cliquez sur l'onglet **Fichiers du pilote**.
2. Cliquez sur **Téléchargements → Fichiers de lots Windows** pour accéder à la page Web de Support Lenovo et télécharger le fichier de lot pour Windows 2016 sur le système local.
3. Cliquez sur l'icône **Importer** ( ).
4. Cliquez sur **Importation locale**.
5. Cliquez sur **Parcourir** pour rechercher et sélectionner l'image SE que vous souhaitez importer (par exemple, `bundle_win2016_20180126130051.zip`).
6. Cliquez sur **Importer** pour charger le fichier dans le référentiel des images SE.
7. Attendez la fin de l'importation. Cette opération peut prendre un certain temps.

Etape 3. Téléchargez le logiciel personnalisé sur le système local et importez les fichiers dans le référentiel d'images SE. Pour plus d'informations, voir Importation de logiciels personnalisés.

1. Cliquez sur l'onglet **Logiciels**.

2. Cliquez sur l'icône **Importer** ().
3. Cliquez sur **Importation locale**.
4. Sélectionnez `Windows` comme système d'exploitation.
5. Cliquez sur **Parcourir** pour rechercher et sélectionner le fichier de paramètres de configuration à importer (par exemple, `jre-8u151-windows-x64-with-configfile.zip`).
6. Cliquez sur **Importer** pour charger le fichier dans le référentiel des images SE.
7. Cliquez de nouveau sur l'icône **Importer** ().
8. Cliquez sur **Importation locale**.
9. Sélectionnez `Windows` comme système d'exploitation.
10. Cliquez sur **Parcourir** pour rechercher et sélectionner le fichier de paramètres de configuration à importer (par exemple, `eclipse-java-oxygen-1a-win32-x86_64.zip`).
11. Cliquez sur **Importer** pour charger le fichier dans le référentiel des images SE.

Etape 4. Créez un script de post-installation personnalisé et importez le fichier dans le référentiel d'images SE.

Ajoutez les commandes pour installer le logiciel, par exemple :

```
Write-Output "Install Java...."
Invoke-Command -ScriptBlock
        {#predefined.otherSettings.deployDataAndSoftwareLocation#\jre-8u151-windows-x64.exe
        [INSTALLCFG=#predefined.otherSettings.deployDataAndSoftwareLocation#\java_configfile.cfg]
        /s}

Write-Output "Install Eclipse..."
$eclipseDir="C:\Users\Administrator\Desktop\eclipse"
New-Item -ItemType directory -Path $eclipseDir
Expand-Archive -LiteralPath
        "#predefined.otherSettings.deployDataAndSoftwareLocation#\eclipse-java-oxygen-1a-win32-x86_64.zip"
        -DestinationPath $eclipseDir
```

Notez que ces commandes utilisent la macro prédéfinie pour le chemin d'accès aux fichiers de données et logiciels extraits (**predefined.otherSettings.deployDataAndSoftwareLocation**).

Vous pouvez également ajouter des commandes pour envoyer des messages personnalisés aux travaux qui se connectent dans XClarity Administrator, comme illustré dans le modèle de fichier. Pour plus d'informations, voir Ajout de rapport d'état personnalisé aux scripts d'installation.

Pour importer le script d'installation personnalisé, procédez comme suit. Pour plus d'informations, voir Importation de scripts d'installation personnalisés

1. Cliquez sur l'onglet **Scripts d'installation**.
2. Cliquez sur l'icône **Importer** ().
3. Cliquez sur **Importation locale**.
4. Sélectionnez `Windows` comme système d'exploitation.
5. Cliquez sur **Parcourir** pour rechercher et sélectionner le fichier sans opérateur à importer (par exemple, `Windows_installSoftware_customScript.ps1`).
6. Cliquez sur **Importer** pour charger le fichier dans le référentiel des images SE.

Etape 5. Créez un profil d'image SE personnalisé qui inclut le fichier sans opérateur personnalisé. Pour plus d'informations, voir Création d'un profil d'image SE personnalisé.

1. Cliquez sur l'onglet **Images SE**.

2. Sélectionnez un profil d'image SE à personnaliser (par exemple, `Datacenter virtualization`).
3. Cliquez sur l'icône **Créer** () pour afficher la boîte de dialogue Créer un profil personnalisé.
4. Sur l'onglet **Général** :
   a. Entrez un nom pour le profil (par exemple, `Windows personnalisé avec des logiciels`).
   b. Utilisez la valeur par défaut pour la zone **Chemin d'accès des données et des fichiers personnalisés**.
   c. Sélectionnez **Aucun** comme type de personnalisation.
   d. Cliquez sur **Suivant**.
5. Sous l'onglet **Options de pilote**, cliquez sur **Suivant** . Les pilotes d'appareil fournis par Windows sont inclus par défaut.
6. Sous l'onglet **Options d'amorçage**, cliquez sur **Suivant**. Le fichier d'amorçage WinPE prédéfini est sélectionné par défaut.
7. Sous l'onglet **Logiciels**, sélectionnez les fichiers d'installation des logiciels (par exemple `jre-8u151-windows-x64-with-configfile.zip` et `eclipse-java-oxygen-1a-win32-x86_64.zip`), puis cliquez sur **Suivant**.
8. Sous l'onglet **Scripts d'installation**, sélectionnez les scripts d'installation (par exemple, `Windows_installSoftware_customScript.ps1`), puis cliquez sur **Suivant**.
9. Sous l'onglet **Récapitulatif**, passez les paramètres en revue.
10. Cliquez sur **Personnaliser** pour créer le profil d'image SE personnalisé.

Etape 6. Déployez le profil d'image SE personnalisé sur les serveurs cible. Pour plus d'informations, voir Déploiement d'une image du système d'exploitation.

1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Déployer des images SE** pour afficher la page Déployer un système d'exploitation : déployer des images SE.
2. Pour chacun des serveurs cible :
   a. Sélectionnez le serveur.
   b. Cliquez sur **Modifier la sélection → Paramètres réseau**, puis indiquez le nom d'hôte, l'adresse IP, les paramètres DNS, MTU et VLAN pour le serveur.

      Astuce : Les paramètres VLAN sont disponibles uniquement lorsque le mode VLAN est défini dans **Paramètres globaux → Affectation d'IP → Utiliser les réseaux VLAN**.
   c. Sélectionnez le profil d'image SE personnalisé (par exemple, *<base_OS>*|*<timestamp>*_`Windows personnalisé avec des logiciels`) dans la liste déroulante de la colonne **Image à déployer**

      Remarque : Vérifiez que tous les serveurs cible utilisent le même profil personnalisé.
   d. (Facultatif) Cliquez sur l'icône **Clé de licence** () et indiquez la clé de licence à utiliser pour activer le système d'exploitation une fois qu'il est installé.
   e. Sélectionnez l'emplacement de stockage préféré sur lequel vous souhaitez déployer l'image du système d'exploitation dans la colonne **Stockage**.

      Remarque : Pour faire en sorte que les déploiements de système d'exploitation aboutissent, déconnectez toutes les unités de stockage du serveur géré, à l'exception de l'unité de stockage qui a été choisie pour le déploiement du système d'exploitation.
   f. Vérifiez que l'état de déploiement du serveur sélectionné est **Prêt**.
3. Sélectionnez tous les serveurs cible, puis cliquez sur l'icône **Déployer l'image** () pour lancer le déploiement du système d'exploitation.
4. Sous l'onglet **Récapitulatif**, passez les paramètres en revue.

5. Cliquez sur **Déployer** pour déployer le système d'exploitation.

Déploiement de Windows 2016 pour le japonais

Ce scénario installe le système d'exploitation Windows 2016 sur plusieurs serveurs en activant le japonais pour le clavier et les paramètres régionaux du système d'exploitation. Un profil personnalisé comprenant un fichier d'amorçage WinPE personnalisé et sans opérateur est utilisé. Ce profil personnalisé peut ensuite être sélectionné sur la page Déployer des images de SE.

Avant de commencer

Ce scénario utilise les modèles de fichiers suivants.

- `WinPE_64_ja.zip`. Ce fichier d'amorçage Windows personnalisé (WinPE) installe les paramètres régionaux japonais.
- Windows_locale_customUnattend.xml. Ce fichier sans opérateur personnalisé utilise le fichier WinPE pour installer le japonais.

Remarques : L'exemple de fichier sans opérateur personnalisé suppose ce qui suit :

- Le serveur comporte un seul disque visible (0) et il n'a pas déjà de partition système.
- Le mode IPv4 statique est utilisé et il définit une adresse IP statique (qui est utilisée dans le fichier sans opérateur personnalisé comme macro prédéfinie).

Procédure

Pour déployer la version japonaise de Windows 2016 sur des serveurs cible à l'aide d'un profil d'image SE personnalisé, procédez comme suit.

Etape 1. Téléchargez la version japonaise du système d'exploitation Windows 2016 sur le système local, puis importez l'image dans le référentiel d'images SE. Pour plus d'informations, voir Importation d'images du système d'exploitation.

1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Gérer les images de SE** pour afficher la page Déployer un système d'exploitation : déployer des images de SE.
2. Cliquez sur l'onglet **Images SE**.
3. Cliquez sur l'icône **Importer** ( ).
4. Cliquez sur **Importation locale**.
5. Cliquez sur **Parcourir** pour rechercher et sélectionner l'image SE que vous souhaitez importer (par exemple, `ja_windows_server_2016_x64_dvd_9720230.iso`).
6. Cliquez sur **Importer** pour charger l'image dans le référentiel des images SE.
7. Attendez la fin de l'importation. Cette opération peut prendre un certain temps.

Etape 2. Téléchargez le fichier de lot pour Windows 2016 sur le système local, puis importez l'image dans le référentiel d'images SE. Pour plus d'informations, voir Importation de pilotes de périphérique.

Le fichier de lot contient les pilotes de périphérique et les fichiers d'amorçage de WinPE les plus récents que vous pouvez ajouter à vos profils d'images SE personnalisés. Ce scénario utilise un fichier d'amorçage personnalisé, de sorte que le fichier d'amorçage du lot n'est pas utilisé.

1. Cliquez sur l'onglet **Fichiers du pilote**.
2. Cliquez sur **Téléchargements → Fichiers de lots Windows** pour accéder à la page Web de Support Lenovo et télécharger le fichier de lot pour Windows 2016 sur le système local.
3. Cliquez sur l'icône **Importer** ( ).

4. Cliquez sur **Importation locale**.
5. Cliquez sur **Parcourir** pour rechercher et sélectionner l'image SE que vous souhaitez importer (par exemple, `bundle_win2016_20180126130051.zip`).
6. Cliquez sur **Importer** pour charger le fichier dans le référentiel des images SE.
7. Attendez la fin de l'importation. Cette opération peut prendre un certain temps.

Etape 3. Créez un fichier d'amorçage WinPE personnalisé qui utilise les paramètres régionaux japonais pendant l'installation de WinPE, puis importez le fichier dans le référentiel d'images SE.

XClarity Administrator utilise un fichier d'amorçage de préinstallation Windows (WinPE) prédéfini pour installer le système d'exploitation Windows. Les paramètres régionaux utilisés avec ce fichier d'amorçage prédéfini sont ceux de l'anglais (English [en-US]). Si vous souhaitez modifier les paramètres régionaux utilisés lors de l'installation de Windows, vous pouvez créer un fichier d'amorçage WinPE personnalisé avec les paramètres régionaux de votre choix et affecter ce fichier d'amorçage personnalisé à votre profil personnalisé.

