



# Lenovo XClarity Administrator Guide de planification et d'installation pour les environnements Docker



**Version 4.0.0**

## Remarque

Avant d'utiliser le présent document et le produit associé, prenez connaissance des [mentions générales et légales dans la documentation en ligne de XClarity Administrator](#).

Première édition (Février 2023)

© Copyright Lenovo 2022.

**REMARQUE SUR LES DROITS LIMITÉS ET RESTREINTS** : si les données ou les logiciels sont fournis conformément à un contrat GSA (« General Services Administration »), l'utilisation, la reproduction et la divulgation sont soumises aux restrictions stipulées dans le contrat n° GS-35F-05925.

# Table des matières

<b>Table des matières</b> . . . . .	<b>i</b>
<b>Figures</b> . . . . .	<b>.iii</b>
<b>Tableaux</b> . . . . .	<b>v</b>
<b>Récapitulatif des modifications</b> . . . .	<b>vii</b>
<b>Chapitre 1. Présentation de Lenovo XClarity Administrator</b> . . . . .	<b>1</b>
<b>Chapitre 2. Planification pour XClarity Administrator</b> . . . . .	<b>7</b>
Licences et la version d'évaluation gratuite de 90 jours . . . . .	7
Configurations matérielles et logicielles requises . . . .	8
Pare-feux et serveurs proxy . . . . .	10
Disponibilité de port . . . . .	12
Considérations relatives à la gestion. . . . .	17
Remarques sur le réseau . . . . .	18
Limitations de la configuration IP . . . . .	18
Types de réseaux . . . . .	19
Configurations réseau . . . . .	19
Remarques liées à la sécurité . . . . .	31
Gestion de l'encapsulation. . . . .	31
Gestion cryptographique . . . . .	32
Certificats de sécurité . . . . .	34
Authentification . . . . .	35
Comptes utilisateur et groupes de rôles . . . . .	38
Sécurité de compte utilisateur . . . . .	38
Remarques sur la haute disponibilité . . . . .	38
Features on Demand (FoD) . . . . .	39
<b>Chapitre 3. Installation de Lenovo XClarity Administrator</b> . . . . .	<b>41</b>
Donnée unique et réseau de gestion. . . . .	41
Étape 1 : Câblez le châssis, les serveurs rack et l'hôte Lenovo XClarity Administrator sur les commutateurs de la partie supérieure de l'armoire . . . . .	43
Étape 2 : Configurer les commutateurs de la partie supérieure de l'armoire. . . . .	44
Étape 3 : Configurer les Chassis Management Modules (modules CMM) . . . . .	45
Étape 4 : Configurer Commutateurs Flex . . . . .	46
Étape 5 : installation et configuration de l'hôte . . . . .	47
Étape 6. Installation et configuration d'un XClarity Administrator . . . . .	48
Données séparées physiquement et réseaux de gestion . . . . .	51
Étape 1 : Câblez le châssis, les serveurs rack et l'hôte Lenovo XClarity Administrator sur les commutateurs de la partie supérieure de l'armoire . . . . .	53
Étape 2 : Configurer les commutateurs de la partie supérieure de l'armoire. . . . .	54
Étape 3 : Configurer les Chassis Management Modules (modules CMM) . . . . .	54
Étape 4 : Configurer Commutateurs Flex . . . . .	56
Étape 5 : installation et configuration de l'hôte . . . . .	57
Étape 6 : installation et configuration de XClarity Administrator . . . . .	58
Données séparées virtuellement et topologie du réseau de gestion . . . . .	61
Étape 1 : Câblez le châssis et les serveurs rack sur les commutateurs de la partie supérieure de l'armoire . . . . .	64
Étape 2 : Configurer les commutateurs de la partie supérieure de l'armoire. . . . .	65
Étape 3 : Configurer les Chassis Management Modules (modules CMM) . . . . .	66
Étape 4 : configuration de Commutateurs Flex. . . . .	68
Étape 5 : installation et configuration de l'hôte . . . . .	69
Étape6: installation et configuration de XClarity Administrator . . . . .	70
Topologie du réseau de gestion uniquement . . . . .	73
Étape 1 : Câblez le châssis, les serveurs rack et l'hôte Lenovo XClarity Administrator sur les commutateurs de la partie supérieure de l'armoire . . . . .	75
Étape 2 : Configurer les commutateurs de la partie supérieure de l'armoire. . . . .	76
Étape 3 : Configurer les Chassis Management Modules (modules CMM) . . . . .	76
Étape 4 : Configurer Commutateurs Flex . . . . .	78
Étape 5 : installation et configuration de l'hôte . . . . .	79
Étape 6 : installation et configuration de XClarity Administrator . . . . .	80
Mise en place de la haute disponibilité . . . . .	83
<b>Chapitre 4. Configuration des Lenovo XClarity Administrator</b> . . . . .	<b>85</b>
Accès à l'interface Web Lenovo XClarity Administrator la première fois . . . . .	85

Création de comptes utilisateur. . . . .	88
Configuration de l'accès réseau . . . . .	89
Configuration de la date et de l'heure . . . . .	96
Configuration du service et du support . . . . .	98
Configuration de la sécurité . . . . .	101
Gestion des appareils . . . . .	102

**Chapitre 5. Inscription de XClarity Administrator . . . . .115**

**Chapitre 6. Installation de la licence d'activation de l'ensemble des fonctionnalités . . . . .117**

Installation de licences d'activation de l'ensemble des fonctionnalités à l'aide de l'interface Web XClarity Administrator. . . . .	119
Installation de licences d'activation de l'ensemble des fonctionnalités à l'aide du portail Web Features on Demand. . . . .	123

**Chapitre 7. Mise à jour de XClarity Administrator en tant que . . . . .127**

**Chapitre 8. Désinstallation de XClarity Administrator . . . . .131**

---

## Figures

1.	Exemple d'implémentation d'un réseau unique pour la gestion, les données et le déploiement du système d'exploitation . . . . .	23
2.	Exemple d'implémentation de réseaux de données et de gestion séparés physiquement avec le réseau du système d'exploitation faisant partie du réseau de données . . . . .	25
3.	Exemple d'implémentation de réseaux de données et de gestion séparés physiquement avec le réseau du système d'exploitation faisant partie du réseau de gestion . . . . .	26
4.	Exemple d'implémentation de réseaux de données et de gestion séparés virtuellement avec le réseau du système d'exploitation faisant partie du réseau de données . . . . .	28
5.	Exemple d'implémentation de réseaux de gestion et de données virtuellement séparés avec le réseau du système d'exploitation faisant partie du réseau de gestion . . . . .	29
6.	Exemple d'implémentation d'un réseau de gestion uniquement dans lequel le déploiement du système d'exploitation n'est pas pris en charge . . . . .	30
7.	Exemple d'implémentation d'un réseau de gestion uniquement dans lequel le déploiement du système d'exploitation est pris en charge . . . . .	31
8.	Exemple de donnée unique et de topologie de réseau de gestion pour un dispositif virtuel . . . . .	42
9.	Exemple de topologie du réseau de donnée unique et de gestion pour les conteneurs . . . . .	43
10.	Exemple de câblage pour un réseau de donnée unique et de gestion . . . . .	44
11.	Emplacements Commutateur Flex dans un châssis . . . . .	47
12.	Exemple de données séparées physiquement et de topologie du réseau de gestion pour un dispositif virtuel . . . . .	52
13.	Exemple de données séparées physiquement et de topologie du réseau de gestion pour les conteneurs . . . . .	53
14.	Exemple de câblage pour les réseaux de gestion et de données séparées physiquement . . . . .	54
15.	Emplacements Commutateur Flex dans un châssis . . . . .	57
16.	Exemple de données séparées virtuellement et de topologie du réseau de gestion pour un dispositif virtuel . . . . .	62
17.	Exemple de données séparées virtuellement et de topologie du réseau de gestion pour les conteneurs . . . . .	63
18.	Exemple de câblage pour les réseaux de données séparées virtuellement et de gestion . . . . .	65
19.	Exemple de configuration pour Commutateurs Flex sur des réseaux de données séparées virtuellement et de gestion (VMware ESXi) dans lesquels le marquage VLAN est activé sur le réseau de gestion. . . . .	66
20.	Exemple de configuration pour Commutateurs Flex sur des réseaux de données séparées virtuellement et de gestion (VMware ESXi) dans lesquels le marquage VLAN est activé sur le réseau de gestion. . . . .	69
21.	Exemple de topologie du réseau de gestion uniquement pour un dispositif virtuel . . . . .	74
22.	Exemple de topologie du réseau de gestion uniquement pour les conteneurs . . . . .	75
23.	Exemple de câblage pour un réseau de gestion uniquement . . . . .	76
24.	Emplacements Commutateur Flex dans un châssis . . . . .	79





# Tableaux

- 1. Connexions Internet requises . . . . . 11
- 2. Rôle de chaque interfaces réseau en fonction de la topologie de réseau . . . . . 21
- 3. Rôle de chaque interfaces réseau en fonction de la topologie de réseau . . . . . 91





---

## 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.

Pour plus d'informations sur tout le matériel pris en charge (y compris les serveurs, les châssis et les commutateurs Flex), voir [Configurations matérielles et logicielles requises](#).

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

Les matériels suivants sont pris en charge dans cette version.

- **Serveurs et dispositifs**

- ThinkAgile HX630 V3 (7D6M)
- ThinkAgile HX645 V3 (7D9M)
- ThinkAgile HX650 V3 (7D6N)
- ThinkAgile HX665 V3 (7D9N)
- ThinkAgile MX630 V3 (7D6U)
- ThinkAgile MX650 V3 (7D6S)
- ThinkAgile VX630 V3 (7D6X, 7Z63)
- ThinkAgile VX635 V3 (7D9V)
- ThinkAgile VX645 V3 (7D9K)
- ThinkAgile VX650 V2-DPU (7Z63)
- ThinkAgile VX650 V3 (7D6W)
- ThinkAgile VX650 V3-DPU (7D6W)
- ThinkAgile VX655 V3 (7D9W)
- ThinkAgile VX665 V3 (7D9L)
- ThinkAgile VX850 V3 (7DDK)
- ThinkEdge SE350 V2 (7DA9)
- ThinkEdge SE455 V3 (7DBY)
- ThinkEdge SE360 V2 (7DAM)
- ThinkSystem SD555 V3 (7DDP, 7DDQ)
- ThinkSystem SD650 V3 (7D7M)
- ThinkSystem SD650-I V3 (7D7L)
- ThinkSystem SD650-N V3 (7D7L)
- ThinkSystem SD665 V3 (7D9P)
- ThinkSystem SD665-N V3 (7DAZ)
- ThinkSystem SR630 V3 (7D72, 7D73, 7D74)
- ThinkSystem SR635 V3 (7D9G, 7D9H)
- ThinkSystem SR645 V3 (7D9C, 7D9D)
- ThinkSystem SR650 V3 (7D75, 7D76, 7D77)
- ThinkSystem SR655 V3 (7D9E, 7D9F)
- ThinkSystem SR665 V3 (7D9B, 7D9A)
- ThinkSystem SR675 V3 (7D9Q, 7D9R)
- ThinkSystem SR850 V3 (7D96, 7D97, 7D98)
- ThinkSystem SR860 V3 (7D93, 7D94, 7D95)
- ThinkSystem SR950 V3 (7DC4, 7DC5, 7DC6)
- ThinkSystem ST650 V3 (7D7A, 7D7B)

- **Dispositifs de stockage**

- ThinkSystem DE6400F Système tout flash (7DB6)
  - ThinkSystem DE6400H Système flash hybride (7DB6)
  - ThinkSystem DE6600F Système tout flash (7DB7)
  - ThinkSystem DE6600H Système flash hybride (7DB7)
- **Commutateurs**
    - Commutateur ThinkSystem DB730S FC SAN (7D9J)
    - Directeur SAN FC ThinkSystem DB400D (6684)
    - Directeur SAN FC ThinkSystem DB800D (6682)

Cette version prend en charge les améliorations de planification ou d'installation ci-après du logiciel de gestion.

Fonction	Description
Planification et installation	Retrait de l'algorithme ssh-rsa et ajout des algorithmes ssh-ed25519, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384 et ecdsa-sha2-nistp521 à la liste des algorithmes de clé pris en charge (voir <a href="#">Gestion cryptographique</a> ).

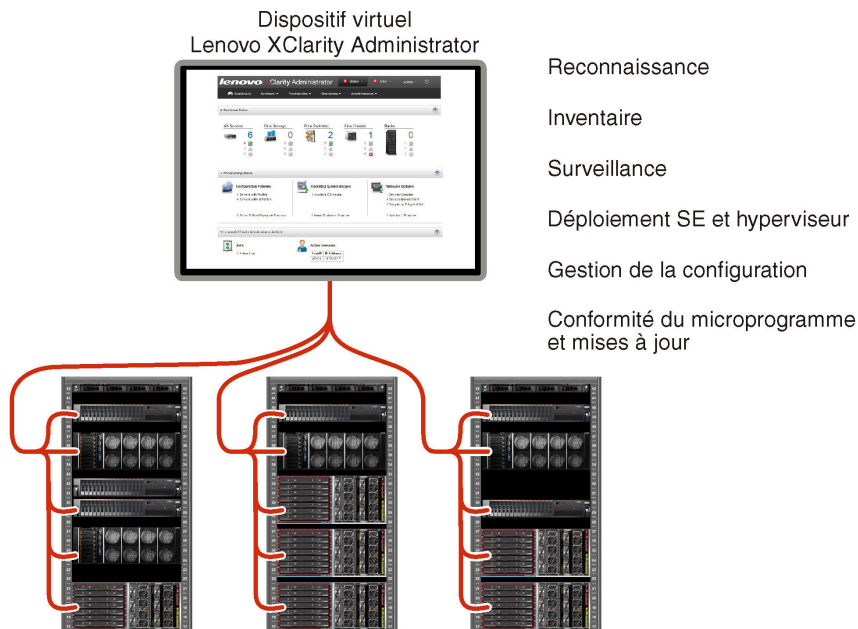
---

# 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](#) et [Gestion des commutateurs](#) dans la documentation en ligne de XClarity Administrator.