Pour plus d'informations sur l'injection de paramètres régionaux dans WinPE, voir Windows WinPE : Page Web d'ajout de modules.

Important : La spécification de paramètres régionaux autre que l'anglais dans le fichier d'amorçage WinPE ne modifie pas les paramètres régionaux du système d'exploitation final en cours de déploiement. Cela change uniquement les paramètres régionaux qui s'affichent durant l'installation et la configuration de Windows.

Pour créer un fichier d'amorçage WinPE personnalisé qui inclut les paramètres régionaux japonais, procédez comme suit. Pour plus d'informations, voir Création d'un fichier d'amorçage (WinPE).

1. À l'aide d'un ID utilisateur disposant de droits d'administrateur, exécutez la commande Windows ADK « Deployment and Imaging Tools Environment. » Une session de commande s'affiche.
2. Depuis la session de commande, accédez au répertoire contenant les fichiers `genimage.cmd` et `starnet.cmd` téléchargés (par exemple `C:\customwim`).
3. Assurez-vous qu'aucune image préalablement monté ne se trouve sur l'hôte, en exécutant la commande suivante :
   ```
   dism /get-mountedwiminfo
   ```
   S'il y a des images montées, supprimez-les à l'aide de la commande suivante :
   ```
   dism /unmount-wim /MountDir:C:\<mount_path> /Discard
   ```
4. Si vous ajoutez des pilotes de périphérique fournis avec Windows à un profil Windows personnalisé, copiez les fichiers de pilote de périphérique bruts, au format .inf, sur le système hôte dans le répertoire `C:\drivers`.
5. Exécutez la commande suivante pour générer le fichiers d'amorçage, au format .wim, puis patientez quelques minutes le temps que la commande s'exécute.
   ```
   genimage.cmd amd64 <ADK_Version>
   ```
   Où <*ADK_Version*> est l'une des valeurs suivantes.
   - **8.1**. Pour Windows 2012 R2
   - **10**. Pour Windows 2016

   Cette commande crée un fichier d'amorçage nommé `C:\WinPE_64\media\Boot\WinPE_64.wim`.
6. Montez le fichier d'amorçage en exécutant la commande suivante :
   ```
   DISM /Mount-Image /ImageFile:C:\WinPE_64\media\Boot\WinPE_64.wim /index:1 /MountDir:C:\WinPE_64\mount
   ```
7. Si vous ajoutez des pilotes de périphérique non fournis avec Windows directement dans le fichier d'amorçage, procédez comme suit.

a. Créez la structure de répertoire suivante, où <*os_release*> est `2012R2` ou `2016`
`drivers\<os_release>\`

b. Copiez les pilotes de périphérique, au format .inf, dans un répertoire de ce chemin, par exemple :
`drivers\<os_release>\<driver1>\<driver1_files>`

c. Copiez le répertoire `drivers` dans le répertoire de montage, par exemple :
`C:\WinPE_64\mount\drivers`

8. **Facultatif :** Apportez des personnalisations supplémentaires au fichier d'amorçage, comme l'ajout de dossiers, de fichiers, de scripts de démarrage, de modules linguistiques et d'applications. Pour plus d'informations sur la personnalisation des fichiers d'amorçage, consultez le Site Web sur le montage et la personnalisation WinPE.
9. Ajoutez les modules japonais, par exemple.
10. Affichez les logiciels installés pour vous assurer que les modules spécifiques au japonais sont installés.
```
Dism /Add-Package /Image:"C:\WinPE_64\mount"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment
and Deployment Kit\Windows Preinstallation Environment\amd64\WinPE_OCs\ja-jp\lp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-DismCmdlets_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-NetFx_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-PowerShell_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-RNDIS_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-Scripting_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-StorageWMI_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-WDS-Tools_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\ja-jp\WinPE-WMI_ja-jp.cab"
/PackagePath="C:\Program Files (x86)\Windows Kits\10\Assessment and Deployment Kit\Windows
Preinstallation Environment\amd64\WinPE_OCs\WinPE-FontSupport-JA-JP.cab"
```
11. Passez en revue les paramètres internationaux dans l'image.
```
Dism /Get-Packages /Image:"C:\WinPE_64\mount"
```
12. Démontez l'image en exécutant la commande suivante.
```
DISM /Unmount-Image /MountDir:C:\WinPE_64\mount /commit
```
13. Compressez le contenu du répertoire `C:\WinPE_64\media` dans un fichier zip appelé `WinPE_64_ja.zip`.
14. Importez le fichier .zip dans XClarity Administrator (voir Importation de fichiers d'amorçage).
    a. Cliquez sur l'onglet **Fichiers d'amorçage**.
    b. Cliquez sur l'icône **Importer** ( ).
    c. Cliquez sur **Importation locale**.
    d. Sélectionnez `Windows` comme système d'exploitation.
    e. Cliquez sur **Parcourir** pour rechercher et sélectionner le fichier d'amorçage personnalisé (par exemple, `WinPE_64_ja.zip`).
    f. Cliquez sur **Importer** pour charger le fichier dans le référentiel des images SE.

Etape 4. Modifiez le fichier sans opérateur de Windows pour indiquer que le japonais est inclus dans l'image SE, puis importez le fichier personnalisé dans le référentiel d'images SE.

Lors de l'étape « windowsPE » de l'installation Windows, ajoutez le japonais comme langue du système d'exploitation et paramètres régionaux, par exemple :

```
<settings pass="windowsPE">
   <component name="Microsoft-Windows-International-Core-WinPE" processorArchitecture="amd64"
              publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
              xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
              xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <SetupUILanguage>
         <UILanguage>ja-JP</UILanguage>
      </SetupUILanguage>
      <SystemLocale>ja-JP</SystemLocale>
      <UILanguage>ja-JP</UILanguage>
      <UserLocale>ja-JP</UserLocale>
      <InputLocale>0411:00000411</InputLocale>
   </component>
</settings>
```

Remarque : Lorsque vous utilisez un fichier sans opérateur personnalisé, XClarity Administrator n'offre pas la plupart des fonctionnalités normales dont vous bénéficiez lorsque vous utilisez un fichier sans opérateur prédéfini. Par exemple, les cibles `<DiskConfiguration>`, `<ImageInstall>`, `<ProductKey>` et `<UserAccounts>` pour l'administrateur, `<Interfaces>` pour le réseau, et la liste `<package>` pour les fonctionnalités d'installation doivent être spécifiées dans le fichier sans opérateur personnalisé qui est en cours de téléchargement.

XClarity Administrator fournit certaines macros de base, par exemple l'injection de pilotes OOB, la génération de rapports d'état, des scripts de post-installation et des logiciels personnalisés. Toutefois, pour tirer parti de ces macros prédéfinies, vous devez spécifier les macros suivantes dans le fichier sans opérateur personnalisé.

- `#predefined.unattendSettings.preinstallConfig#`
- `#predefined.unattendSettings.postinstallConfig#`

Le fichier exemple contient déjà les macros requises. Pour plus d'informations sur l'ajout de macros dans les fichiers sans opérateur, voir Injection de macros prédéfinies et de macros personnalisées dans un fichier sans opérateur. Pour plus d'informations sur les macros prédéfinies disponibles, voir Macros prédéfinies.

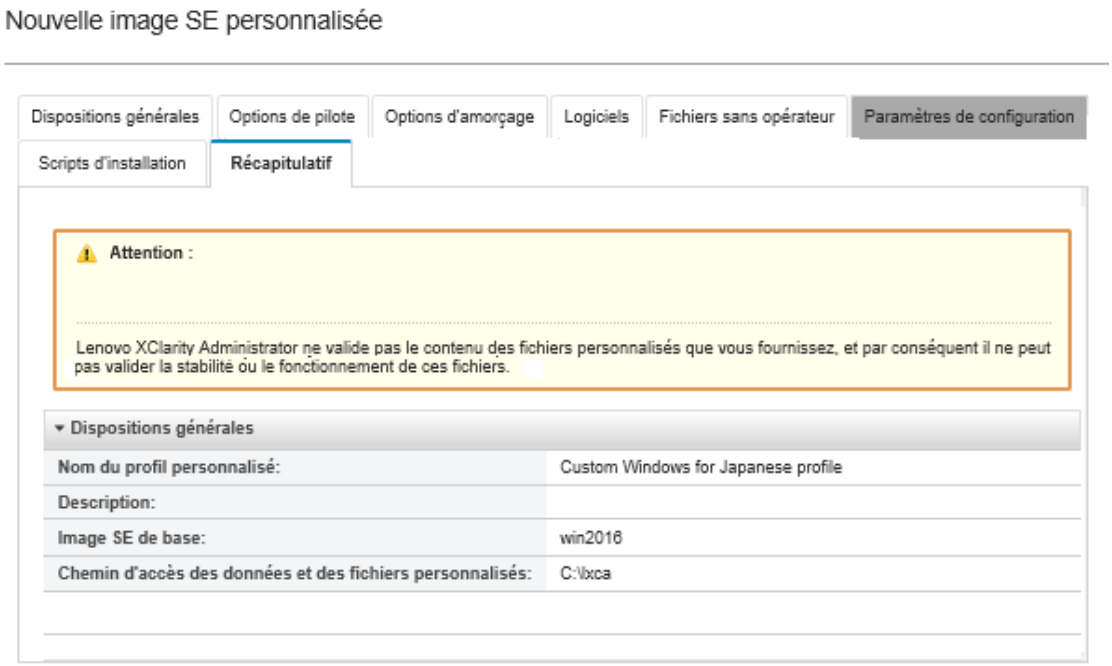
Pour importer le fichier sans opérateur personnalisé, procédez comme suit. Pour plus d'informations, voir Importation de fichiers sans opérateur personnalisés.

1. Cliquez sur l'onglet **Fichiers sans opérateur**.
2. Cliquez sur l'icône **Importer** ( ).
3. Cliquez sur **Importation locale**.
4. Sélectionnez `Windows` comme système d'exploitation.
5. Cliquez sur **Parcourir** pour rechercher et sélectionner le fichier sans opérateur personnalisé (par exemple, `Windows_locale_customUnattend.xml`).
6. Cliquez sur **Importer** pour charger le fichier dans le référentiel des images SE.

Etape 5. Créez un profil d'image SE personnalisé qui inclut le fichier d'amorçage (WinPE) et le fichier sans opérateur personnalisés. Pour plus d'informations, voir Création d'un profil d'image SE personnalisé.

1. Cliquez sur l'onglet **Images SE**.
2. Sélectionnez le profil à personnaliser (par exemple, `win2016-x86_64-install-Datacenter_Virtualization`).
3. Cliquez sur l'icône **Créer** ( ) pour afficher la boîte de dialogue Créer un profil personnalisé.

4. Sur l'onglet **Général** :
   a. Entrez un nom pour le profil (par exemple, `Profil Windows personnalisé pour le japonais`).
   b. Utilisez la valeur par défaut pour la zone **Chemin d'accès des données et des fichiers personnalisés**.
   c. Sélectionnez **Fichiers sans opérateur uniquement** comme type de personnalisation.
   d. Cliquez sur **Suivant**.
5. Sous l'onglet **Options de pilote**, cliquez sur **Suivant** . Les pilotes d'appareil fournis par Windows sont inclus par défaut.
6. Dans l'onglet **Fichiers d'amorçage**, sélectionnez le fichier d'amorçage personnalisé (par exemple, `WinPE_64_ja`), puis cliquez sur **Suivant**.
7. Sous l'onglet **Software**, cliquez sur **Suivant**.
8. Sous l'onglet **Fichiers sans opérateur**, sélectionnez des fichiers sans opérateur personnalisés (par exemple, `Windows_locale_customUnattend.xml`), puis cliquez sur **Suivant**.
9. Sous l'onglet **Scripts d'installation**, cliquez sur **Suivant**.
10. Sous l'onglet **Récapitulatif**, passez les paramètres en revue.