**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](#) dans la documentation en ligne de XClarity Administrator.

**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](#) et [Utilisation des alertes](#) dans la documentation en ligne de XClarity Administrator.

**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 de serveurs à l'aide de XClarity Administrator](#) dans la documentation en ligne de XClarity Administrator.

**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](#) dans la documentation en ligne de XClarity Administrator.

#### 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 [Déploiement d'une image du système d'exploitation](#) dans la documentation en ligne de XClarity Administrator.

#### 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](#) dans la documentation en ligne de XClarity Administrator.

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 multifactor 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](#) dans la documentation en ligne de XClarity Administrator.

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 de rôles](#) dans la documentation en ligne de XClarity Administrator.

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](#) dans la documentation en ligne de XClarity Administrator.

### 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](#) dans la documentation en ligne de XClarity Administrator.

- **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](#) dans la documentation en ligne de XClarity Administrator.

## 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](#) dans la documentation en ligne de XClarity Administrator.

## 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 des 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](#).

### 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`





---

## Chapitre 2. Planification pour XClarity Administrator

Avant d'installer Lenovo XClarity Administrator, prenez en compte les remarques suivantes pour vous aider à planifier l'installation et la gestion quotidienne.

---

### Licences et la version d'évaluation gratuite de 90 jours

Lenovo XClarity Administrator propose une licence de période d'évaluation gratuite de 90 jours qui vous permet d'utiliser l'ensemble des fonctions disponibles pendant une durée limitée.

Vous pouvez déterminer l'état de la licence, y compris le nombre de jours restants dans la période d'évaluation, en cliquant sur le menu d'action utilisateur (  ) dans la barre de titre de XClarity Administrator, puis en cliquant sur **À propos de**.

XClarity Administrator prend en charge la licence suivante.

- **Lenovo XClarity Pro.** Chaque licence fournit les droits suivants pour un seul appareil.
  - Service et support pour Lenovo XClarity Integrator
  - Service et support pour XClarity Administrator
  - Fonctions avancées dans XClarity Administrator :
    - Configuration des serveurs à l'aide de modèles de configuration
    - Déploiement des systèmes d'exploitation
    - Signalement de problèmes liés à XClarity Administrator à l'aide de l'appel vers Lenovo (l'appel vers Lenovo pour les alertes matérielles n'est pas affecté).

Vous devez acheter une licence pour chaque appareil géré prenant en charge les fonctions avancées. Une licence n'est pas liée à un appareil spécifique.

La conformité de licence est déterminée en fonction du nombre d'appareils gérés qui prennent en charge les fonctions avancées. Le nombre d'appareils gérés ne doit pas dépasser le nombre total de licences de toutes les clés de licences actives. Si XClarity Administrator n'est pas conforme aux licences installées (par exemple, si des licences expirent ou si la gestion d'appareils supplémentaires dépasse le nombre total de licences actives), vous disposez d'un délai autorisé de 90 jours pour installer des licences appropriées. Chaque fois que XClarity Administrator devient non compatible, le délai autorisé se réinitialise à 90 jours. Si la période de grâce (y compris l'essai gratuit) se termine avant que les licences ne soient conformes, les fonctions avancées sont désactivées pour tous les appareils.

#### Remarques :

- La configuration du serveur et les fonctions de déploiement du système d'exploitation sont désactivées à l'expiration du délai autorisé.
- La fonction Appel vers Lenovo concernant les problèmes de XClarity Administrator (fonction logicielle Appel vers Lenovo) est désactivée lorsque les licences ne sont pas conformes. Aucun délai autorisé n'est disponible pour cette fonctionnalité. Toutefois, la fonctionnalité Appel vers Lenovo pour les alertes matérielles n'est pas affectée.

Si les licences sont déjà installées, aucune nouvelle licence n'est requise lors de la mise à niveau vers une nouvelle édition de XClarity Administrator.

Pour plus d'informations sur l'achat de licences Lenovo XClarity Pro, contactez votre représentant Lenovo ou votre partenaire commercial agréé.

Pour plus d'informations sur l'installation de la licence, voir [Installation de la licence d'activation de l'ensemble des fonctionnalités](#) dans la documentation en ligne de XClarity Administrator.

---

## Configurations matérielles et logicielles requises

Le dispositif de gestion de Lenovo XClarity Administrator s'exécute dans une machine virtuelle sur un système hôte.

### Exigences en matière d'hyperviseur

#### Environnements de conteneur

Les environnements de conteneur ci-après sont pris en charge pour l'exécution de XClarity Administrator en tant que conteneur.

- Docker v20.10.9
- Docker-compose v1.29.2

#### Hyperviseurs

Les hyperviseurs ci-après sont pris en charge pour l'exécution de XClarity Administrator en tant que dispositif virtuel.

- Citrix Hypervisor v8.2
- Citrix XenServer v7.6
- CentOS 7 et 8<sup>1</sup>
- Microsoft Windows Server 2022 avec Hyper-V installé
- Microsoft Windows Server 2019 avec Hyper-V installé
- Microsoft Windows Server 2016 avec Hyper-V installé
- Microsoft Windows Server 2012 R2 avec Hyper-V installé
- Microsoft Windows Server 2012 avec Hyper-V installé
- Hyperviseur Nutanix Acropolis (AHV)
- Red Hat v8.x avec KVM (Kernel-based Virtual Machine) v2.12.0 installé
- Red Hat v7.x avec KVM v1.2.17 installé
- Ubuntu 20.40.2 LTS avec KVM v4.2.3 installé
- VMware ESXi 7.0, U1, U2 et U3
- VMware ESXi 6.7, U1, U2<sup>2</sup> et U3

#### Remarques :

1. CentOS Linux ne reçoit plus de mises à jour par Red Hat. Vous pouvez envisager de migrer vers Red Hat Enterprise Linux (voir la [Red Hat : procédure de conversion de CentOS ou Oracle Linux vers une page Web RHEL](#)).
2. Pour VMware ESXi 6.7 U2, vous devez utiliser l'image ISO VMware-ESXi-6.7.0.update02-13981272-LNV-20190630.iso ou ultérieure.

Pour VMware et Citrix, la machine virtuelle est disponible en tant que modèle OVF. Pour Hyper-V et Nutanix AHV, la machine virtuelle est une image de disque virtuel (VHD). Pour CentOS et KVM, la machine virtuelle est disponible au format qcow2.

**Important :** Pour les environnements Hyper-V qui s'exécutent sur des invités Linux avec une base de noyau 2.6 et qui utilisent de grandes quantités de mémoire pour le dispositif virtuel, vous devez désactiver l'utilisation de l'accès mémoire non uniforme sur le panneau des paramètres Hyper-V du gestionnaire Hyper-V. Lorsque vous modifiez ce paramètre, vous devez redémarrer le service Hyper-V, ce qui a pour conséquence de redémarrer toutes les machines virtuelles en cours d'exécution. Si ce paramètre n'est pas désactivé, des problèmes peuvent survenir lors du démarrage initial du dispositif virtuel XClarity Administrator.

## Configuration matérielle

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](#) dans la documentation en ligne de XClarity Administrator.

## Configuration logicielle

### • Serveur Orchestrator

Si vous gérez un grand nombre d'appareils à l'aide de plusieurs instances de XClarity Administrator, vous pouvez centraliser la surveillance, la gestion, la distribution et l'analyse à l'aide de Lenovo XClarity Orchestrator. XClarity Orchestrator peut prendre en charge un nombre illimité d'instances XClarity Administrator qui gèrent collectivement un maximum de **10 000** dispositifs clients autres que ThinkEdge.

Pour gérer des instances XClarity Administrator de version 4.0 ou ultérieure à l'aide de Lenovo XClarity Orchestrator, XClarity Orchestrator version 2.0 ou ultérieure est requis.

### • Serveur d'authentification

Si vous choisissez d'utiliser un serveur d'authentification externe, seule la session Microsoft Active Directory qui s'exécute sur Windows Server 2008 ou version ultérieure est prise en charge.

Si vous choisissez d'utiliser un fournisseur d'identité SAML, seule la session Microsoft Active Directory Federation Services (AD FS) versions 2.0 ou ultérieures qui s'exécute sur Windows Server 2012 est prise en charge.

- **Serveur NTP**

Un serveur NTP (Network Time Protocol) est requis afin de s'assurer que les horodatages relatifs à tous les événements et alertes reçus à partir d'appareils gérés soient synchronisés avec XClarity Administrator. Assurez-vous que le serveur NTP est accessible via le réseau de gestion (généralement, l'interface Eth0).

**Astuce :** Vous pouvez choisir d'utiliser le système hôte sur lequel XClarity Administrator est installé comme serveur NTP. Dans ce cas, vous devez vous assurer que le système hôte est accessible via le réseau de gestion.

### Ressources pouvant être gérées

Une seule instance XClarity Administrator peut gérer, surveiller et assurer la mise à disposition d'un maximum de **1 000** dispositifs physiques.

Vous pouvez trouver une liste complète des appareils et options pris en charge (par exemple, les E-S, les modules DIMM et les adaptateurs de stockage), les niveaux de microprogramme minimum requis, ainsi que des remarques concernant les limites depuis [Support de XClarity Administrator – Page Web de compatibilité](#) en cliquant sur l'onglet **Compatibilité**, puis en cliquant sur le lien approprié en fonction du type d'appareil.

Pour obtenir des informations générales sur la configuration matérielle et les options d'un appareil spécifique, voir [page Web de Lenovo Server Proven](#).

**Restriction :** si le système hôte sur lequel XClarity Administrator est installé est un serveur rack ou un nœud de traitement géré, vous ne pouvez pas utiliser XClarity Administrator pour appliquer des mises à jour de microprogramme à ce système hôte ou à l'ensemble du châssis en une seule fois. Lorsque des mises à jour de microprogramme sont appliquées au système hôte, celui-ci doit être redémarré. Lorsque vous redémarrez le système hôte, XClarity Administrator redémarre également, ce qui rend XClarity Administrator indisponible et l'empêche de terminer les mises à jour sur le système hôte.

### Navigateurs Web pris en charge

L'interface Web XClarity Administrator fonctionne avec ces navigateurs Web.

- 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)

---

## Pare-feux et serveurs proxy

Certaines fonctions de Lenovo XClarity Administrator, y compris les mises à jour du serveur gestion, les mises à jour de microprogramme, la maintenance et le support, nécessitent l'accès à Internet. Si vous avez des pare-feux dans votre réseau, configurez-les afin de permettre au serveur de gestion XClarity Administrator d'effectuer ces opérations. Si le serveur de gestion ne dispose pas d'un accès direct à Internet, configurez XClarity Administrator pour l'utilisation d'un serveur proxy.

### Pare-feux

Vérifiez que les noms DNS et les ports sont ouverts sur le pare-feu.

**Remarque :** Les adresses IP sont susceptibles d'être modifiées. Utilisez des noms DNS chaque fois que possible.

Tableau 1. Connexions Internet requises

Nom DNS	Adresse IPv4	Adresse IPv6	les ports,	Protocoles
<b>Télécharger les clés d'activation de licence</b>				
fod.lenovo.com	N/A	N/A	443	https
<b>Télécharger les bulletins de maintenance</b>				
download.lenovo.com/servers/LXCA_Bulletin_Service.json	N/A	N/A	443 et 80	https
<b>Télécharger des mises à jour (mises à jour du serveur de gestion, mises à jour de microprogramme, UpdateXpress System Packs (pilotes de périphérique SE) et modules de référentiel)</b>				
datacentersupport.lenovo.com	N/A	N/A	443 et 80	https
download.lenovo.com	N/A	N/A	443 et 80	https
filedownload.lenovo.com	N/A	N/A	443 et 80	https
support.lenovo.com	N/A	N/A	443 et 80	https et http
supportapi.lenovo.com	N/A	N/A	443 et 80	https
<b>Téléchargez le microprogramme (Flex System x220, x222, x240, x280 X6, x440, x480 X6, x880 X6, certains commutateurs Flex et des modules CMM première génération seulement)</b>				
www.ibm.com	129.42.56.216, 129.42.58.216, 129.42.60.216, 129.42.160.51, 207.25.252.19-7	N/A	443 et 80	https et http
www-03.ibm.com	204.146.30.17	N/A	443 et 80	https et http
download3.boulder.ibm.com	170.225.126.2-4	N/A	443	https
download4.boulder.ibm.com	170.225.126.4-3	N/A	443 et 80	https et http
delivery04-bld.dhe.ibm.com	170.225.126.4-5	N/A	443 et 80	https et http
delivery04-mul.dhe.ibm.com	170.225.126.4-6	N/A	443 et 80	https et http
delivery04.dhe.ibm.com	170.225.126.4-4	N/A	443 et 80	https et http
<b>Charger des données de maintenance vers le support Lenovo (Appel vers Lenovo)</b>				
soaus.lenovo.com	3.222.8.29, 52.6.14.20	N/A	443	https
logupload.lenovo.com/BLL/Logupload.ashx	N/A	N/A	443 et 80	https

Tableau 1. Connexions Internet requises (suite)

Nom DNS	Adresse IPv4	Adresse IPv6	les ports,	Protoco- les
<b>Charger des données de maintenance vers la Fonction de téléchargement Lenovo</b>				
logupload.lenovo.com/BLL/ Logupload.ashx	N/A	N/A	443 et 80	https
<b>Télécharger les informations relatives à la garantie</b>				
ibase.lenovo.com (worldwide)	N/A	N/A	443 et 80	https et http
service.lenovo.com.cn (Chine uniquement)	114.247.140.2- 12 (Chine uniquement)	N/A	83	http
supportapi.lenovo.com	N/A	N/A	443 et 80	https et http

**Attention** : Pour les utilisateurs en Chine, pour l'obtention des informations de garantie des appareils gérés à l'aide de XClarity Administrator, vous devez effectuer une mise à jour vers XClarity Administrator version 1.3.1 ou version ultérieure.

### Serveur proxy

Si le serveur de gestion ne dispose pas d'un accès direct à Internet, vérifiez qu'il est configuré pour utiliser un serveur proxy HTTP (voir [Configuration de l'accès réseau](#)).

- 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.

## Disponibilité de port

Plusieurs ports doivent être disponibles, en fonction de la façon dont les pare-feu sont implémentés dans votre environnement. Si les ports requis sont bloqués ou utilisés par un autre processus, certaines fonctions de Lenovo XClarity Administrator peuvent ne pas fonctionner.

Pour déterminer quels ports doivent être ouverts en fonction de votre environnement, consultez les sections suivantes. Les tableaux des sections suivantes donnent des informations sur l'utilisation de chaque port dans XClarity Administrator, l'appareil géré affecté, le protocole (TCP ou UDP) et la direction du trafic. Le trafic *entrant* identifie les flux de l'appareil géré ou des systèmes externes sur XClarity Administrator, de sorte que les ports doivent s'ouvrir sur le dispositif XClarity Administrator. Le trafic *Sortant* va de XClarity Administrator à l'appareil géré.

- [Accéder au serveur XClarity Administrator](#)
- [Accès entre XClarity Administrator et les appareils gérés](#)
- [Accès entre XClarity Administrator et le réseau de données pour le déploiement SE et les mises à jour de pilote de périphérique SE](#)

### Accéder au serveur XClarity Administrator

Si le serveur XClarity Administrator et tous les appareils gérés sont protégés par un pare-feu, et que vous avez l'intention d'accéder à ces appareils à partir d'un navigateur qui se trouve à l'extérieur du pare-feu, vous devez vous assurer que les ports de XClarity Administrator sont ouverts. Si vous utilisez SNMP et SMTP pour

la gestion des événements, vous devrez peut-être également vous assurer que les ports utilisés par le serveur XClarity Administrator pour l'acheminement d'événement sont ouverts.

Le serveur XClarity Administrator écoute sur les ports répertoriés dans le tableau suivant, et répond sur ces mêmes ports.

**Remarques :**

- XClarity Administrator est une application RESTful qui communique en toute sécurité via TCP sur le port 443.
- XClarity Administrator peut éventuellement être configuré pour établir des connexions sortantes à des services externes, tels que LDAP, SMTP ou syslog. Ces connexions peuvent nécessiter des ports supplémentaires qui ne sont généralement pas configurables par l'utilisateur et ne sont pas inclus dans cette liste. Ces connexions peuvent aussi nécessiter l'accès à un serveur DNS sur le port TCP ou UDP 53 pour résoudre les noms de serveur externe.

Communication	Dispositif XClarity Administrator	Serveurs d'authentification externes	Services d'acheminement d'événement	Services Lenovo (y compris Appel vers Lenovo)
<b>Sortant</b> (ports ouverts sur des systèmes externes)	<ul style="list-style-type: none"> <li>• DNS - TCP/UDP sur le port <b>53</b></li> </ul>	<ul style="list-style-type: none"> <li>• LDAP – TCP sur le port <b>389</b><sup>1</sup></li> <li>• LDAPS-TCP sur le port <b>636</b></li> <li>• Authentification SAML - TCP sur les ports <b>3268, 3269</b></li> </ul>	<ul style="list-style-type: none"> <li>• Serveur FTP - TCP sur le port <b>21</b><sup>1</sup></li> <li>• Serveur e-mail (SMTP) - UDP sur le port <b>25</b><sup>1</sup></li> <li>• Service Web REST (HTTP) – UDP sur le port <b>80</b><sup>1</sup></li> <li>• Gestionnaire SNMP - UDP sur le port <b>161</b><sup>2</sup>, <b>162</b><sup>1</sup></li> <li>• MS Azure - UDP sur le port <b>443</b><sup>1</sup></li> <li>• Syslog - UDP sur le port <b>514</b><sup>1</sup></li> <li>• Apple Push<sup>3</sup> - TCP sur les ports <b>443, 2195, 5223</b></li> <li>• Google Push<sup>4</sup> - TCP sur les ports <b>443, 5288, 5299, 5230</b></li> </ul>	<ul style="list-style-type: none"> <li>• Garantie (Chine uniquement) - TCP sur le port <b>83</b><sup>5</sup></li> <li>• HTTPS (appel vers Lenovo) - TCP sur le port <b>443</b></li> </ul>
<b>Entrant</b> (ports ouverts sur l'appareil XClarity Administrator)	<ul style="list-style-type: none"> <li>• HTTPS - TCP sur le port <b>443</b></li> </ul>	Sans objet	<ul style="list-style-type: none"> <li>• SNMP – UDP sur le port <b>161</b></li> </ul>	Sans objet

1. Il s'agit du port par défaut. Ce port est configurable à partir de l'interface utilisateur.
2. Ce port est utilisé lorsque l'acheminement d'événement SNMP avec une authentification utilisateur est configuré.

3. Ouvrez ce port lorsque le Wi-Fi est protégé par un pare-feu ou un nom de point d'accès (APN) privé pour les données cellulaires. Une connexion directe et sans proxy est requise pour les serveurs APN sur ce port. Ce port est utilisé comme un basculement sur le Wi-Fi uniquement, lorsque les appareils ne peuvent pas joindre le service de notifications push Apple sur le port 5223. La plage d'adresses IP est 17.0.0.0/8.
4. Pour connaître la plage d'adresses IP, voir Google ASN 15169. Le domaine est android.googleapis.com.
5. Bien que cela ne soit pas requis hors de Chine, XClarity Administrator peut essayer de se connecter à ce service dans d'autres pays.

### Accès entre XClarity Administrator et les appareils gérés

Si des appareils gérés (par exemple, des nœuds de traitement ou des serveurs rack) sont protégés par un pare-feu et que vous avez l'intention de gérer ces appareils à partir d'un serveur XClarity Administrator qui se trouve à l'extérieur de ce pare-feu, vous devez vous assurer que tous les ports impliqués dans des communications entre XClarity Administrator et le contrôleur de gestion de la carte mère de chaque appareil géré sont ouverts.

Si vous prévoyez d'installer des systèmes d'exploitation sur des appareils gérés à l'aide de XClarity Administrator, consultez la liste des ports fournie dans la section [Accès entre XClarity Administrator et le réseau de données pour le déploiement SE et les mises à jour de pilote de périphérique SE](#).

#### • CMM Flex Chassis

Communication	CMM Flex Chassis
<b>Sortant</b> (ports ouverts sur des systèmes externes)	<ul style="list-style-type: none"> <li>- SLP - UDP/TCP sur le port <b>427</b></li> <li>- CIM HTTP - TCP sur le port <b>5988</b><sup>2</sup></li> <li>- CIM HTTPS - TCP sur le port <b>5989</b></li> <li>- Commande TCP - TCP sur le port <b>6090</b><sup>2</sup></li> <li>- Commande TCP sécurisé - TCP sur le port <b>6091</b></li> </ul>
<b>Entrant</b> (ports ouverts sur l'appareil XClarity Administrator)	<ul style="list-style-type: none"> <li>- SFTP - TCP sur le port <b>22</b><sup>1</sup></li> <li>- Indications CIM HTTPS - TCP <b>9090</b></li> <li>- LDAPS - TCP sur les ports <b>50637</b></li> </ul>

1. Ce port est utilisé pour le transfert de mises à jour du microprogramme via SFTP.
2. Par défaut, la gestion est réalisée via des ports sécurisés. Les ports non sécurisés sont en option.

#### • Serveurs et nœuds de traitement



Communi- cation	ThinkSystem et ThinkAgile	System x	Flex System	ThinkServer
<b>Sortant</b> (ports ouverts sur des systèmes externes)	<ul style="list-style-type: none"> <li>- SFTP – TCP sur le port <b>115</b></li> <li>- SLP - UDP/TCP sur le port <b>427</b></li> <li>- HTTPS - TCP sur le port <b>443</b></li> <li>- Reconnaissance SSDP – UDP sur le port <b>1900</b></li> <li>- Contrôle à distance – TCP sur le port <b>3888</b><sup>4</sup></li> <li>- KVM distant – TCP sur le port <b>3889</b><sup>4</sup></li> <li>- CIM HTTPS - TCP sur le port <b>5989</b></li> <li>- Mises à jour de microprogramme - TCP sur le port <b>6990</b><sup>5</sup></li> </ul>	<ul style="list-style-type: none"> <li>- SLP - UDP/TCP sur le port <b>427</b></li> <li>- HTTPS - TCP sur le port <b>443</b></li> <li>- IPMI – TCP sur le port <b>623</b></li> <li>- Contrôle à distance – TCP sur le port <b>3888</b><sup>4</sup></li> <li>- KVM distant – TCP sur le port <b>3889</b><sup>4</sup></li> <li>- CIM HTTP – TCP sur le port <b>5988</b><sup>3</sup></li> <li>- CIM HTTPS – TCP sur le port <b>5989</b><sup>3</sup></li> <li>- Mises à jour de microprogramme - TCP sur le port <b>6990</b><sup>5</sup></li> </ul>	<ul style="list-style-type: none"> <li>- SLP - UDP/TCP sur le port <b>427</b></li> <li>- Contrôle à distance – TCP sur le port <b>3888</b><sup>4</sup></li> <li>- KVM distant – TCP sur le port <b>3889</b><sup>1, 4</sup></li> <li>- CIM HTTP – TCP sur le port <b>5988</b><sup>3</sup></li> <li>- CIM HTTPS – TCP sur le port <b>5989</b><sup>3</sup></li> <li>- Mises à jour de microprogramme - TCP sur le port <b>6990</b><sup>5</sup></li> </ul>	<ul style="list-style-type: none"> <li>- Alertes SNMP – UDP sur le port <b>162</b></li> <li>- IPMI – UDP sur le port <b>623</b></li> </ul>
<b>Entrant</b> (ports ouverts sur l'appareil XClarity Adminis- trator)	<ul style="list-style-type: none"> <li>- SFTP – TCP sur le port <b>22</b><sup>2</sup></li> <li>- HTTPS - TCP sur le port <b>443</b></li> <li>- Reconnaissance SSDP – UDP sur le port <b>1900</b></li> <li>- Mises à jour de microprogramme - TCP sur le port <b>6990</b><sup>5</sup></li> <li>- Indications CIM HTTPS - TCP <b>9090</b></li> <li>- LDAPS – TCP sur les ports <b>50636</b><sup>6</sup>, <b>50637</b></li> </ul>	<ul style="list-style-type: none"> <li>- SFTP – TCP sur le port <b>22</b><sup>2</sup></li> <li>- HTTPS - TCP sur le port <b>443</b></li> <li>- Mises à jour de microprogramme - TCP sur le port <b>6990</b><sup>5</sup></li> <li>- Indications CIM HTTPS - TCP <b>9090</b></li> <li>- LDAPS – TCP sur les ports <b>50636</b><sup>6</sup>, <b>50637</b></li> </ul>	<ul style="list-style-type: none"> <li>- SFTP – TCP sur le port <b>22</b><sup>2</sup></li> <li>- HTTPS - TCP sur le port <b>443</b></li> <li>- Mises à jour de microprogramme - TCP sur le port <b>6990</b><sup>5</sup></li> <li>- Indications CIM HTTPS - TCP <b>9090</b></li> <li>- LDAPS – TCP sur les ports <b>50636</b><sup>6</sup>, <b>50637</b></li> </ul>	<ul style="list-style-type: none"> <li>- Alertes SNMP – UDP sur le port <b>162</b></li> </ul>

1. Ce port doit être ouvert uniquement pour les serveurs avec IMM2.
2. Ce port est utilisé pour le transfert de mises à jour du microprogramme via SFTP.
3. Par défaut, la gestion est réalisée via des ports sécurisés. Les ports non sécurisés sont en option.
4. Le contrôle et KVM à distance sont démarrés depuis le navigateur Web, et non le serveur XClarity Administrator.
5. Ce port est utilisé pour se connecter au S.E. BMU pour transférer des fichiers et exécuter les commandes de mise à jour.
6. Ce port est requis pour configurer des serveurs à l'aide de modèles de configuration.