11. Cliquez sur **Personnaliser** pour créer le profil d'image SE personnalisé.

Etape 6. Déployez le profil d'image SE personnalisé sur les serveurs cible. Pour plus d'informations, voir Déploiement d'une image du système d'exploitation.

1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Déployer des images SE** pour afficher la page Déployer un système d'exploitation : déployer des images SE.
2. Pour chacun des serveurs cible :
   a. Sélectionnez le serveur.
   b. Cliquez sur **Modifier la sélection → Paramètres réseau**, puis indiquez le nom d'hôte, l'adresse IP, le masque de sous-réseau, la passerelle, les paramètres DNS, MTU et VLAN pour le serveur.

      Astuce : Les paramètres VLAN sont disponibles uniquement lorsque le mode VLAN est défini dans **Paramètres globaux → Affectation d'IP → Utiliser les réseaux VLAN**.

c. Sélectionnez le profil d'image SE personnalisé (par exemple, *<base_OS>*|*<timestamp>*_`Profil Windows personnalisé pour le japonais`) dans la liste déroulante de la colonne **Image à déployer**.

   Remarque : Vérifiez que tous les serveurs cible utilisent le même profil personnalisé.

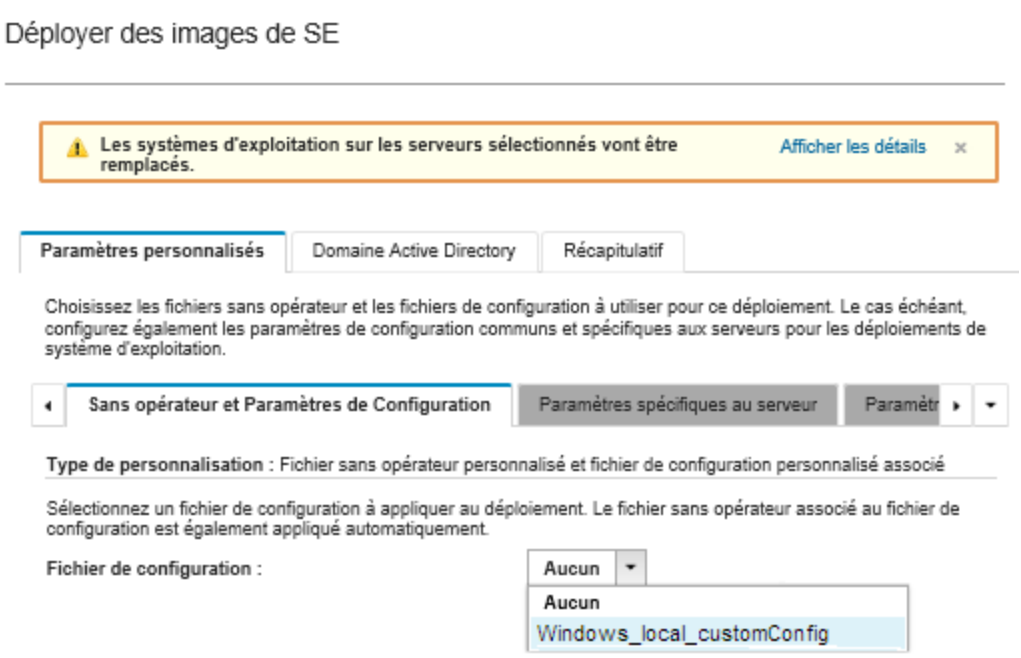
d. (Facultatif) Cliquez sur l'icône **Clé de licence** ( ) et indiquez la clé de licence à utiliser pour activer le système d'exploitation une fois qu'il est installé.

e. Sélectionnez l'emplacement de stockage préféré sur lequel vous souhaitez déployer l'image du système d'exploitation dans la colonne **Stockage**.

   Remarque : Pour faire en sorte que les déploiements de système d'exploitation aboutissent, déconnectez toutes les unités de stockage du serveur géré, à l'exception de l'unité de stockage qui a été choisie pour le déploiement du système d'exploitation.

f. Vérifiez que l'état de déploiement du serveur sélectionné est **Prêt**.

3. Sélectionnez tous les serveurs cible, puis cliquez sur l'icône **Déployer l'image** ( ) pour lancer le déploiement du système d'exploitation.
4. Sous l'onglet **Paramètres personnalisés**, cliquez sur le sous-onglet **Paramètres de configuration et sans opérateur**, puis sélectionnez le fichier sans opérateur personnalisé (par exemple, `Windows_locale_customUnattend.xml`).



5. (Facultatif) Dans l'onglet **Domaine Active Directory**, indiquez les informations pour rejoindre un domaine Active Directory dans le cadre d'un déploiement d'image Windows (voir Intégration à Windows Active Directory).
6. Sous l'onglet **Récapitulatif**, passez les paramètres en revue.
7. Cliquez sur **Déployer** pour déployer le système d'exploitation.

   La boîte de dialogue d'installation Windows s'affiche en japonais.

Une fois l'installation terminée, la page de connexion Windows s'affiche également en japonais.

Chapitre 16. Scénarios de bout en bout pour la configuration de nouveaux appareils

Utilisez ces scénarios de bout en bout pour vous aider à utiliser Lenovo XClarity Administrator pour configurer de nouveaux appareils de manière cohérente et facilement répétitive.

Déploiement d'ESXi sur un disque dur local

Utilisez ces procédures pour déployer VMware ESXi 5.5 sur un disque dur installé localement sur un Nœud de traitement x240 Flex System. Elles montrent comment reconnaître un modèle de serveur à partir d'un serveur existant, modifier le modèle de catégorie des paramètres d'UEFI étendu pour ce modèle de serveur, et installer VMware ESXi.

VMware ESXi 5.5 requiert qu'un espace MMIO (memory-mapped I/O) soit configuré dans les 4 Go initiaux du système. Selon la configuration, certains systèmes tentent d'utiliser une mémoire supérieure à 4 Go, ce qui peut provoquer une défaillance. Pour résoudre ce problème, vous pouvez augmenter la valeur de l'option MM Config à 3 Go via Setup Utility pour chaque serveur sur lequel VMware ESXi 5.5 va être installé.

Une alternative consiste à déployer un modèle de serveur qui contient l'un des modèles de catégorie d'UEFI étendu prédéfinis lié à la virtualisation, ce qui définit l'option MM Config et désactive l'allocation de la ressource PCI 64 bits.

Déploiement d'un modèle de virtualisation prédéfini

Un modèle de catégorie définit des paramètres de microprogramme spécifiques réutilisables par plusieurs modèles de serveur. Pour déployer un modèle de virtualisation prédéfini, vous créez un modèle de serveur, puis vous appliquez un modèle UEFI étendu prédéfini à ce modèle de serveur. Ce modèle de serveur peut ensuite être appliqué à plusieurs serveurs du même type, par exemple, Nœud de traitement x240 Flex System ou Nœud de traitement Flex System x880 X6.

À propos de cette tâche

Lorsque vous créez un modèle de serveur, vous pouvez choisir d'effectuer la configuration vous-même ou d'obtenir les attributs de modèle à partir d'un serveur existant qui est déjà configuré. Lorsque vous obtenez un nouveau modèle à partir d'un serveur existant, la plupart des attributs de modèle sont déjà définis.

Pour plus d'informations sur les modèles de serveur et les modèles de catégorie, voir Utilisation de modèles de serveur.

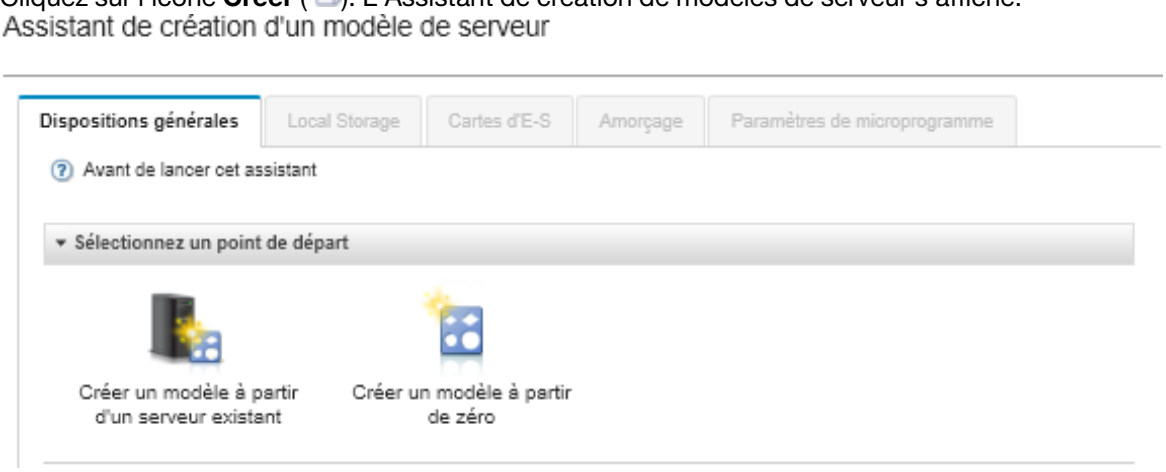
Procédure

Pour obtenir un nouveau modèle à partir d'un serveur existant, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Administrator, cliquez sur **Distribution → Modèles**. La page Modèles de configuration : Modèles s'affiche.

Etape 2. Cliquez sur l'onglet **Modèles de serveur**.

Etape 3. Cliquez sur l'icône **Créer** ( ). L'Assistant de création de modèles de serveur s'affiche.



Etape 4. Cliquez sur **Créer un modèle à partir d'un serveur existant**. Vous pouvez choisir de créer un modèle à partir de zéro, mais il est généralement plus efficace de créer un modèle à partir d'un serveur existant doté de la configuration souhaitée.

Lorsque vous créez un modèle de serveur à partir d'un serveur existant, XClarity Administrator obtient les paramètres à partir d'un serveur géré (y compris les paramètres de port étendu, UEFI étendu et de contrôleur de gestion de la carte mère) et crée dynamiquement des modèles de catégorie pour ces paramètres. Dans le cas d'un tout nouveau serveur, XClarity Administrator mémorise les paramètres d'usine. Dans le cas d'un serveur déjà utilisé, XClarity Administrator mémorise les paramètres personnalisés. Vous pouvez ensuite modifier les paramètres en fonction du serveur sur lequel ce modèle doit être déployé.

Etape 5. Sélectionnez le serveur à utiliser comme configuration de base lorsque vous créez le modèle.

Remarque : Gardez à l'esprit que le serveur que vous choisissez doit être du même modèle que les serveurs sur lesquels vous prévoyez de déployer le modèle de serveur. Ce scénario repose sur le choix d'un Nœud de traitement x240 Flex System.

Etape 6. Entrez le nom du nouveau modèle et indiquez une description.

Par exemple :

- Nom : **x240_ESXi_deployment**
- Description : **Modèle avec paramètres UEFI étendus qui sont appropriés pour le déploiement de VMware ESXi**

Etape 7. Cliquez sur **Suivant** pour charger les informations à partir du serveur sélectionné.

Etape 8. Sur l'onglet **Stockage local**, sélectionnez **Spécifier une configuration de stockage** et choisissez l'un des types de stockage. Cliquez ensuite sur **Suivant**.

Pour plus d'informations sur les paramètres de stockage local, voir Définition d'un stockage local.

Etape 9. Sur l'onglet **Cartes d'E-S**, entrez les informations relatives aux cartes figurant dans les serveurs sur lesquels vous prévoyez d'installer VMware ESXi.

Toutes les cartes présentes dans le serveur qui a servi de base sont affichées.

Si tous les serveurs Nœuds de traitement Flex System x240 présents dans votre installation comportent les mêmes cartes, vous n'avez pas besoin de modifier les paramètres de cet onglet.

Pour plus d'informations sur les paramètres de cartes d'E-S, voir Définition de cartes d'E-S.

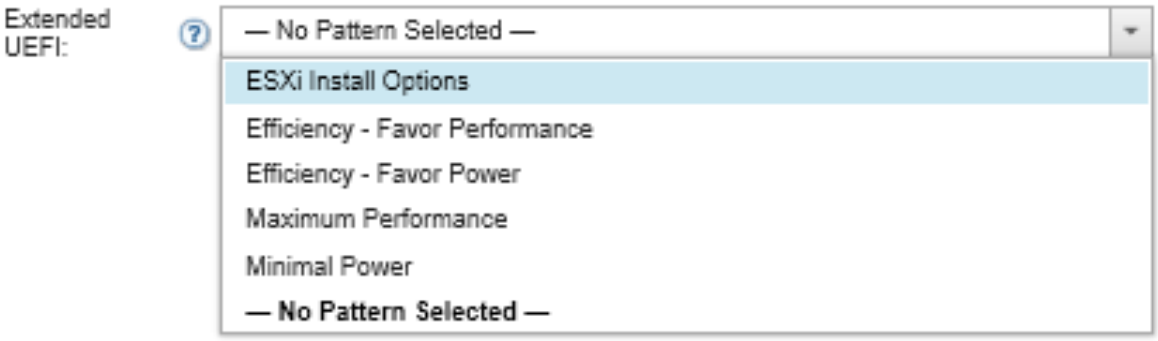
Etape 10. Cliquez sur **Suivant** pour continuer.

Etape 11. Sur l'onglet **Amorçage**, configurez les paramètres pour l'environnement d'amorçage Legacy Only et les environnements d'amorçage SAN. Sauf si vous utilisez l'un de ces environnements, acceptez la valeur par défaut, **Amorçage uniquement UEFI**, puis cliquez sur **Suivant**.

Pour plus d'informations sur les paramètres d'amorçage, voir Définition d'options d'amorçage.

Etape 12. Sur l'onglet **Paramètres de microprogramme**, spécifiez les paramètres de contrôleur de gestion et de microprogramme UEFI qui devront être utilisés pour les serveurs cible lorsque du déploiement de ce modèle (par exemple, sélectionnez **Virtualisation x240**).

Cet onglet vous permet de choisir l'un des modèles UEFI étendu prédéfinis :



Pour plus d'informations sur les paramètres de microprogramme, voir Définition de paramètres de microprogramme.

Etape 13. Cliquez sur **Enregistrer et déployer** pour enregistrer le modèle sur XClarity Administrator et le déployer sur les serveurs sur lesquels vous prévoyez d'installer VMware ESXi.

Après avoir terminé

Une fois le modèle de serveur déployé sur tous les serveurs, vous pouvez installer le système d'exploitation sur ces serveurs.

Déploiement de VMware ESXi sur un Nœud de traitement x240 Flex System

Utilisez cette procédure comme exemple de flux pour illustrer le processus de déploiement du système d'exploitation ESXi sur un Nœud de traitement x240 Flex System.

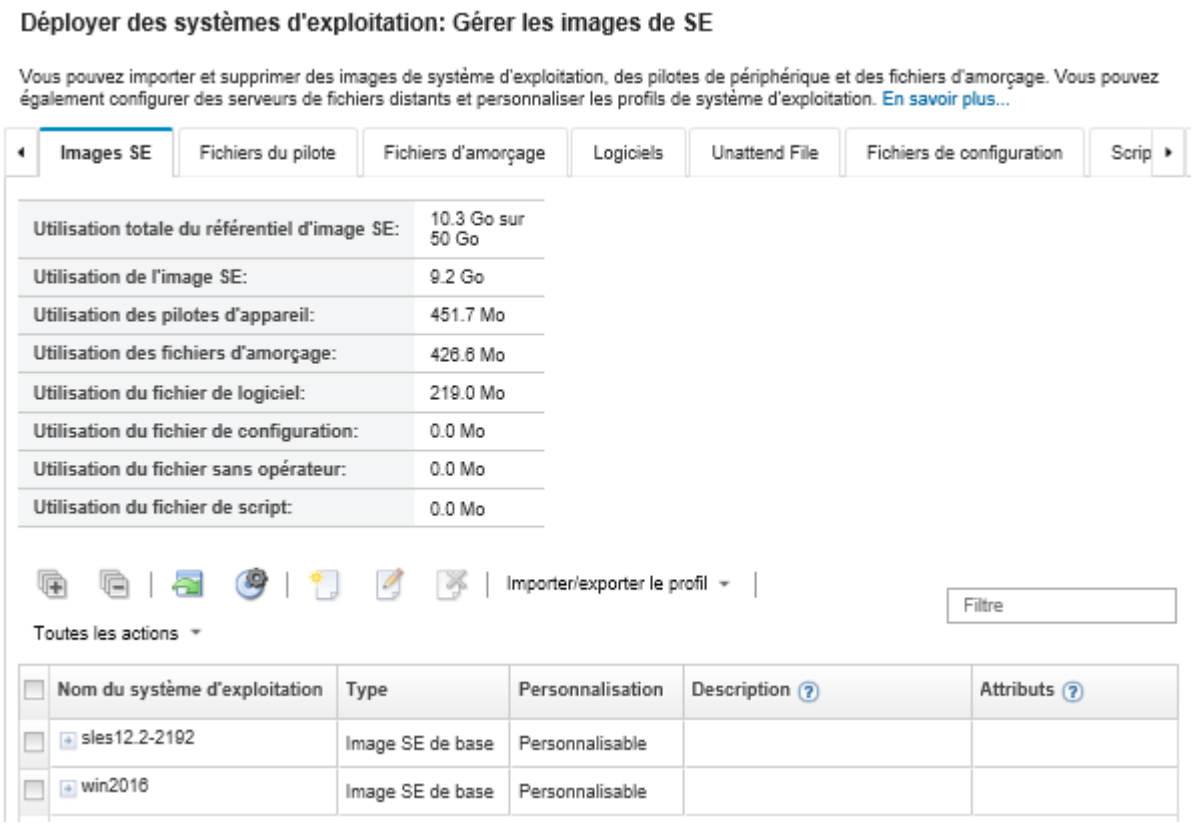
Avant de commencer

Avant de commencer cette procédure, vérifiez que Lenovo XClarity Administrator gère le châssis sur lequel le Nœud de traitement x240 Flex System est installé.

Procédure

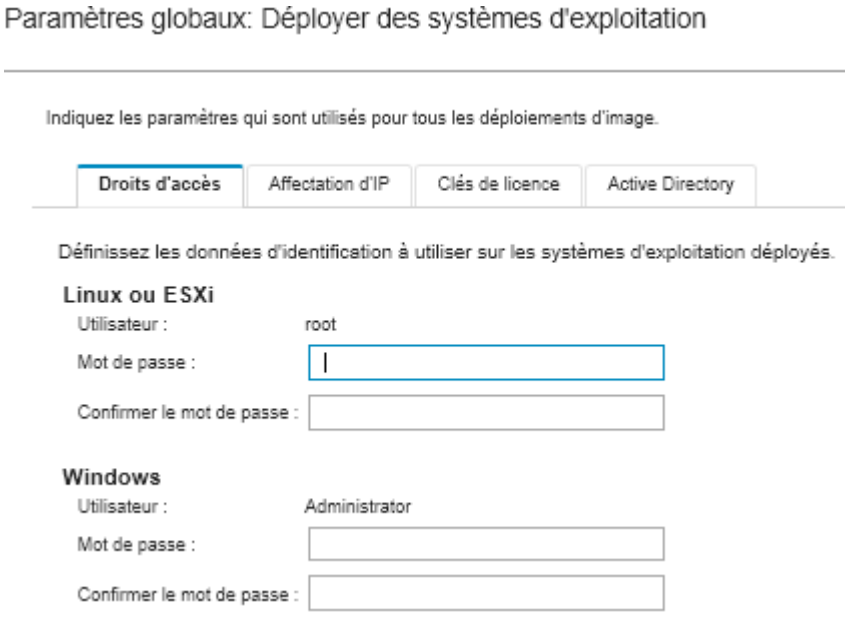
Procédez comme suit pour déployer le système d'exploitation ESXi sur un Nœud de traitement x240 Flex System.

Etape 1. Vérifiez que l'image à déployer est déjà chargée dans le Référentiel d'images SE en cliquant sur **Toutes les actions → Gérer les images SE** pour afficher la liste de toutes les images disponibles.



Etape 2. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Distribution → Déployer des images SE**. La page Déployer des images SE s'affiche.

Etape 3. Définissez les paramètres globaux qui doivent être utilisés comme valeurs par défaut pour tous les déploiements d'image en cliquant sur **Toutes les actions → Paramètres globaux** pour afficher la boîte de dialogue Paramètres globaux.



a. Sur l'onglet **Données d'identification**, entrez le mot de passe qui doit être utilisé par le compte administrateur pour se connecter au système d'exploitation.

b. Sur l'onglet **Affectation d'IP**, indiquez comment l'adresse IP du système d'exploitation est affectée au serveur.