- **Commutateurs Rack et Flex**

Communication	Commutateur en rack	Commutateurs Flex
<b>Sortant</b> (ports ouverts sur des systèmes externes)	<ul style="list-style-type: none"> <li>- SSH – TCP sur le port <b>22</b><sup>1,3</sup></li> <li>- SNMP - UDP sur le port <b>161</b><sup>2</sup></li> <li>- SLP - UDP/TCP sur le port <b>427</b><sup>6</sup></li> <li>- HTTPS – TCP sur le port <b>443</b><sup>7</sup></li> </ul>	<ul style="list-style-type: none"> <li>- SSH – TCP sur le port <b>22</b><sup>3</sup></li> <li>- SNMP - UDP sur le port <b>161</b><sup>5</sup></li> </ul>
<b>Entrant</b> (ports ouverts sur l'appareil XClarity Administrator)	<ul style="list-style-type: none"> <li>- SFTP – TCP sur le port <b>22</b><sup>4</sup></li> <li>- Alertes SNMP – TCP sur les ports <b>162</b><sup>2</sup></li> </ul>	<ul style="list-style-type: none"> <li>- SFTP – TCP sur le port <b>22</b><sup>4</sup></li> <li>- Alertes SNMP – TCP sur le port <b>162</b><sup>2</sup></li> </ul>

1. Concernant les commutateurs de rack ENOS, ce port permet de configurer les données d'identification Head of Stack (HoS) utilisées entre les commutateurs CMM et Flex, d'activer l'emplacement du microprogramme et d'effacer les clés d'hôte SSH avant les opérations de transfert de fichier SFTP.
2. Ce port doit être ouvert sur l'appareil XClarity Administrator (entrant) quand les commutateurs se trouvent sur un réseau autre que XClarity Administrator, de sorte que XClarity Administrator peut recevoir les événements pour ces appareils.
3. Ce port est utilisé pour la gestion (SSH).
4. Ce port est utilisé pour le transfert de mises à jour du microprogramme via SFTP.
5. Pour les commutateurs de rack ENOS, ce port est utilisé pour transférer des données d'inventaire.
6. Ce port est utilisé pour la détection (SSH).
7. Ce port est utilisé pour appliquer les mises à jour du microprogramme.

• **Dispositifs de stockage**

Communication	Dispositifs de stockage
<b>Sortant</b> (ports ouverts sur des systèmes externes)	<ul style="list-style-type: none"> <li>- FTP – TCP sur le port <b>21</b></li> <li>- SFTP – TCP sur le port <b>22</b><sup>2</sup></li> <li>- SLP - UDP/TCP sur le port <b>427</b></li> <li>- HTTPS – TCP sur le port <b>443</b><sup>1</sup></li> </ul>
<b>Entrant</b> (ports ouverts sur l'appareil XClarity Administrator)	<ul style="list-style-type: none"> <li>- HTTPS – TCP sur le port <b>443</b><sup>2</sup></li> <li>- Alertes SNMP – UDP sur le port <b>115</b></li> </ul>

1. Ce port est utilisé pour le transfert de mises à jour du microprogramme.
2. Ce port est utilisé pour le transfert et l'application de mises à jour du microprogramme.

## Accès entre XClarity Administrator et le réseau de données pour le déploiement SE et les mises à jour de pilote de périphérique SE

Communication	Déploiement SE <sup>1, 2, 3</sup>	Mises à jour de pilote de périphériques SE <sup>2</sup>
<b>Sortant</b> (ports ouverts sur des systèmes externes)		<ul style="list-style-type: none"><li>• WinRM sur HTTP - TCP sur le port <b>5985</b><sup>5</sup></li><li>• WinRM sur HTTPS - TCP sur le port <b>5986</b><sup>6</sup></li></ul>
<b>Entrant</b> (ports ouverts sur l'appareil XClarity Administrator)	<ul style="list-style-type: none"><li>• Communication SMB – TCP sur le port <b>445</b><sup>4</sup></li><li>• HTTPS (sauf ThinkServer) - TCP sur le port <b>8443</b><sup>6</sup></li></ul>	<ul style="list-style-type: none"><li>• Communication SMB – TCP sur le port <b>445</b><sup>4</sup></li></ul>

1. Si vous avez configuré XClarity Administrator pour utiliser un réseau de déploiement de système d'exploitation, les ports doivent être ouverts sur ce réseau.
2. Pour obtenir la liste des ports qui doivent être disponibles pour déployer des systèmes d'exploitation, voir [Disponibilité de port pour les systèmes d'exploitation déployés](#) dans la documentation en ligne de XClarity Administrator. Par exemple, si le déploiement du système d'exploitation est configuré pour utiliser le réseau de données (eth1), ces ports doivent être ouverts sur ce réseau.
3. Chaque instance XClarity Administrator dispose d'une autorité de certification unique (CA) qui est utilisée uniquement pour le déploiement SE. Cette autorité de certification signe un certificat qui est utilisé pour le serveur cible sur le port 8443. Lorsque le déploiement SE est initié, le certificat de l'autorité de certification est inclus dans l'image SE qui est envoyée au serveur cible. Dans le cadre du processus de déploiement, le serveur se reconnecte sur le port 8443, puis vérifie le certificat fourni par le port 8443 lors de l'établissement de liaison car ils comportent le certificat de l'autorité de certification.
4. Ce port est utilisé pour transférer des fichiers de pilote Windows.
5. Ce port est utilisé pour la connexion au serveur cible WinRM.
6. Ce port est utilisé pour échanger des données entre le SE cible et XClarity Administrator, dont les états et les images SE.

---

## 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.

---

## Remarques sur le réseau

Lors de la planification de l'installation de Lenovo XClarity Administrator, tenez compte de la topologie de réseau qui est implémentée dans votre environnement et de la façon dont XClarity Administrator s'intègre dans cette topologie.

**Important** : Configurez les appareils et les composants de manière à réduire au minimum les modifications d'adresse IP. Envisagez d'utiliser des adresses IP statiques au lieu du protocole DHCP (Dynamic Host Configuration Protocol). Si le protocole DHCP est utilisé, faites en sorte que les modifications d'adresse IP soient réduits au minimum.

## Limitations de la configuration IP

Pour les fonctions et les appareils gérés ci-dessous, les interfaces réseau doivent être configurées avec une adresse IPv4. Les adresses IPv6 ne sont pas prises en charge.

- Mises à jour du microprogramme pour les dispositifs Lenovo Storage
- Serveurs ThinkServer
- Dispositifs Lenovo Storage

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.

La conversion d'adresses réseau (NAT), qui remappe un espace d'adresse IP dans un autre, n'est pas prise en charge.

## Types de réseaux

En général la plupart des environnements implémentent les types de réseaux suivants. Suivant vos exigences, vous ne pourrez implémenter qu'un seul de ces réseaux ou vous pourrez les implémenter tous les trois.

- **Réseau de gestion**

Le réseau de gestion est généralement réservé aux communications entre Lenovo XClarity Administrator et les processeurs de gestion pour les appareils gérés. Par exemple, le réseau de gestion peut être configuré pour inclure XClarity Administrator, les modules CMM pour chaque châssis géré et le contrôleur de gestion de la carte mère de chaque serveur géré par XClarity Administrator.

- **Réseau de données**

Le réseau de données est généralement utilisé pour les communications entre les systèmes d'exploitation installés sur les serveurs et l'intranet de l'entreprise, Internet ou les deux.

- **Réseau de déploiement du système d'exploitation**

Dans certains cas, un réseau de déploiement du système d'exploitation est configuré pour séparer les communications nécessaires au déploiement de systèmes d'exploitation sur des serveurs. S'il est implémenté, ce réseau inclut généralement XClarity Administrator et tous les hôtes de serveur.

Au lieu d'implémenter un réseau de déploiement du système d'exploitation distinct, vous pouvez choisir de combiner cette fonctionnalité dans le réseau de gestion ou dans le réseau de données.

## Configurations réseau

Vous pouvez configurer Lenovo XClarity Administrator pour l'utilisation d'une ou de deux interfaces réseau.

### 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.

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 <ul style="list-style-type: none"> <li>• Reconnaissance et gestion</li> <li>• Configuration du serveur</li> <li>• Mises à jour du microprogramme</li> <li>• Collecte des données de maintenance</li> <li>• Notification de problèmes automatique (par exemple, l'Appel Lenovo et la fonction de mise à jour Lenovo)</li> <li>• Récupération des données relatives à la garantie</li> <li>• Déploiement SE</li> <li>• Mises à jour de pilote de périphériques SE</li> </ul>	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 <ul style="list-style-type: none"> <li>• Reconnaissance et gestion</li> <li>• Configuration du serveur</li> <li>• Mises à jour du microprogramme</li> <li>• Collecte des données de maintenance</li> <li>• Notification de problèmes automatique (par exemple, l'Appel Lenovo et la fonction de mise à jour Lenovo)</li> <li>• Récupération des données relatives à la garantie</li> <li>• Déploiement SE</li> <li>• Mises à jour de pilote de périphériques SE</li> </ul>	Réseau de données <ul style="list-style-type: none"> <li>• Aucun</li> </ul>
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 <ul style="list-style-type: none"> <li>• Reconnaissance et gestion</li> <li>• Configuration du serveur</li> <li>• Mises à jour du microprogramme</li> <li>• Collecte des données de maintenance</li> <li>• Notification de problèmes automatique (par exemple, l'Appel Lenovo et la fonction de mise à jour Lenovo)</li> <li>• Récupération des données relatives à la garantie</li> </ul>	Réseau de données <ul style="list-style-type: none"> <li>• Déploiement SE</li> <li>• Mises à jour de pilote de périphériques SE</li> </ul>

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 sans prise en charge pour le déploiement SE et les mises à jour de pilote de périphérique	Réseau de gestion <ul style="list-style-type: none"> <li>• Reconnaissance et gestion</li> <li>• Configuration du serveur</li> <li>• Mises à jour du microprogramme</li> <li>• Collecte des données de maintenance</li> <li>• Notification de problèmes automatique (par exemple, l'Appel Lenovo et la fonction de mise à jour Lenovo)</li> <li>• Récupération des données relatives à la garantie</li> </ul>	Réseau de données <ul style="list-style-type: none"> <li>• Aucun</li> </ul>
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 <ul style="list-style-type: none"> <li>• Reconnaissance et gestion</li> <li>• Configuration du serveur</li> <li>• Mises à jour du microprogramme</li> <li>• Collecte des données de maintenance</li> <li>• Notification de problèmes automatique (par exemple, l'Appel Lenovo et la fonction de mise à jour Lenovo)</li> <li>• Récupération des données relatives à la garantie</li> </ul>	Aucun

## Réseau de données et de gestion unique

Dans cette topologie de réseau, les communications de gestion, les communications de données et le déploiement du système d'exploitation se produisent sur le même réseau. Cette topologie est appelée réseau *convergé*.

**Important** : L'implémentation d'un réseau de données et de gestion partagé peut entraîner des interruptions du trafic avec, par exemple, des paquets ignorés ou des problèmes liés à la connectivité du réseau de gestion, en fonction de votre configuration réseau (par exemple, si le trafic en provenance de serveurs a une priorité haute et qu'un trafic en provenance des contrôleurs de gestion a une priorité faible). Le réseau de gestion utilise le trafic UDP en plus du trafic TCP. Le trafic UDP peut avoir une priorité plus faible lorsque le trafic réseau est élevé.

Lorsque vous installez Lenovo XClarity Administrator, définissez l'interface réseau eth0 en tenant compte des remarques suivantes :

- 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.

- Vous pouvez installer XClarity Administrator sur tout système qui satisfait aux exigences de XClarity Administrator, comprenant un serveur géré uniquement lorsque vous implémentez une topologie de réseau de données et de gestion unique ou une topologie de réseau de données séparées virtuellement et de gestion ; toutefois, vous ne pouvez pas utiliser XClarity Administrator pour appliquer des mises à jour de microprogramme au serveur géré. Même dans ce cas, seule une partie du microprogramme est appliquée à l'activation immédiate et XClarity Administrator force le serveur cible à redémarrer, ce qui redémarrerait XClarity Administrator également. Une fois le microprogramme appliqué à l'activation reportée, seule une partie est appliquée lorsque l'hôte XClarity Administrator est redémarré.

Vous pouvez également configurer une seconde interface réseau pour la connexion au même réseau à partir de XClarity Administrator afin de prendre en charge la redondance.

La figure suivante présente un exemple d'implémentation pour une topologie de réseau convergé.

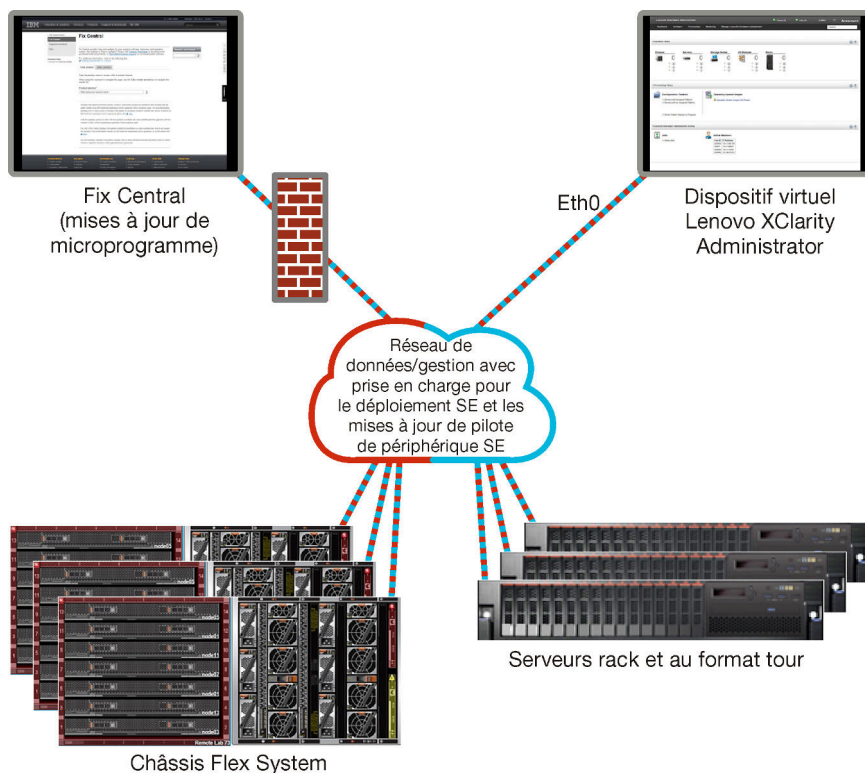


Figure 1. Exemple d'implémentation d'un réseau unique pour la gestion, les données et le déploiement du système d'exploitation

## Réseau de données et réseau de gestion séparés physiquement

Dans cette topologie de réseau, le réseau de gestion et le réseau de données sont des réseaux séparés physiquement, et le réseau de déploiement du système d'exploitation est configuré comme faisant partie du réseau de gestion ou du réseau de données.