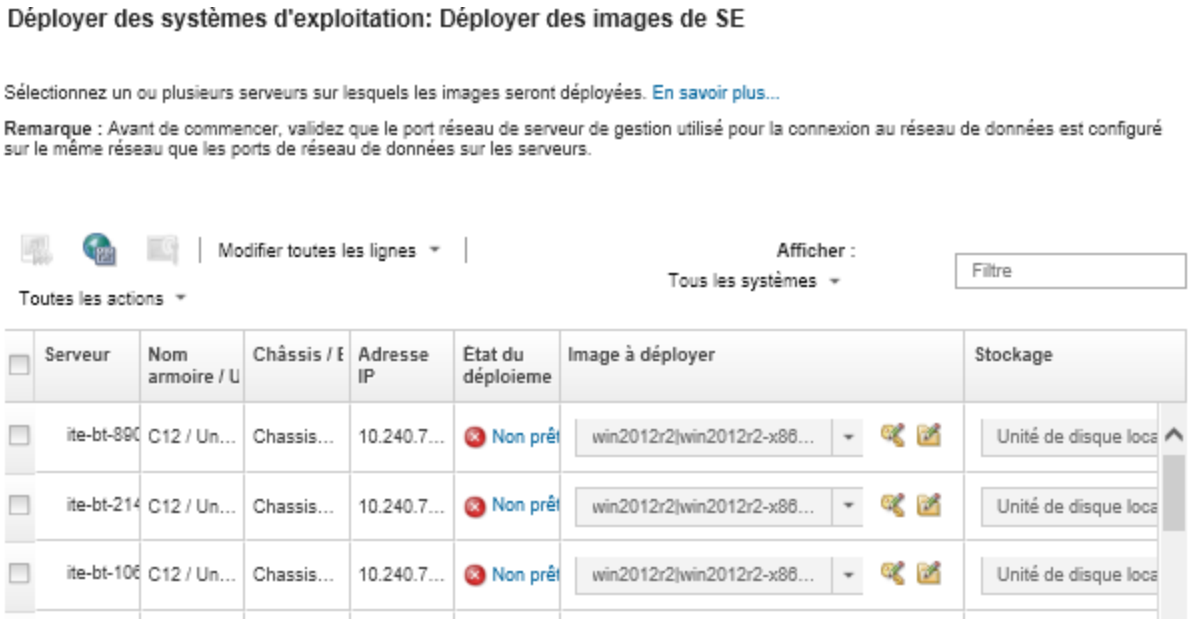
   Si vous choisissez **Utiliser le protocole DHCP (Dynamic Host Configuration Protocol)** pour affecter des adresses IP, les informations d'adresse IP ne sont pas affichées sur la boîte de dialogue Éditer les paramètres réseau (voir l'étape Etape 8 9 à la page 641). Si vous choisissez **Affecter une adresse IP statique (IPv4)**, vous pouvez indiquer une adresse IP, un sous-réseau et une passerelle pour chaque déploiement.

c. Sur l'onglet **Clés de licence**, entrez une clé de licence d'activation de masse, si vous le souhaitez.

d. Cliquez sur **OK** pour fermer la boîte de dialogue.

Etape 4. Vérifiez que le serveur est prêt pour le déploiement du système d'exploitation en sélectionnant le serveur sur lequel le système d'exploitation doit être déployé. Initialement, l'état de déploiement peut être Non prêt. L'état de déploiement doit être Prêt pour que vous puissiez déployer un système d'exploitation sur un serveur.

Astuce : Vous pouvez choisir plusieurs serveurs dans plusieurs châssis Flex System si vous souhaitez déployer le même système d'exploitation sur tous les serveurs. Vous pouvez sélectionner jusqu'à 28 serveurs.



Etape 5. Cliquez sur la colonne **Image à déployer** et sélectionnez VMware ESXi 5.5 (**esxi5.5_2.33|esxi5.5_2.33-x86_64-install-Virtualization**).

Etape 6. Dans la même colonne, cliquez sur l'icône **Clé de licence** ( ) pour entrer la clé de licence pour ce déploiement.

Conseil : vous pouvez également choisir d'utiliser une clé d'activation en masse que vous avez entrée dans la boîte de dialogue Paramètres globaux.

Etape 7. Vérifiez que **Disque local** est sélectionné dans la colonne Stockage.

Etape 8. Cliquez sur **Éditer** dans la colonne **Paramètres réseau** de la ligne de serveur pour configurer les paramètres réseau qui doivent être utilisés pour ce déploiement. La page Éditer les paramètres réseau s'affiche.

Renseignez les zones suivantes :

- Nom d'hôte
- Adresse MAC du port sur l'hôte sur lequel le système d'exploitation doit être installé
- Serveurs DNS (Domain Name System), le cas échéant
- vitesse d'unité MTU (unité de transmission maximale)

Remarques : Si vous avez choisi **Affecter une adresse IP statique (IPv4)** dans la boîte de dialogue des Paramètres globaux (voir l'étape Etape 3 4 à la page 640), entrez également les informations suivantes :

- Adresse IPv4
- Masque de sous-réseau
- Passerelle

Etape 9. Cliquez sur **OK** pour fermer la boîte de dialogue.

Dans la page Déployer des images SE, assurez-vous que le serveur affiche un État du déploiement Prêt.

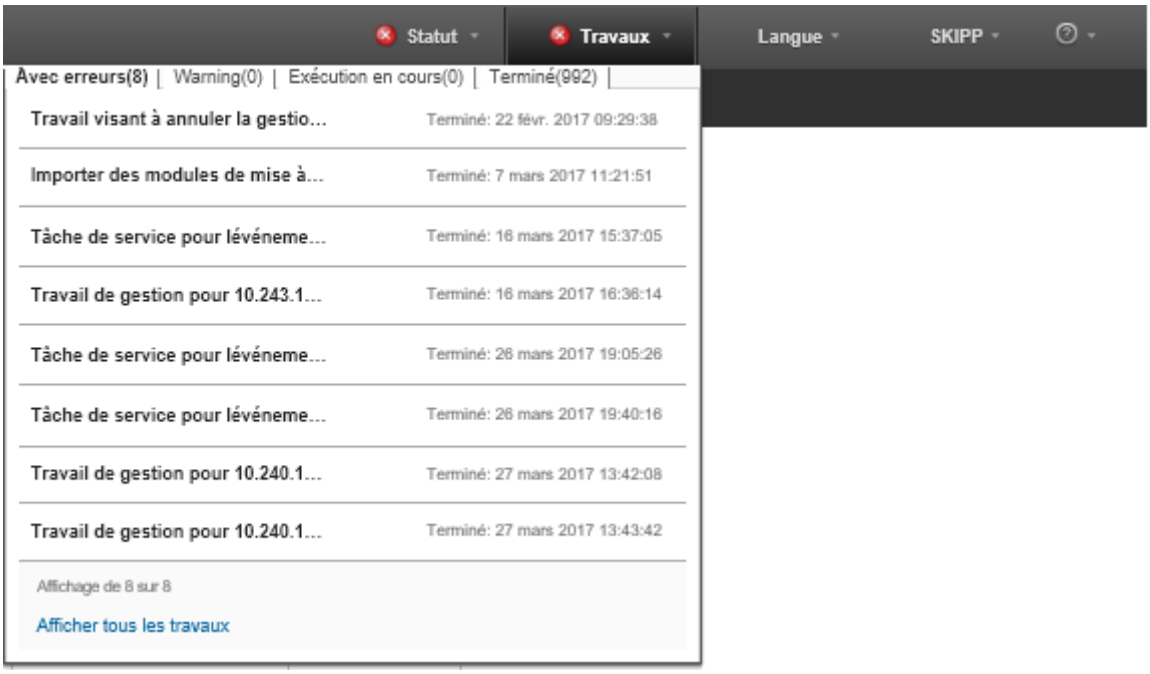
Etape 10. Déployez le système d'exploitation en cliquant sur **Toutes les actions → Déployer des images**.

Etape 11. Sur la page de confirmation, cliquez sur **Déployer** pour déployer l'image.

Si le serveur possède actuellement un système d'exploitation installé, un message d'avertissement s'affiche pour vous informer que le déploiement de l'image remplacera le système d'exploitation installé.

Conseil : vous pouvez installer une session de contrôle à distance pour observer l'installation tandis qu'elle se poursuit. Cliquez sur **Toutes les actions → Contrôle à distance** pour ouvrir une session de Contrôle à distance avec le serveur.

Lorsque vous déployez le système d'exploitation, Lenovo XClarity Administrator démarre un travail pour suivre le déploiement. Pour afficher l'état du travail de déploiement, cliquez sur **Travaux** dans la barre de menus Lenovo XClarity Administrator. Ensuite, cliquez sur l'onglet **Exécution en cours**.

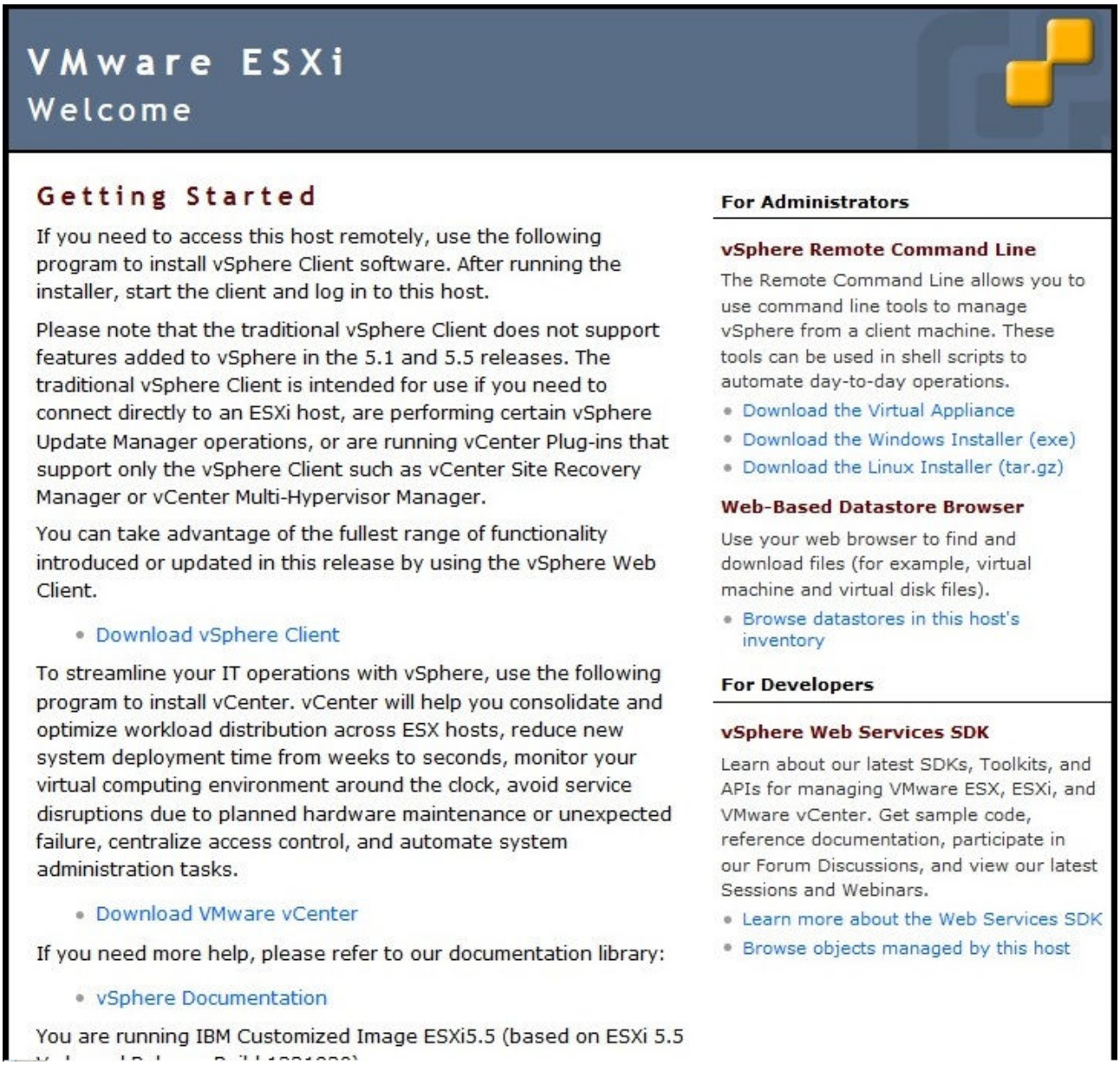


Survolez le travail en cours d'exécution pour afficher les détails, tels que le pourcentage de travail terminé.

Résultats

Une fois le déploiement du système d'exploitation terminé, connectez-vous à l'adresse IP que vous avez spécifiée sur la page Éditer les paramètres réseau pour continuer le processus de configuration.

Remarque : La licence fournie avec l'image est un essai gratuit de 60 jours. Vous êtes responsable du respect de toutes les conditions de licence de VMware.



Déploiement d'ESXi sur un stockage SAN

Ces procédures permettent de déployer VMware ESXi 5.5 sur des volumes SAN connectés aux serveurs.

Lorsque vous déployez un système d'exploitation sur un stockage SAN, le système d'exploitation est déployé sur la première cible d'amorçage SAN configurée via un modèle de serveur. De plus, il n'est pas possible d'activer un disque dur local sur le serveur qui démarre à partir du stockage SAN. Il doit être désactivé ou supprimé si un disque dur est présent.

Déploiement d'un modèle de serveur pour prendre en charge l'amorçage SAN

Lorsque vous créez et déployez un modèle de serveur pour prendre en charge l'amorçage d'un système à partir d'un réseau de stockage SAN, prenez soin d'identifier la cible d'amorçage SAN et les cartes présentes sur le serveur.

Procédure

Pour créer et déployer un modèle de serveur qui prend en charge le déploiement du système d'exploitation sur un système de stockage SAN, procédez comme suit.

Etape 1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Distribution → Modèles**. La page Modèles de configuration : Modèles s'affiche.

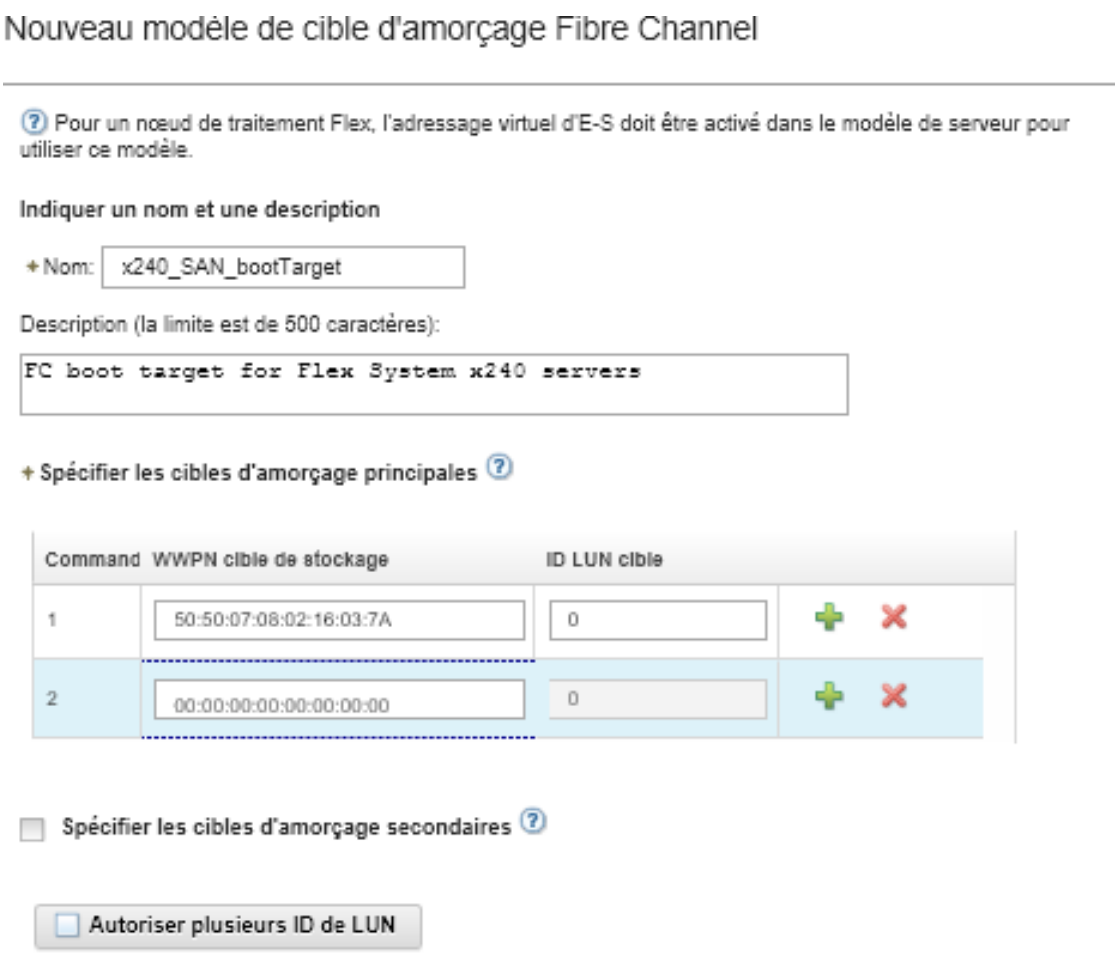
Etape 2. Pour identifier les identificateurs de nom de port universel (WWPN) et d'unité logique (LUN) des volumes de stockage sur lesquels déployer le système d'exploitation, créez un modèle de catégorie.

a. Cliquez sur l'onglet **Modèles de catégorie**.

b. Cliquez sur **Modèles de cible d'amorçage Fibre Channel**, puis sur l'icône **Créer** ( ).

c. Entrez le nom de port universel (WWPN) de la cible de stockage.

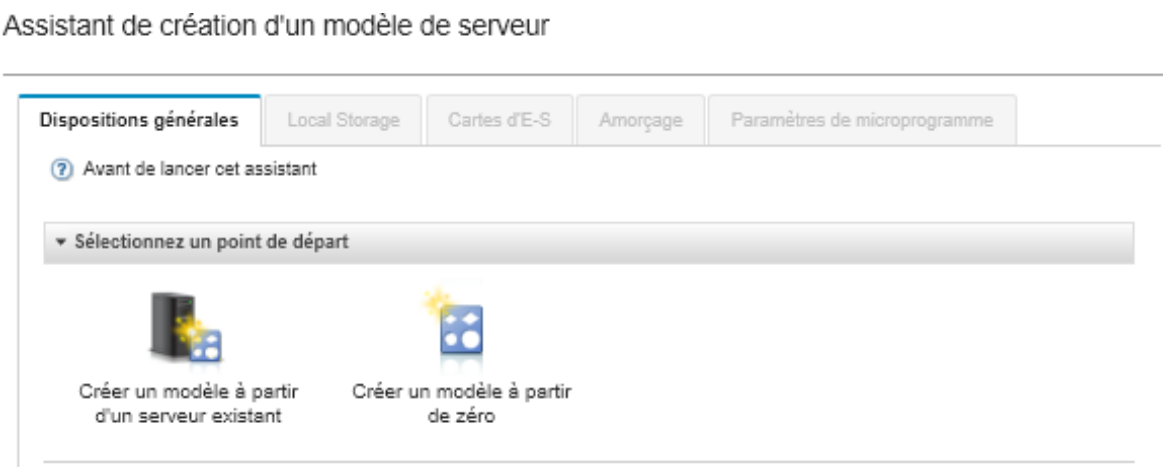
Remarque : Cliquez sur **Autoriser plusieurs identificateurs d'unité logique** pour affecter plusieurs identificateurs d'unité logique cible aux mêmes volumes de stockage.



d. Cliquez sur **Créer** pour créer le modèle. La cible s'affiche dans la liste des modèles cible d'amorçage Fibre Channel.

Etape 3. Cliquez sur l'onglet **Modèles de serveur** pour créer un modèle.

Etape 4. Cliquez sur l'icône **Créer** ( ). L'Assistant de création de modèles de serveur s'affiche.



Etape 5. Cliquez sur **Créer un modèle à partir de zéro**.

Etape 6. Sur l'onglet **Général** :

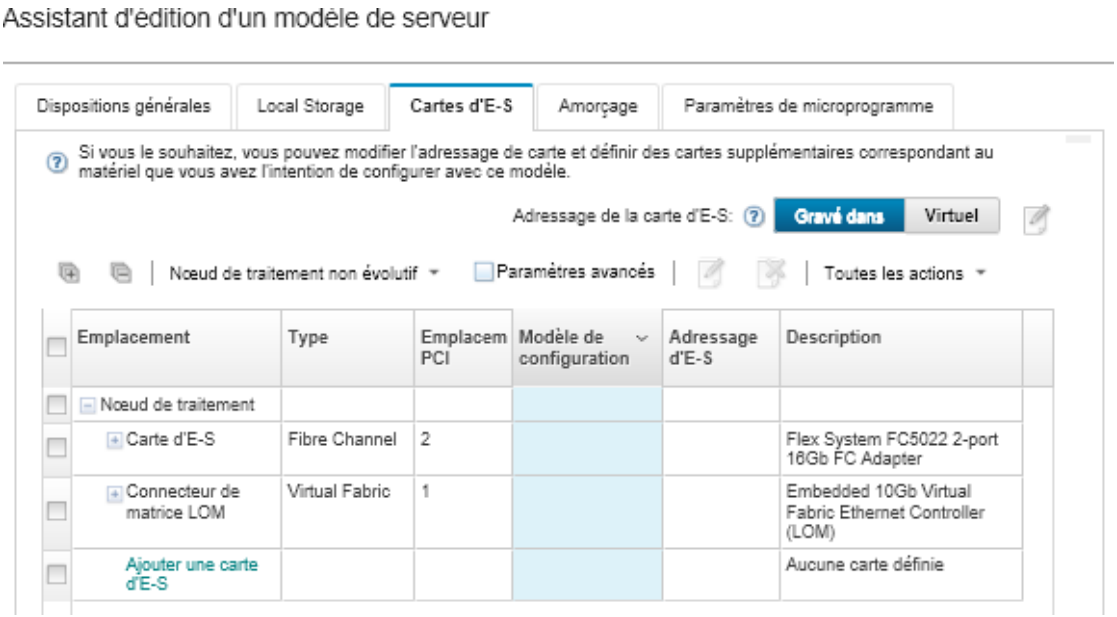
- Sélectionnez **Nœud de traitement Flex** comme format.
- Indiquez un nom de modèle (**x240_san_boot**) et une description.
- Cliquez sur **Suivant**.

Etape 7. Sur l'onglet **Stockage local**, envisagez de désactiver l'adaptateur de stockage local si vous utilisez un système sans disque afin d'améliorer les temps d'amorçage liés à la recherche d'unités locales. Cliquez ensuite sur **Suivant**.

Etape 8. Sur l'onglet **Cartes d'E-S**, ajoutez les cartes Ethernet et Fibre Channel. Assurez-vous qu'elles figurent dans les emplacements PCI appropriés.

a. Pour chaque carte, cliquez sur **Ajouter une carte d'E-S**, choisissez l'emplacement PCI sur lequel se trouve la carte, puis sélectionnez cette dernière.

Remarque : Prenez soin d'indiquer une carte Ethernet et une carte Fibre Channel.



b. Vérifiez que la valeur affectée à l'adressage de carte d'E-S est **Virtuel**. Cliquez ensuite sur l'icône **Éditer** pour spécifier la configuration à utiliser pour l'adressage virtuel Ethernet (MAC) et l'adressage virtuel Fibre Channel (WWN).

Remarque : Sur la page Éditer l'adressage virtuel, vous pouvez choisir d'utiliser les adresses MAC gravées pour la carte Ethernet en désactivant l'adressage virtuel. Toutefois, pour sélectionner et utiliser un modèle cible d'amorçage Fibre Channel, vous devez utiliser l'adressage virtuel pour la carte Fibre Channel.

c. Cliquez sur **Suivant**.