Lorsque vous installez Lenovo XClarity Administrator, définissez les paramètres réseau en tenant compte des remarques suivantes :

- 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.

Figure 2 « Exemple d'implémentation de réseaux de données et de gestion séparés physiquement avec le réseau du système d'exploitation faisant partie du réseau de données » à la page 25 présente un exemple d'implémentation de réseaux de gestion et de données séparés dans lesquels le réseau de déploiement du système d'exploitation est configuré dans le cadre du réseau de données.

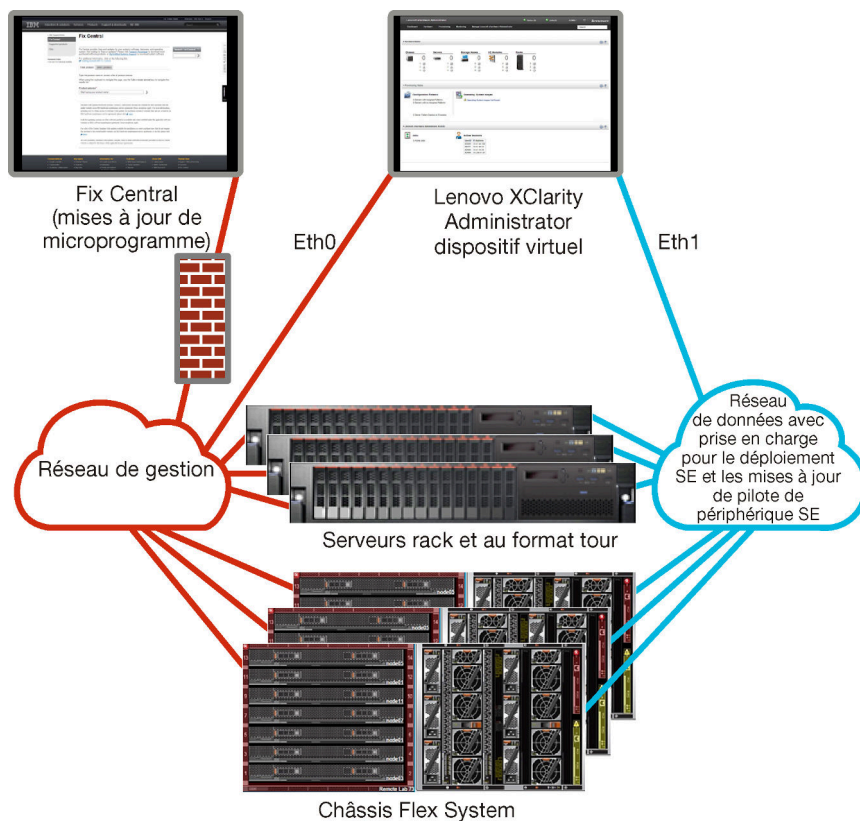


Figure 2. Exemple d'implémentation de réseaux de données et de gestion séparés physiquement avec le réseau du système d'exploitation faisant partie du réseau de données

Figure 3 « Exemple d'implémentation de réseaux de données et de gestion séparés physiquement avec le réseau du système d'exploitation faisant partie du réseau de gestion » à la page 26 présente un exemple d'implémentation de réseaux de gestion et de données séparés dans lequel le réseau de déploiement du système d'exploitation est configuré comme faisant partie du réseau de données. Dans cette implémentation, XClarity Administrator n'a pas besoin d'une connectivité au réseau de données.

**Remarque :** Si le réseau de déploiement du système d'exploitation 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, si nécessaire.

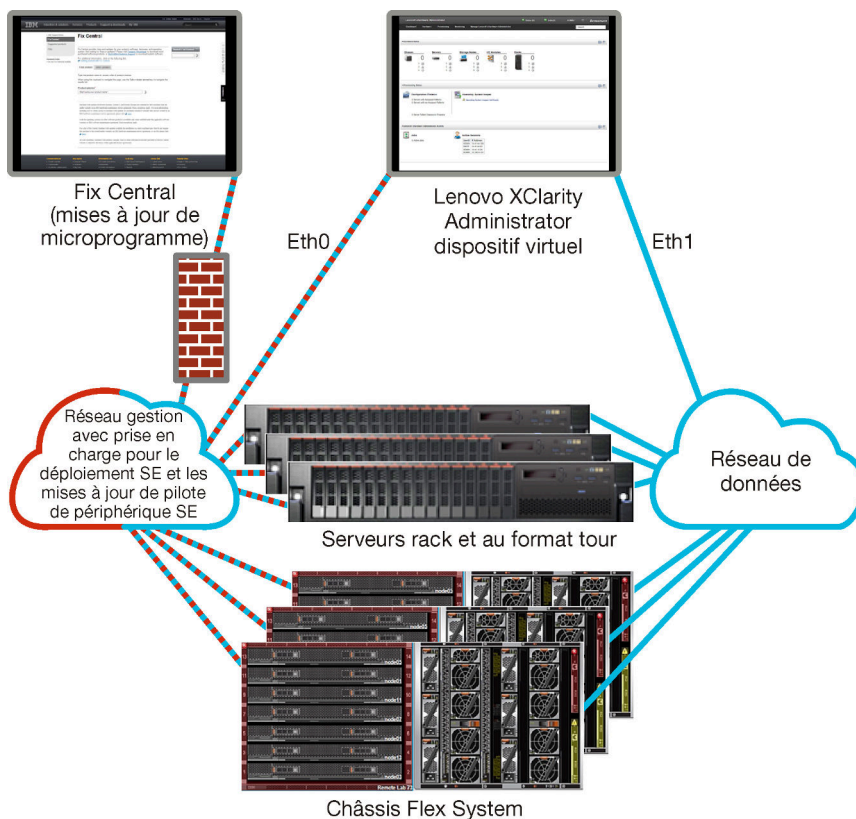


Figure 3. Exemple d'implémentation de réseaux de données et de gestion séparés physiquement avec le réseau du système d'exploitation faisant partie du réseau de gestion

## Réseau de données et réseau de gestion séparés virtuellement

Dans cette topologie, le réseau de données et le réseau de gestion sont virtuellement distincts. Les modules du réseau de données et les modules du réseau de gestion sont envoyés sur la même connexion physique. Le marquage VLAN est utilisé sur tous les modules de données du réseau de gestion afin de conserver le trafic entre les deux réseaux séparé.

**Remarque :** Si Lenovo XClarity Administrator est installé sur un hôte s'exécutant sur un serveur géré dans un châssis, vous ne pouvez pas utiliser XClarity Administrator pour appliquer des mises à jour du microprogramme à l'intégralité de ce châssis en même temps. Lorsque des mises à jour de microprogramme sont appliquées, le système hôte doit être redémarré.

Lorsque vous installez XClarity Administrator, définissez les paramètres réseau en tenant compte des remarques suivantes :

- 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 périphérie 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.

- Vous pouvez installer XClarity Administrator sur tout système qui satisfait aux exigences de XClarity Administrator, comprenant un serveur géré uniquement lorsque vous implémentez une topologie de réseau de données et de gestion unique ou une topologie de réseau de données séparées virtuellement et de gestion ; toutefois, vous ne pouvez pas utiliser XClarity Administrator pour appliquer des mises à jour de microprogramme au serveur géré. Même dans ce cas, seule une partie du microprogramme est appliquée à l'activation immédiate et XClarity Administrator force le serveur cible à redémarrer, ce qui redémarrerait XClarity Administrator également. Une fois le microprogramme appliqué à l'activation reportée, seule une partie est appliquée lorsque l'hôte XClarity Administrator est redémarré.

La [Figure 4 « Exemple d'implémentation de réseaux de données et de gestion séparés virtuellement avec le réseau du système d'exploitation faisant partie du réseau de données »](#) à la [page 28](#) présente un exemple d'implémentation de réseaux de gestion et de données virtuellement séparés dans lequel le réseau de déploiement du système d'exploitation est configuré dans le cadre du réseau de données. Dans cet exemple, XClarity Administrator est installé sur un serveur géré dans un châssis.

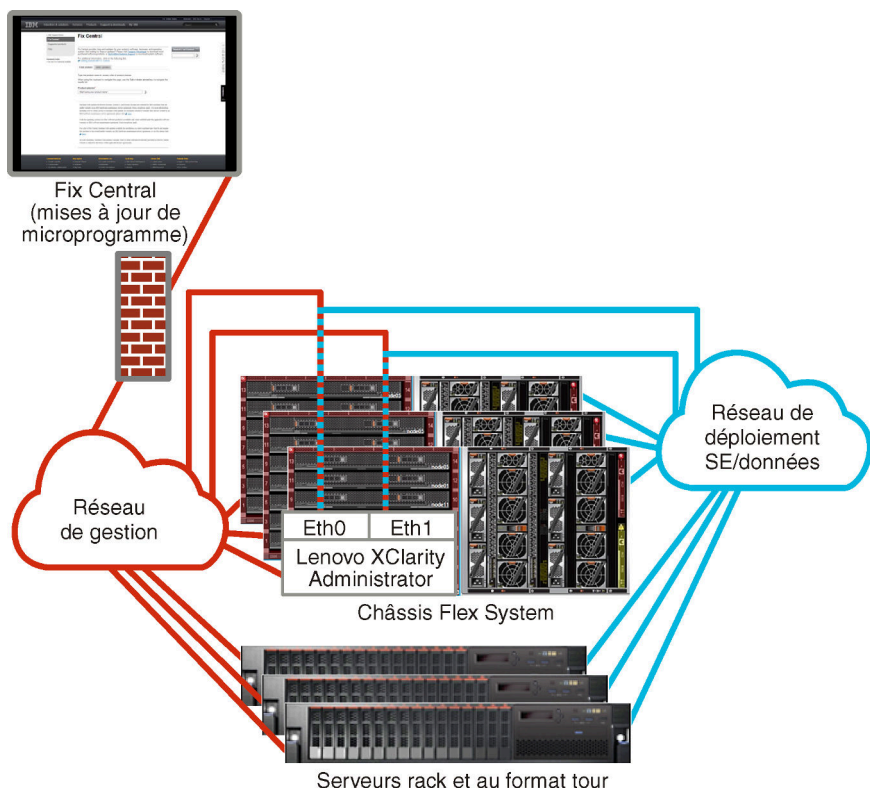


Figure 4. Exemple d'implémentation de réseaux de données et de gestion séparés virtuellement avec le réseau du système d'exploitation faisant partie du réseau de données

Figure 5 « Exemple d'implémentation de réseaux de gestion et de données virtuellement séparés avec le réseau du système d'exploitation faisant partie du réseau de gestion » à la page 29 présente un exemple d'implémentation de réseaux de gestion et de données virtuellement séparés dans lesquels le réseau de déploiement du système d'exploitation est configuré dans le cadre du réseau de gestion, et XClarity Administrator est installé sur un serveur géré dans un châssis. Dans cette implémentation, XClarity Administrator n'a pas besoin d'une connectivité au réseau de données.

**Remarque :** Si le réseau de déploiement du système d'exploitation 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, si nécessaire.



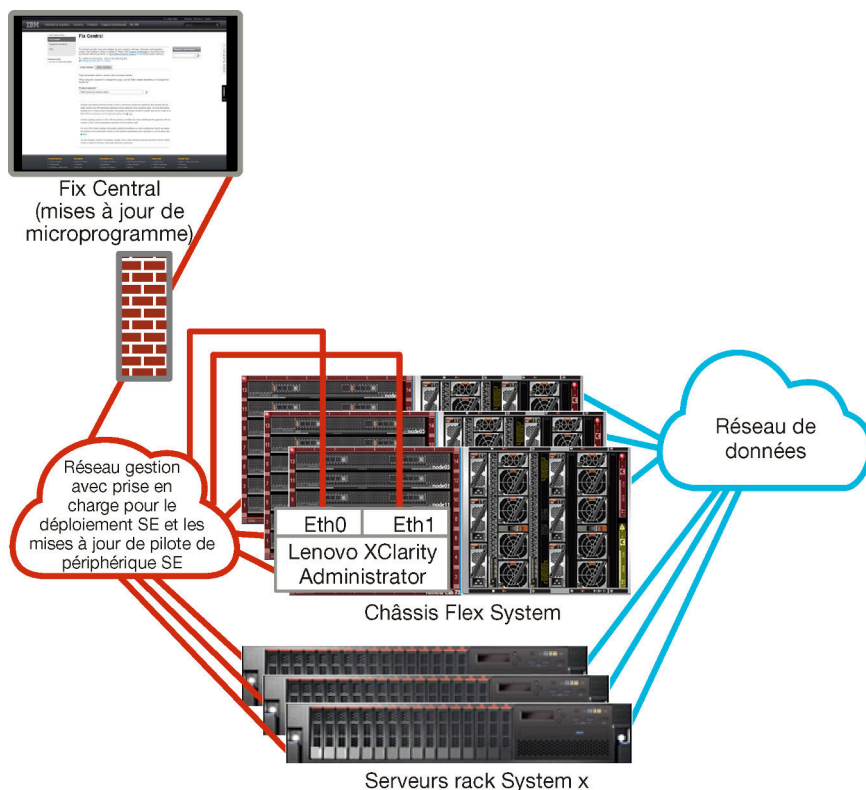


Figure 5. Exemple d'implémentation de réseaux de gestion et de données virtuellement séparés avec le réseau du système d'exploitation faisant partie du réseau de gestion

## Réseau de gestion uniquement

Dans cette topologie, Lenovo XClarity Administrator ne peut accéder qu'au réseau de gestion. Il n'a pas accès au réseau de données. Toutefois, XClarity Administrator doit avoir accès au réseau de déploiement du système d'exploitation si vous prévoyez de déployer des images du système d'exploitation à partir de XClarity Administrator sur les serveurs gérés.