Etape 9. Sur l'onglet **Amorçage**, ajoutez le modèle cible d'amorçage SAN que vous avez créé précédemment.

a. Sur l'onglet **Amorçage SAN**, choisissez le modèle cible d'amorçage que vous avez défini.

b. Cliquez sur **Suivant**.

Etape 10. Sur l'onglet **Paramètres de microprogramme**, définissez les éventuels modèles de catégorie supplémentaires à inclure dans ce modèle de serveur. Vous pouvez définir les modèles de catégorie suivants :

- **Informations système** (voir Définition de paramètres d'informations système).
- **Interface de gestion** (voir Définition de paramètres d'interface de gestion)
- **Appareils et ports d'E-S** (voir Définition de paramètres d'appareils et de ports d'E-S).
- **BMC étendu**. Vous pouvez effectuer une sélection parmi les paramètres de contrôleur de gestion de la carte mère qui ont été obtenus précédemment (voir Définition de paramètres de contrôleur de gestion étendus).
- **UEFI étendu**. Vous pouvez effectuer une sélection parmi les paramètres prédéfinis ou les paramètres UEFI qui ont été obtenus précédemment (voir Définition de paramètres UEFI étendu).

Etape 11. Cliquez sur **Enregistrer et déployer** pour enregistrer le modèle sur Lenovo XClarity Administrator et le déployer sur les serveurs sur lesquels vous prévoyez d'installer VMware ESXi.

Après avoir terminé

Envisagez d'exécuter les étapes suivantes une fois que le modèle de serveur a été déployé sur tous les serveurs :

1. Prenez les adresses WWPN virtualisées qui ont été créées et ajoutez-les à la zone de stockage pour permettre au serveur d'atteindre les numéros d'unité logique de stockage définis.

   Astuce : Une fois que vous avez déployé le profil de serveur, vous pouvez le consulter pour rechercher les adresses WWPN virtualisées.

   a. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Distribution → Profils de serveur**.

   b. Cliquez sur le profil de serveur déployé (par exemple, **x240_SAN_boot**). L'onglet **Mappage d'adresse virtuelle** affiche la liste des adresses.

2. Déployez le système d'exploitation sur le serveur.

Déploiement de VMware ESXi sur un stockage SAN

Utilisez cette procédure comme exemple de flux pour illustrer le processus de déploiement du système d'exploitation ESXi sur un stockage SAN connecté à un serveur.

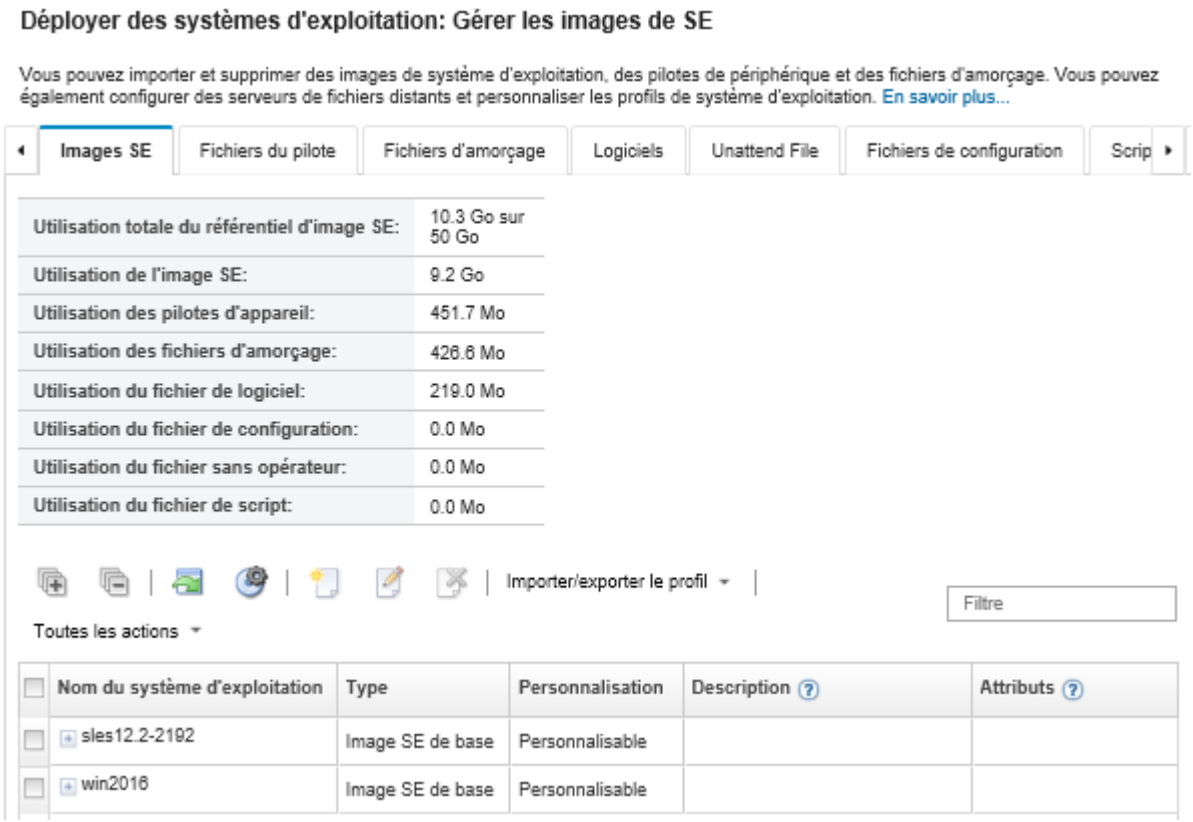
Avant de commencer

Avant de commencer cette procédure, vérifiez que Lenovo XClarity Administrator gère le châssis sur lequel le Nœud de traitement x220 Flex System est installé.

Procédure

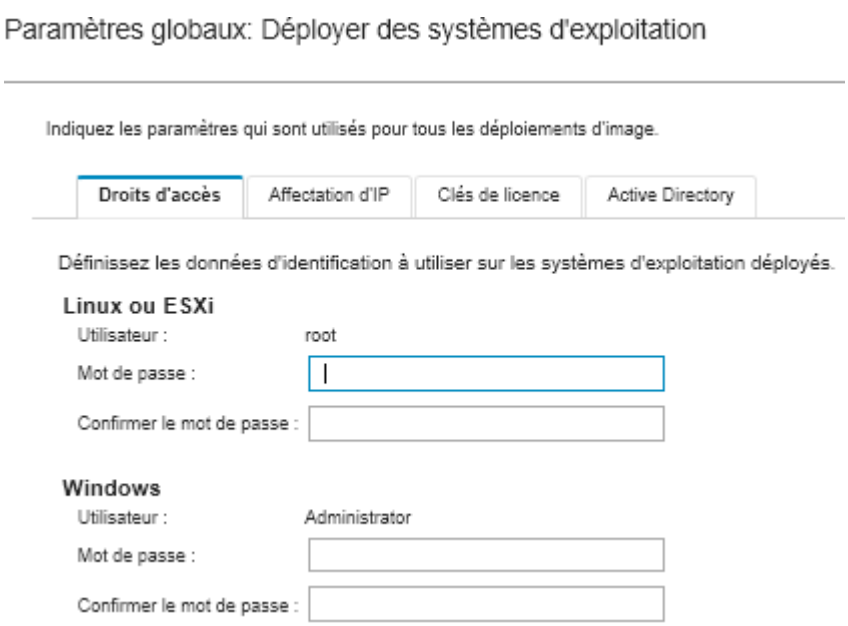
Procédez comme suit pour déployer le système d'exploitation ESXi sur un Nœud de traitement x222 Flex System.

Etape 1. Vérifiez que l'image à déployer est déjà chargée dans le Référentiel d'images SE en cliquant sur **Toutes les actions → Gérer les images SE**.



Etape 2. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Distribution → Déployer des images SE**.

Etape 3. Définissez les paramètres globaux qui doivent être utilisés comme valeurs par défaut pour tous les déploiements d'image en cliquant sur **Toutes les actions → Paramètres globaux** pour afficher la boîte de dialogue Paramètres globaux : Déployer des systèmes d'exploitation.



a. Sur l'onglet **Données d'identification**, entrez le mot de passe qui doit être utilisé par le compte administrateur pour se connecter au système d'exploitation.

b. Sur l'onglet **Affectation** d'IP, indiquez comment l'adresse IP du système d'exploitation doit être affectée au serveur.

   Si vous choisissez **Utiliser le protocole DHCP (Dynamic Host Configuration Protocol)** pour affecter des adresses IP, les informations d'adresse IP ne s'afficheront pas sur la boîte de dialogue Éditer les paramètres réseau (voir l'étape Etape 8 9 à la page 650). Si vous choisissez **Affecter une adresse IP statique (IPv4)**, vous pouvez indiquer une adresse IP, un sous-réseau et une passerelle pour chaque déploiement.

c. Sur l'onglet **Clés de licence**, entrez une clé de licence d'activation de masse, si vous le souhaitez.

d. Cliquez sur **OK** pour fermer la boîte de dialogue.

Etape 4. Vérifiez que le serveur est prêt pour le déploiement du système d'exploitation en sélectionnant le serveur sur lequel le système d'exploitation doit être déployé. Initialement, l'état de déploiement peut être Non prêt. L'état de déploiement doit être Prêt pour que vous puissiez déployer un système d'exploitation sur un serveur.

Astuce : Vous pouvez choisir plusieurs serveurs dans plusieurs châssis Flex System si vous souhaitez déployer le même système d'exploitation sur tous les serveurs. Vous pouvez sélectionner jusqu'à 28 serveurs.

Etape 5. Cliquez sur la colonne **Image à déployer** et sélectionnez VMware ESXi 5.5 (**esxi5.5_2.33|esxi5.5_2.33-x86_64-install-Virtualization**).

Etape 6. Dans la même colonne, cliquez sur l'icône **Clé de licence** ( ) pour entrer la clé de licence pour ce déploiement.

Conseil : vous pouvez également choisir d'utiliser une clé d'activation en masse que vous avez entrée dans la boîte de dialogue Paramètres globaux : Déployer des systèmes d'exploitation.

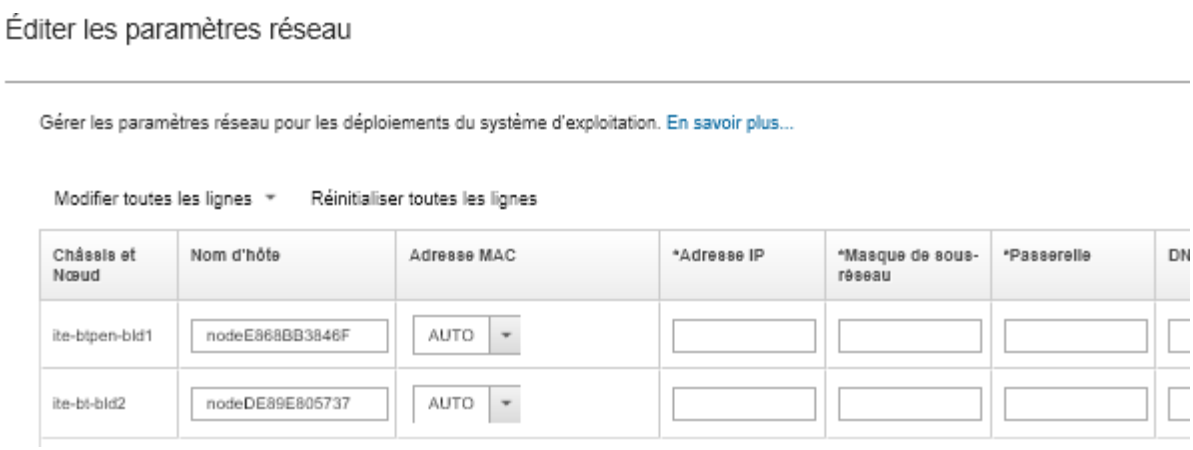
Etape 7. Dans la colonne **Stockage**, sélectionnez le stockage SAN sur lequel le système d'exploitation doit être déployé.