Lorsque vous installez XClarity Administrator et définissez les paramètres réseau, l'interface réseau eth0 doit être configurée pour :

- 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'acquies 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.

Vous pouvez également configurer une seconde interface réseau pour la connexion au même réseau à partir de XClarity Administrator afin de prendre en charge la redondance.

La [Figure 6 « Exemple d'implémentation d'un réseau de gestion uniquement dans lequel le déploiement du système d'exploitation n'est pas pris en charge » à la page 30](#) illustre un exemple d'implémentation d'un réseau de gestion uniquement dans lequel le déploiement du système d'exploitation à partir de XClarity Administrator n'est pas pris en charge.

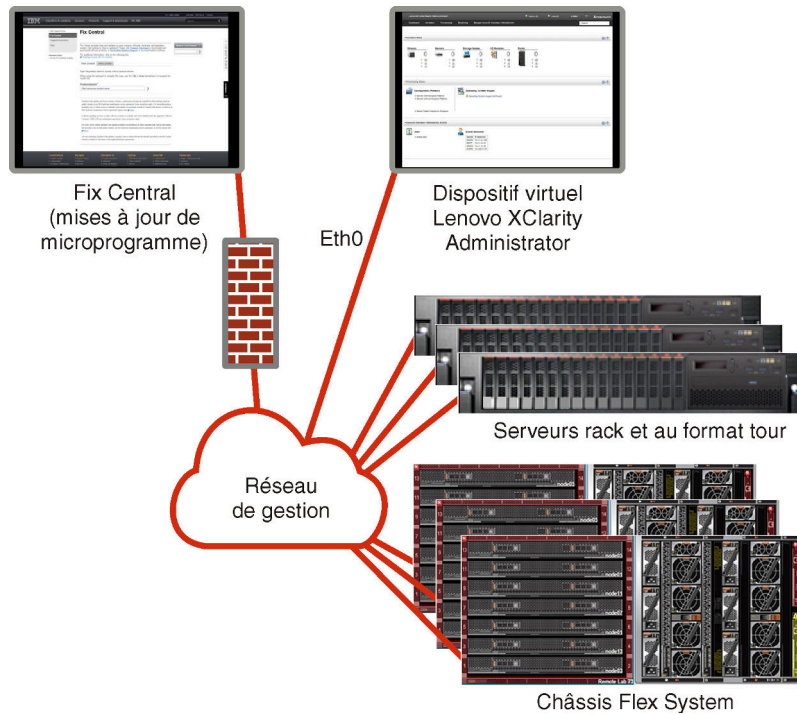


Figure 6. Exemple d'implémentation d'un réseau de gestion uniquement dans lequel le déploiement du système d'exploitation n'est pas pris en charge

La [Figure 6 « Exemple d'implémentation d'un réseau de gestion uniquement dans lequel le déploiement du système d'exploitation n'est pas pris en charge » à la page 30](#) illustre un exemple d'implémentation d'un réseau de gestion uniquement dans lequel le déploiement du système d'exploitation à partir de XClarity Administrator est pris en charge.



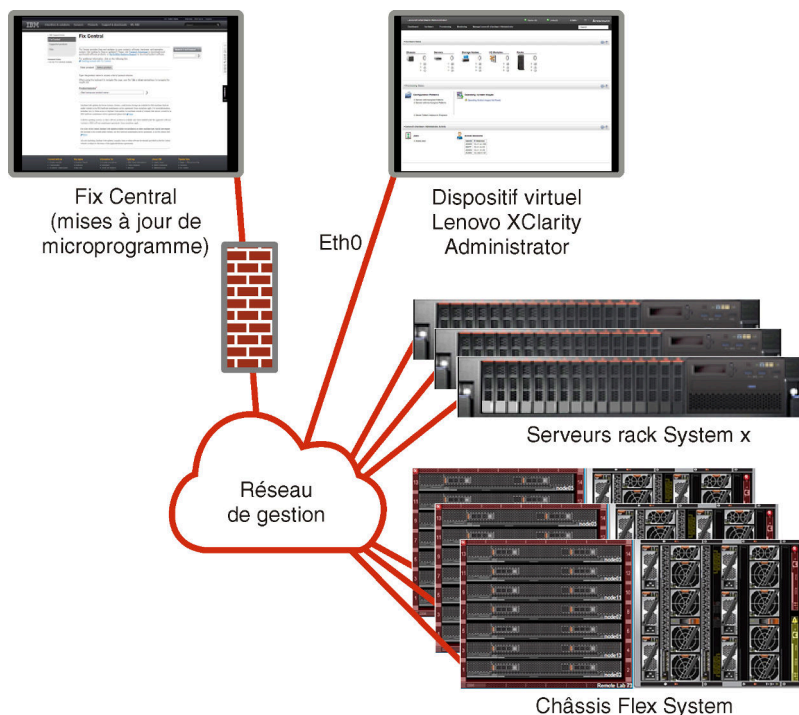


Figure 7. Exemple d'implémentation d'un réseau de gestion uniquement dans lequel le déploiement du système d'exploitation est pris en charge

## Remarques liées à la sécurité

Planifiez la sécurité de Lenovo XClarity Administrator et de tous les appareils gérés.

## Gestion de l'encapsulation

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 *encapsulation*. Vous pouvez également activer ou désactiver l'encapsulation sur les châssis et les serveurs qui sont déjà gérés par Lenovo XClarity Administrator.

Lorsque l'encapsulation est activé sur un appareil qui le prend en charge, Lenovo XClarity Administrator remplace la valeur du mode d'encapsulation 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'encapsulation désactivé, le mode d'encapsulation prend la valeur « Normal ». Si l'encapsulation était précédemment activé sur les appareils, les règles de pare-feu d'encapsulation sont retirées.

**Attention** : Si l'encapsulation 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'encapsulation afin d'établir la communication avec le dispositif. Pour les procédures de récupération, voir [Reprise de la gestion de châssis avec un module CMM après une défaillance du serveur de gestion](#) et [Récupération de la gestion du serveur au format tour après une défaillance du serveur de gestion](#) dans la documentation en ligne de XClarity Administrator.

### Remarques :

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

- 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.

Pour plus d'informations sur l'encapsulation, voir [Activation de l'encapsulation](#) dans la documentation en ligne de XClarity Administrator.

## Gestion cryptographique

La gestion cryptographique se compose des modes et protocoles de communication qui contrôlent la façon dont la communication sécurisée est gérée entre Lenovo XClarity Administrator et les appareils gérés (tels que des châssis, des serveurs et des commutateurs Flex).

### Algorithmes de cryptographie

XClarity Administrator prend en charge le protocole TLS 1.2 et des algorithmes cryptographiques plus puissants pour les connexions réseau sécurisées.

Pour une sécurité maximale, seuls les chiffrements puissants sont désormais pris en charge. Les systèmes d'exploitation client et les navigateurs Web doivent prendre en charge l'un des algorithmes de cryptographie suivants.

- SSH-ED25519
- SSH-ED25519-CERT-V01@OPENSSH.COM
- ECDSA-SHA2-NISTP256
- ECDSA-SHA2-NISTP256-CERT-V01@OPENSSH.COM
- ECDSA-SHA2-NISTP384
- ECDSA-SHA2-NISTP384-CERT-V01@OPENSSH.COM
- ECDSA-SHA2-NISTP521
- ECDSA-SHA2-NISTP521-CERT-V01@OPENSSH.COM
- RSA-SHA2-512
- RSA-SHA2-256
- RSA-SHA2-384

### Modes cryptographiques pour le serveur de gestion

Ce paramètre détermine le mode à utiliser pour les communications sécurisées à partir du serveur de gestion.

- **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 inclut 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](#) dans la documentation en ligne de XClarity Administrator). 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 NIST 800-131A](#) dans la documentation en ligne de XClarity Administrator.

Pour plus d'informations sur le paramétrage des modes de sécurité sur le serveur de gestion, voir [Définition du mode de chiffrement et des protocoles de communication](#) dans la documentation en ligne de XClarity Administrator.

## Modes de sécurité pour les serveurs gérés

Ce paramètre détermine le mode à utiliser pour les communications sécurisées à partir des serveurs gérés.

- **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 algorithmes de chiffrement symétriques 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 serveur 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 bibliothèque 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.

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 régénère 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

Pour plus d'informations sur le paramétrage des modes de sécurité sur le serveur géré, voir [Configuration des paramètres de sécurité pour un serveur](#) dans la documentation en ligne de XClarity Administrator.

## 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.

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 régénérant 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.

Pour plus d'informations sur les certificats, voir [Utilisation de certificats de sécurité](#) dans la documentation en ligne de XClarity Administrator.

## Authentification

### 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.

Pour plus d'informations sur les serveurs d'authentification, voir [Gestion du serveur d'authentification](#) dans la documentation en ligne de XClarity Administrator .

## 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 [Gestion des serveurs](#) dans la documentation en ligne de XClarity Administrator).

**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 utilisateur 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 de châssis avec un module CMM après une défaillance du serveur de gestion](#) et [Récupération de la gestion du serveur au format tour après une défaillance du serveur de gestion](#) dans la documentation en ligne de XClarity Administrator.

## Comptes utilisateur et groupes de rôles

Les *comptes utilisateur* sont utilisés pour se connecter à Lenovo XClarity Administrator et à tous les châssis et serveurs gérés, ainsi que pour en effectuer la gestion. Les comptes utilisateur XClarity Administrator sont soumis à deux processus interdépendants : l'authentification et l'autorisation.

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.

Pour plus d'informations sur les comptes utilisateur et les groupes de rôles, voir [Gestion des comptes utilisateur](#) dans la documentation en ligne de XClarity Administrator.

## Sécurité de compte utilisateur

Les paramètres de 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 de sécurité de compte.

Pour plus d'informations sur les paramètres de sécurité de compte, voir [Modification des paramètres de sécurité d'un compte utilisateur](#) dans la documentation en ligne de Lenovo XClarity Administrator.

---

## Remarques sur la haute disponibilité

Pour configurer la haute disponibilité pour Lenovo XClarity Administrator, utilisez les fonctions de haute disponibilité faisant partie du système d'exploitation hôte ou d'un environnement de conteneurs.

### Docker

Vous pouvez utiliser le centre de données Docker afin de définir un environnement haute disponibilité pour l'exécution des conteneurs XClarity Administrator dans le moteur Docker. Pour plus d'informations sur la haute disponibilité du centre de données Docker, voir [Page Web Architecture et applications haute disponibilité avec le centre de données Docker](#).



## Citrix

Utilisez la fonctionnalité de haute disponibilité fournie pour l'environnement Citrix. Pour plus d'informations, voir [Implémentation de la haute disponibilité \(Citrix\)](#) dans la documentation en ligne de XClarity Administrator.

## KVM (CentOS, RedHat et Ubuntu)

Vous pouvez utiliser OpenStack, ou si vous possédez déjà un environnement haute disponibilité, vous pouvez continuer d'utiliser vos processus internes. Pour plus d'informations sur la haute disponibilité OpenStack, voir [Implémentation de la haute disponibilité \(KVM\)](#) dans la documentation en ligne de XClarity Administrator.

## Microsoft Hyper-V

Utilisez la fonctionnalité de haute disponibilité fournie pour l'environnement ESXi. Pour plus d'informations, voir [Mise en œuvre de la haute disponibilité \(Microsoft Hyper-V\)](#) dans la documentation en ligne XClarity Administrator.

## Nutanix AHV

utilisez la fonction Virtual Machine High Availability fournie pour l'environnement Nutanix AHV. Pour plus d'informations, voir [Implémentation de la haute disponibilité \(Nutanix\)](#) dans la documentation en ligne de XClarity Administrator.

## VMware ESXi

Dans un environnement VMware High Availability, plusieurs hôtes sont configurés en tant que cluster. Le stockage partagé est utilisé pour rendre l'image disque d'une machine virtuelle disponible sur les hôtes du cluster. La machine virtuelle s'exécute sur un seul hôte à la fois. En cas de problème avec la machine virtuelle, une autre instance de cette machine virtuelle est démarrée sur un hôte de sauvegarde.

VMware High Availability requiert les composants suivants :

- Au moins deux hôtes sur lesquels ESXi est installé. Ces hôtes deviennent membres du cluster VMware.
- Un troisième hôte sur lequel VMware vCenter est installé.

**Astuce :** Prenez soin d'installer une version de VMware vCenter qui est compatible avec les versions de ESXi installées sur les hôtes à utiliser dans le cluster.

VMware vCenter peut être installé sur l'un des hôtes utilisés dans le cluster. Toutefois, si cet hôte est hors tension ou inutilisable, vous perdez également l'accès à l'interface VMware vCenter .