Le stockage est répertorié comme suit :
`LUN: <LUN_VALUE>  WWPN: <WWPN_VALUE>`

Etape 8. Cliquez sur **Éditer** dans la colonne **Paramètres réseau** de la ligne de serveur pour configurer les paramètres réseau qui doivent être utilisés pour ce déploiement. La page Éditer les paramètres réseau s'affiche.

Renseignez les zones suivantes :
- Nom d'hôte
- Adresse MAC du port sur l'hôte sur lequel le système d'exploitation sera installé
- Serveurs DNS (Domain Name System), le cas échéant
- Vitesse d'unité MTU (unité de transmission maximale)

Remarques : Si vous avez choisi **Affecter une adresse IP statique (IPv4)** dans la boîte de dialogue Paramètres globaux : Déployer des systèmes d'exploitation (étape Etape 3 4 à la page 648), entrez également les informations suivantes :
- Adresse IPv4
- Masque de sous-réseau
- Passerelle



Etape 9. Cliquez sur **OK** pour fermer la boîte de dialogue.

Sur la page Déployer des images SE, le serveur affiche désormais un état du déploiement Prêt.

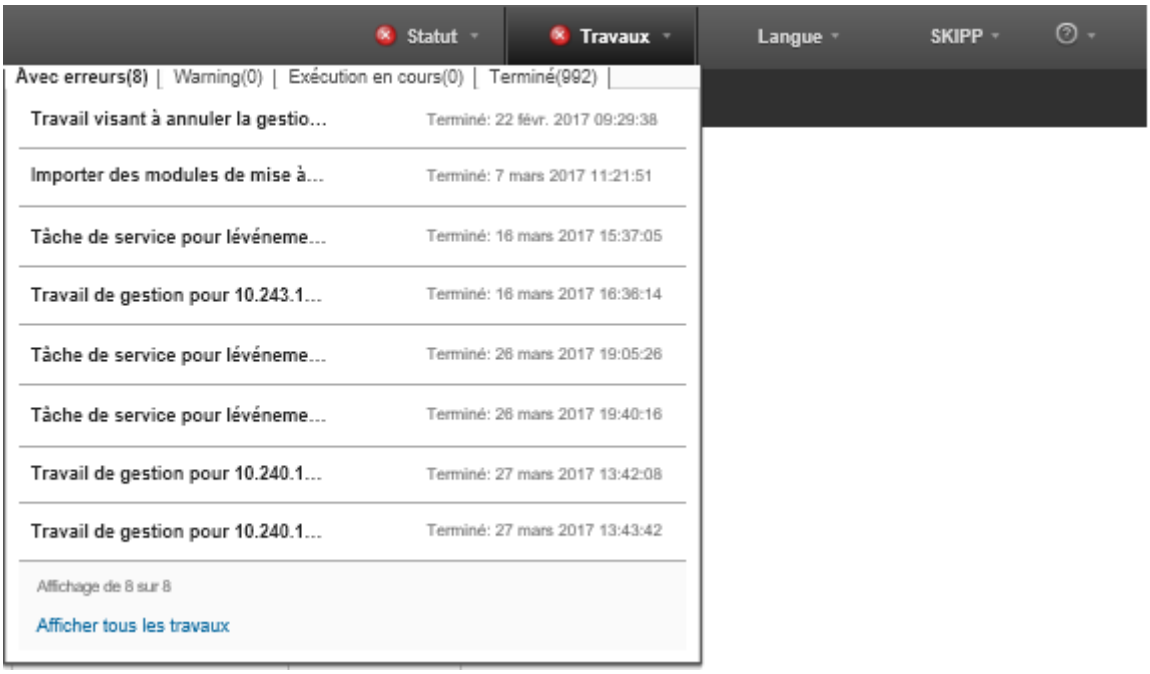
Etape 10. Déployez le système d'exploitation en cliquant sur **Toutes les actions → Déployer des images**.

Etape 11. Sur la page de confirmation, cliquez sur **Déployer** pour déployer l'image.

Si le serveur possède actuellement un système d'exploitation installé, un message d'avertissement s'affiche pour vous informer que le déploiement de l'image remplacera le système d'exploitation installé.

Conseil : vous pouvez installer une session de contrôle à distance pour observer l'installation tandis qu'elle se poursuit. Cliquez sur **Toutes les actions → Contrôle à distance** pour ouvrir une session de contrôle à distance avec le serveur.

Lorsque vous déployez le système d'exploitation, Lenovo XClarity Administrator démarre un travail pour suivre le déploiement. Pour afficher l'état du travail de déploiement, cliquez sur **Travaux** dans la barre de menus Lenovo XClarity Administrator. Ensuite, cliquez sur l'onglet **Exécution en cours**.

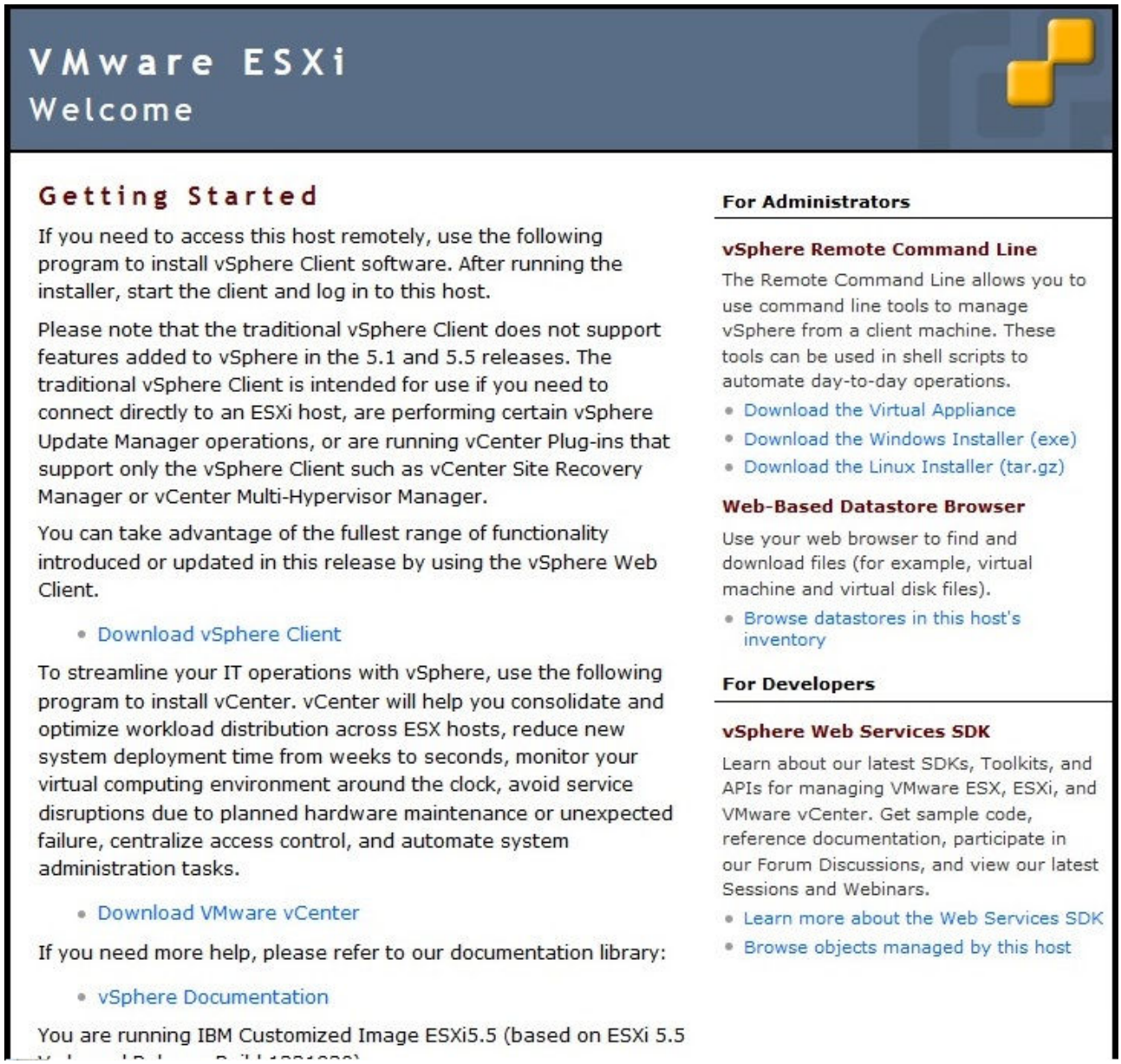


Survolez le travail en cours d'exécution pour afficher les détails, tels que le pourcentage de travail terminé.

Résultats

Une fois le déploiement du système d'exploitation terminé, connectez-vous à l'adresse IP que vous avez spécifiée sur la page Éditer les paramètres réseau pour continuer le processus de configuration.

Remarque : La licence fournie avec l'image est un essai gratuit de 60 jours. Vous êtes responsable du respect de toutes les conditions de licence de VMware.



Consignes

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services Lenovo non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial Lenovo.

Toute référence à un produit, logiciel ou service Lenovo n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit de Lenovo. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par Lenovo.

Lenovo peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document n'est pas une offre et ne fournit pas de licence sous brevet ou demande de brevet. Vous pouvez en faire la demande par écrit à l'adresse suivante :

Lenovo (United States), Inc.
1009 Think Place
Morrisville, NC 27560
U.S.A.
Attention: Lenovo VP of Intellectual Property

LE PRÉSENT DOCUMENT EST LIVRÉ « EN L'ÉTAT ». LENOVO DÉCLINE TOUTE RESPONSABILITÉ, EXPLICITE OU IMPLICITE, RELATIVE AUX INFORMATIONS QUI Y SONT CONTENUES, Y COMPRIS EN CE QUI CONCERNE LES GARANTIES DE NON-CONTREFAÇON ET D'APTITUDE A L'EXÉCUTION D'UN TRAVAIL DONNÉ. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Il est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Lenovo peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les produits décrits dans ce document ne sont pas conçus pour être implantés ou utilisés dans un environnement où un dysfonctionnement pourrait entraîner des dommages corporels ou le décès de personnes. Les informations contenues dans ce document n'affectent ni ne modifient les garanties ou les spécifications des produits Lenovo. Rien dans ce document ne doit être considéré comme une licence ou une garantie explicite ou implicite en matière de droits de propriété intellectuelle de Lenovo ou de tiers. Toutes les informations contenues dans ce document ont été obtenues dans des environnements spécifiques et sont présentées en tant qu'illustration. Les résultats peuvent varier selon l'environnement d'exploitation utilisé.

Lenovo pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les références à des sites Web non Lenovo sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit Lenovo et l'utilisation de ces sites relève de votre seule responsabilité.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats

peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Marques

Lenovo