- Un stockage partagé (magasins de données) accessible par tous les hôtes membres du cluster. Vous pouvez utiliser n'importe quel type de stockage partagé pris en charge par VMware. Le magasin de données est utilisé par VMware pour déterminer si une machine virtuelle doit basculer vers un autre hôte (pulsations).

Pour plus de détails sur la configuration d'un cluster VMware High Availability, voir [Implémentation de la haute disponibilité \(VMware ESXi\)](#) dans la documentation en ligne de XClarity Administrator..

---

## Features on Demand (FoD)

Features on Demand (FoD) active des fonctions sans qu'il soit nécessaire d'installer du matériel ou d'acquérir de nouveaux équipements. Cette activation est effectuée en achetant et en installant la clé Features on Demand (FoD) correspondante.

Pour utiliser les opérations de déploiement de système d'exploitation et de contrôle à distance dans Lenovo XClarity Administrator, vous devez activer XClarity Controller Enterprise level ou MM Advanced Upgrade pour les serveurs qui ne sont pas livrés avec ces fonctions déjà activées par défaut. Ces opérations nécessitent également l'installation d'une clé Features on Demand (FoD) de présence à distance sur les

serveurs ThinkSystem, Converged 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](#) dans la documentation en ligne de XClarity Administrator).

Certaines fonctions de serveur avancées sont activées à l'aide de clés Features on Demand (FoD). Si les fonctions comportent des paramètres configurables qui sont exposés lors d'une configuration UEFI, vous pouvez configurer ces paramètres à l'aide de Modèles de configuration ; toutefois, la configuration obtenue ne sera pas activée tant que la clé Features on Demand (FoD) correspondante n'aura pas été installée.

**Remarque :** Vous ne pouvez pas installer ou gérer des clés Features on Demand (FoD) à partir de XClarity Administrator ; toutefois, vous pouvez afficher la liste des clés Features on Demand (FoD) actuellement installées sur des serveurs gérés. Pour plus d'informations sur l'affichage des clés Features on Demand (FoD) installées, voir [Affichage des clés Feature on Demand](#) dans la documentation en ligne de XClarity Administrator.

Pour acquérir et installer des clés Features on Demand (FoD) :

1. Achetez la mise à niveau de Features on Demand (FoD) à l'aide du numéro de référence approprié.

Vous pouvez acheter des clés à partir de la [Portail Web Features on Demand](#). Lorsque vous avez terminé votre achat, un code d'autorisation vous est envoyé par e-mail.

2. Sur la [Portail Web Features on Demand](#), entrez le code d'autorisation que vous avez reçu, ainsi que l'identificateur système unique du serveur que vous prévoyez de mettre à niveau.
3. Téléchargez la clé d'activation dans un fichier .KEY.
4. Téléchargez la clé d'activation sur le contrôleur de gestion du serveur.
5. Redémarrez le serveur. Une fois le serveur redémarré, la fonction est activée.

Pour plus d'informations sur les clés Features on Demand (FoD), voir [Utilisation des fonctions Lenovo à la demande](#).

---

## Chapitre 3. Installation de Lenovo XClarity Administrator

Il existe plusieurs méthodes pour connecter les appareils gérables au réseau et pour configurer le dispositif virtuel Lenovo XClarity Administrator pour gérer ces appareils. Suivez les informations de cette section comme guide pour configurer les appareils gérables et installer le XClarity Administrator

Cette section explique comment configurer plusieurs topologies communes. Cette section ne couvre pas toutes les topologies de réseau possibles.

**Attention** : Pour la gestion des appareils, XClarity Administrator doit avoir accès au réseau de gestion.

### En savoir plus :

-  [Installation de Lenovo XClarity Administrator sur VMware vCenter](#)
-  [Installation de Lenovo XClarity Administrator sur VMware vSphere](#)
-  [Installation de Lenovo XClarity Administrator sur Windows Hyper-V](#)
-  [Installation de Lenovo XClarity Administrator sur Red Hat KVM](#)

---

## Donnée unique et réseau de gestion

Dans cette topologie de réseau, le réseau de données et le réseau de gestion sont le même réseau.

### Avant de commencer

Vérifiez que tous les ports appropriés sont activés, y compris les ports requis par XClarity Administrator (voir [Disponibilité de port](#)).

Vérifiez que le microprogramme minimal requis est installé sur chaque appareil 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** : Configurez les appareils et les composants de manière à réduire au minimum les modifications d'adresse IP. Envisagez d'utiliser des adresses IP statiques au lieu du protocole DHCP (Dynamic Host Configuration Protocol). Si le protocole DHCP est utilisé, faites en sorte que les modifications d'adresse IP soient réduits au minimum.

### À propos de cette tâche

Pour les dispositifs virtuels, toutes les communications entre XClarity Administrator et le réseau se produisent via l'interface réseau eth0 sur l'hôte. Pour les conteneurs, vous pouvez utiliser un nom personnalisé. Ce scénario utilise toutefois eth0.

**Important** : L'implémentation d'un réseau de données et de gestion partagé peut entraîner des interruptions du trafic avec, par exemple, des paquets ignorés ou des problèmes liés à la connectivité du réseau de gestion, en fonction de votre configuration réseau (par exemple, si le trafic en provenance de serveurs a une priorité haute et qu'un trafic en provenance des contrôleurs de gestion a une priorité faible). Le réseau de gestion utilise le trafic UDP en plus du trafic TCP. Le trafic UDP peut avoir une priorité plus faible lorsque le trafic réseau est élevé.

La figure suivante montre un moyen de configurer votre environnement si les réseaux de données et de gestion sont identiques. Les nombres indiqués dans la figure correspondent aux étapes numérotées dans les sections suivantes.

**Remarque :** Cette figure ne représente pas toutes les options de câblage qui peuvent être requises pour votre environnement. Au lieu de cela, cette figure affiche uniquement les exigences d'option de câblage pour les serveurs rack, les commutateurs rack, les commutateurs Flex et les CMM car ils concernent la configuration d'un réseau de donnée unique/de gestion.

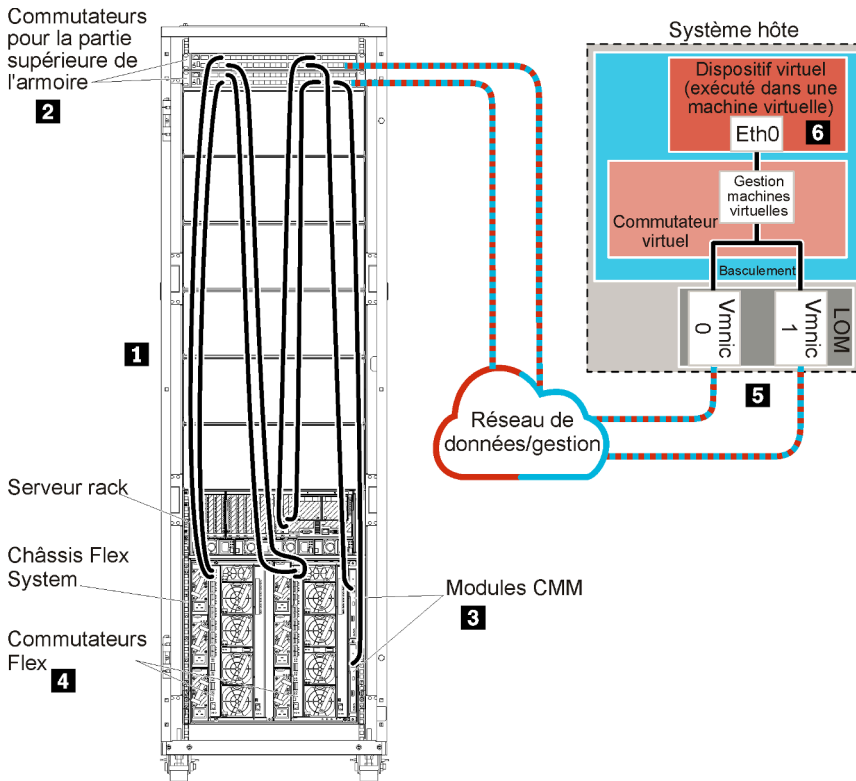


Figure 8. Exemple de donnée unique et de topologie de réseau de gestion pour un dispositif virtuel

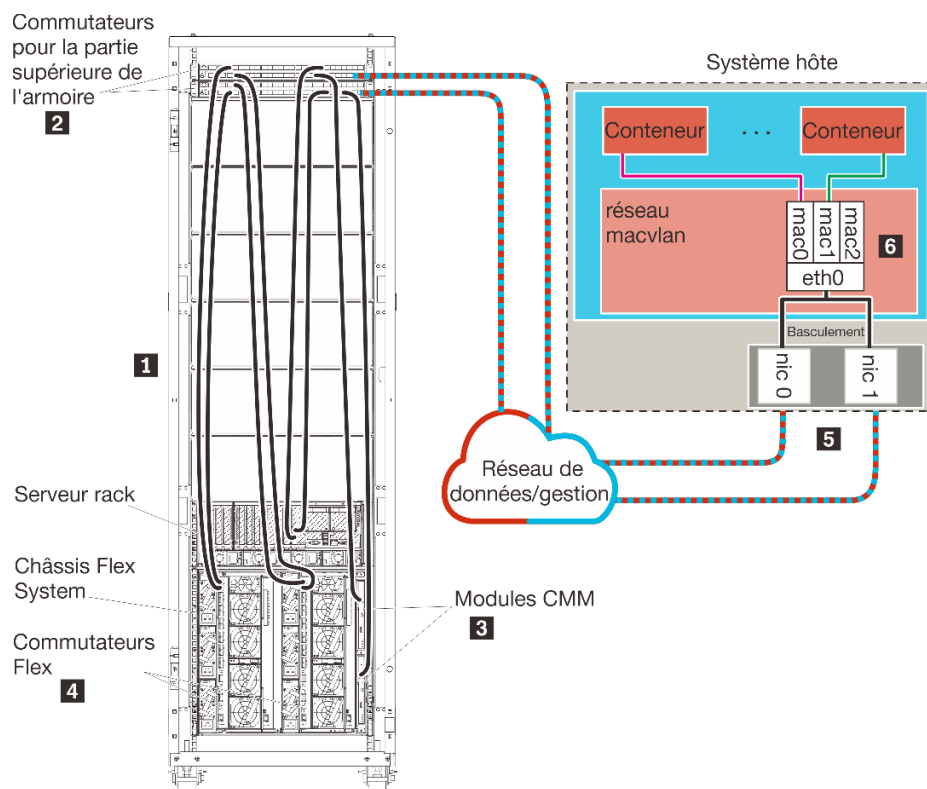


Figure 9. Exemple de topologie du réseau de donnée unique et de gestion pour les conteneurs

**Important :** Vous pouvez configurer XClarity Administrator sur tout système qui satisfait aux exigences de XClarity Administrator, dont un serveur géré. Si vous utilisez un serveur géré pour l'hôte XClarity Administrator :

- Vous devez mettre en œuvre une topologie du réseau de gestion et de données séparées virtuellement ou une topologie du réseau de gestion et de donnée unique.
- Vous ne pouvez pas utiliser XClarity Administrator pour appliquer des mises à jour de microprogramme à ce serveur géré. Même dans ce cas, seule une partie du microprogramme est appliquée à l'activation immédiate et XClarity Administrator force le serveur cible à redémarrer, ce qui redémarrerait XClarity Administrator également. Une fois le microprogramme appliqué à l'activation reportée, seule une partie est appliquée lorsque l'hôte XClarity Administrator est redémarré.
- Si vous utilisez un serveur dans un châssis Flex System, vérifiez que le serveur est défini pour se mettre sous tension automatiquement. Vous pouvez définir cette option à partir de l'interface Web CMM en cliquant sur **Gestion de châssis** → **Nœuds de traitement**, puis en sélectionnant le serveur, et en sélectionnant **Alimentation automatique** pour **Mode de mise sous tension automatique**.

Si vous prévoyez d'installer XClarity Administrator pour gérer des châssis et serveurs rack existants qui ont déjà été configurés, passez à [Étape 5 : installation et configuration de l'hôte](#).

Pour plus d'informations sur la planification pour cette topologie, notamment des informations sur les paramètres réseau et la configuration Eth1 et Eth0, voir [Réseau de données et de gestion unique](#).

## Étape 1 : Câblez le châssis, les serveurs rack et l'hôte Lenovo XClarity Administrator sur les commutateurs de la partie supérieure de l'armoire

Câblez le châssis, les serveurs rack et l'hôte XClarity Administrator aux commutateurs de la partie supérieure de l'armoire pour activer les communications entre les dispositifs et votre réseau.

## Procédure

Câblez chaque commutateur Flex et module CMM dans chaque châssis, chaque serveur rack, et l'hôte XClarity Administrator aux commutateurs de la partie supérieure de l'armoire. Vous pouvez choisir n'importe quel port dans les commutateurs de la partie supérieure de l'armoire.

La figure suivante est un exemple qui montre le câblage du châssis (Commutateurs Flex et modules CMM), des serveurs rack et de l'hôte XClarity Administrator aux commutateurs de la partie supérieure de l'armoire.

**Remarque :** Cette figure ne représente pas toutes les options de câblage qui peuvent être requises pour votre environnement. Au lieu de cela, cette figure affiche uniquement les exigences d'option de câblage pour les serveurs rack, les commutateurs rack, les commutateurs Flex et les CMM car ils concernent la configuration d'un réseau de donnée unique/de gestion.

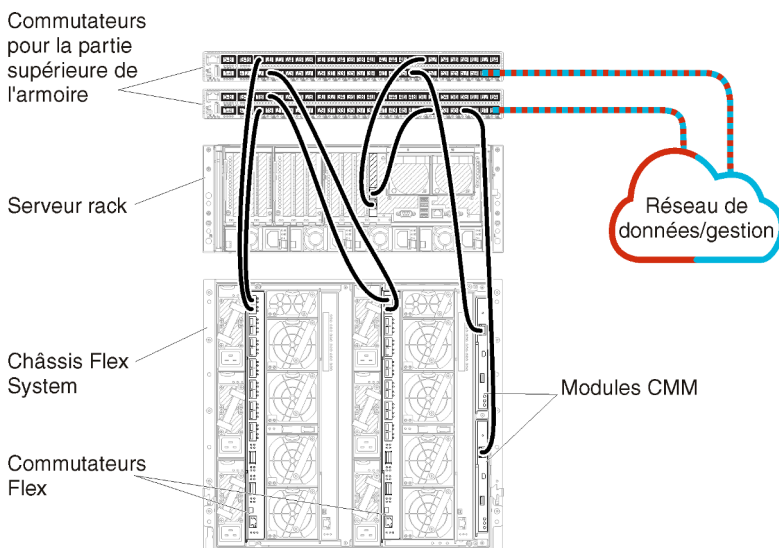


Figure 10. Exemple de câblage pour un réseau de donnée unique et de gestion

## Étape 2 : Configurer les commutateurs de la partie supérieure de l'armoire

Configurez les commutateurs de la partie supérieure de l'armoire.

### Avant de commencer

Outre les exigences de configuration type des commutateurs de la partie supérieure de l'armoire, vérifiez que tous les ports appropriés sont activés, y compris les ports externes sur les Commutateurs Flex, les serveurs rack, le réseau et les ports internes sur le module CMM, les serveurs rack et le réseau.

## Procédure

Les étapes de configuration peuvent varier, selon le type de commutateurs de type armoire qui sont installés.

Pour savoir comment configurer les commutateurs de la partie supérieure de l'armoire Lenovo, voir [Commutateurs d'armoire dans la documentation en ligne System x](#). Si un autre commutateur de la partie supérieure de l'armoire est installé, consultez la documentation fournie avec ce commutateur.

## Étape 3 : Configurer les Chassis Management Modules (modules CMM)

Configurez le module Chassis Management Module (CMM) principal dans votre châssis pour gérer tous les dispositifs du châssis.

### À propos de cette tâche

Pour obtenir des informations détaillées sur la configuration d'un module CMM, voir [Configuration des composants du châssis dans la documentation en ligne Flex System](#).

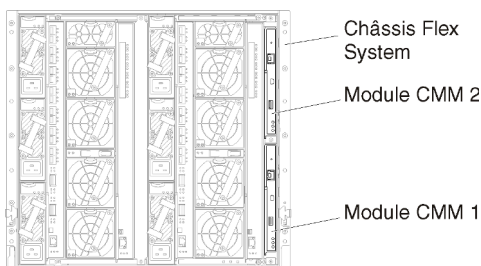
En outre, reportez-vous aux étapes 4.1 à 4.5 sur l'affiche d'instructions fournie avec votre châssis.

### Procédure

Pour configurer le module CMM, procédez comme suit.

Si deux modules CMM sont installés, configurez uniquement le module CMM *principale*, qui synchronise automatiquement la configuration avec le module CMM de secours.

Étape 1. Connectez un câble Ethernet du module CMM de la baie 1 à un poste de travail client pour créer une connexion directe.



Lors de la première connexion au module CMM, vous devrez peut-être modifier les propriétés du protocole Internet sur le poste de travail client.

**Important :** Vérifiez que le sous-réseau du poste de travail client est identique au sous-réseau CMM. (Le sous-réseau CMM par défaut est 255.255.255.0). L'adresse IP choisie pour le poste de travail client doit se trouver sur le même réseau que le module CMM (par exemple, 192.168.70.0 - 192.168.70.24).

Étape 2. Pour lancer l'interface de gestion du module CMM, ouvrez un navigateur Web sur le poste de travail client, et dirigez-le sur l'adresse IP du module CMM.

#### Remarques :

- Veillez à utiliser une connexion sécurisée et à ajouter **https** dans l'URL (par exemple, <https://192.168.70.100>). Si vous n'ajoutez pas https, vous recevez une erreur de page introuvable.
- Si vous utilisez l'adresse IP par défaut, 192.168.70.100, l'interface de gestion du module CMM peut être disponible après quelques minutes. Ce délai est lié au fait que le module CMM tente d'obtenir une adresse DHCP pendant deux minutes avant de retomber à l'adresse statique par défaut.

Étape 3. Connectez-vous à l'interface de gestion du module CMM à l'aide de l'ID utilisateur `USERID` et du mot de passe `PASSWORD` par défaut. Après votre connexion, vous devez changer le mot de passe par défaut.

Étape 4. Exécutez l'assistant de configuration initiale du module CMM pour indiquer les détails de votre environnement. L'assistant de configuration initiale comporte les options suivantes :

- Affichez l'inventaire et la santé des châssis.

- Importez la configuration à partir d'un fichier de configuration existant.
- Configurez les paramètres du module CMM général.
- Configurez la date et l'heure du module CMM.

**Conseil :** Lorsque vous installez XClarity Administrator, vous configurez XClarity Administrator et tous les châssis gérés par XClarity Administrator pour utiliser un serveur NTP.

- Configurez les informations IP du module CMM.
- Configurez la stratégie de sécurité du module CMM.
- Configurez le Domain Name System (DNS).
- Configurez les réexpéditeurs d'événement.

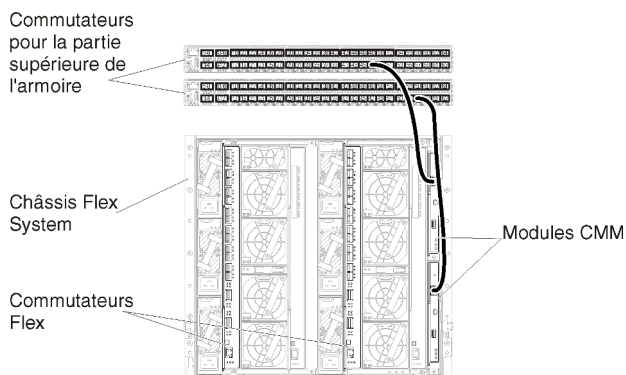
Etape 5. Après avoir sauvegardé les paramètres de l'assistant de configuration et appliqué les modifications, configurez les adresses IP de tous les composants du châssis.

Reportez-vous à l'étape 4.6 de l'affiche d'instructions fournie avec votre châssis.

**Remarque :** Vous devez réinitialiser le processeur de gestion du système pour chaque nœud de traitement et redémarrer les commutateurs Flex pour afficher la nouvelle adresse IP.

Etape 6. Redémarrez le module CMM à l'aide de l'interface de gestion CMM.

Etape 7. Lorsque le module CMM redémarre, connectez un câble du port Ethernet sur le module CMM à votre réseau.



Etape 8. Connectez-vous à l'interface de gestion du module CMM à l'aide de la nouvelle adresse IP.

## Après avoir terminé

Vous pouvez également configurer le module CMM pour prendre en charge la redondance. Utilisez le système d'aide du module CMM pour en savoir plus sur les zones disponibles sur chacune des pages suivantes.

- Configurez le basculement pour le module CMM en cas de panne matérielle dans le module CMM principal. Dans l'interface de gestion du module CMM, cliquez sur **Gestion du module de gestion → Propriétés → Basculement avancé**.
- Configurez le basculement suite à un problème de réseau (liaison montante). Dans l'interface de gestion du module CMM, cliquez sur **Gestion du module de gestion → Réseau**, cliquez sur l'onglet **Ethernet**, puis cliquez sur **Ethernet avancé**. Au minimum, assurez-vous de sélectionner **Basculement en cas de perte de liaison réseau physique**.

## Étape 4 : Configurer Commutateurs Flex

Configurez Commutateurs Flex (modules d'E-S) dans chaque châssis.



## Avant de commencer

Vérifiez que tous les ports appropriés sont activés, y compris les ports externes du commutateur Flex au commutateur de la partie supérieure de l'armoire et les ports internes au module CMM.

Si les commutateurs Flex sont configurés de façon à obtenir des paramètres réseau dynamique (adresse IP, masque de réseau, passerelle et adresse DNS) sur DHCP, vérifiez que les commutateurs Flex possèdent des paramètres identiques (par exemple, vérifiez que les adresses IP sont dans le même sous-réseau que le module CMM).

**Important :** Pour chaque châssis Flex System, vérifiez que le type de matrice de la carte d'extension dans chaque serveur du châssis est compatible avec le type de matrice de tous les commutateurs Flex installés dans le même châssis. Par exemple, si des commutateurs Ethernet sont installés dans un châssis, tous les serveurs de ce châssis doivent disposer d'une connectivité Ethernet via le connecteur LAN-on-motherboard ou sur une carte d'extension Ethernet. Pour plus d'informations sur la configuration des commutateurs Flex, voir [Configuration des modules d'E-S dans la documentation en ligne Flex Systems](#).

## Procédure

Les étapes de configuration peuvent varier, selon le type de Commutateurs Flex qui sont installés. Pour plus d'informations sur chacun des Commutateurs Flex pris en charge, voir [Commutateurs réseau Flex System dans la documentation en ligne Flex Systems](#).

En général, vous devez configurer les commutateurs Flex dans les baies de commutateurs Flex 1 et 2.

**Astuce :** La baie de commutateur Flex 2 est la troisième baie de module lorsque l'on regarde à l'arrière du châssis.

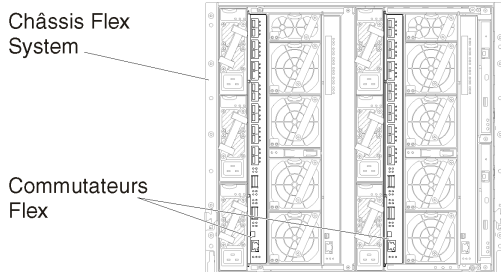


Figure 11. Emplacements Commutateur Flex dans un châssis

## Étape 5 : installation et configuration de l'hôte

Vous pouvez installer Docker sur tout serveur qui satisfait aux exigences de Lenovo XClarity Administrator.

### Avant de commencer

Vous pouvez utiliser le centre de données Docker afin de définir un environnement haute disponibilité pour l'exécution des conteneurs XClarity Administrator dans le moteur Docker. Pour plus d'informations sur la haute disponibilité du centre de données Docker, voir [Page Web Architecture et applications haute disponibilité avec le centre de données Docker](#).

Vérifiez que l'hôte respecte les prérequis définis dans [Configurations matérielles et logicielles requises](#).

Vérifiez que le système hôte est dans le même réseau que les dispositifs à gérer.

**Important** : Vous pouvez configurer XClarity Administrator sur tout système qui satisfait aux exigences de XClarity Administrator, dont un serveur géré. Si vous utilisez un serveur géré pour l'hôte XClarity Administrator :

- Vous devez mettre en œuvre une topologie du réseau de gestion et de données séparées virtuellement ou une topologie du réseau de gestion et de donnée unique.
- Vous ne pouvez pas utiliser XClarity Administrator pour appliquer des mises à jour de microprogramme à ce serveur géré. Même dans ce cas, seule une partie du microprogramme est appliquée à l'activation immédiate et XClarity Administrator force le serveur cible à redémarrer, ce qui redémarrerait XClarity Administrator également. Une fois le microprogramme appliqué à l'activation reportée, seule une partie est appliquée lorsque l'hôte XClarity Administrator est redémarré.
- Si vous utilisez un serveur dans un châssis Flex System, vérifiez que le serveur est défini pour se mettre sous tension automatiquement. Vous pouvez définir cette option à partir de l'interface Web CMM en cliquant sur **Gestion de châssis** → **Nœuds de traitement**, puis en sélectionnant le serveur, et en sélectionnant **Alimentation automatique** pour **Mode de mise sous tension automatique**.

## Procédure

Installez et configurez Docker sur l'hôte à l'aide des instructions fournies avec votre distribution Docker.

## Étape 6. Installation et configuration d'un XClarity Administrator

Installez et configurez le conteneur Lenovo XClarity Administrator sur l'hôte Docker que vous venez d'installer.

### Avant de commencer

Vérifiez que le système hôte respecte les exigences logicielles et matérielles minimales (voir [Configurations matérielles et logicielles requises](#)).

Vérifiez que tous les ports appropriés sont activés, y compris les ports requis par XClarity Administrator (voir [Disponibilité de port](#)).

Vérifiez que le système hôte est dans le même réseau que les dispositifs à gérer.

Assurez-vous que le système d'exploitation hôte et XClarity Administrator utilisent le même serveur NTP.

XClarity Administrator permet un nom personnalisé pour le réseau à utiliser pour la gestion des données et du matériel, ainsi que le déploiement SE (voir [Configurations réseau](#)). Les exemples de la procédure ci-après utilisent eth0.

Assurez-vous qu'un réseau macvlan est chargé dans le noyau sur le système hôte. Utilisez la commande **lsmod | grep macvlan** pour vérifier s'il est bien chargé. Exécutez la commande **modprobe macvlan** afin de charger macvlan dans le noyau.

Assurez-vous de bien utiliser un nom unique et une adresse IP pour chaque conteneur lors de l'exécution de plusieurs conteneurs XClarity Administrator dans le même hôte.

Si vous avez l'intention de gérer des appareils ThinkServer et d'autres appareils existants, assurez-vous que Docker est activé pour prendre en charge le protocole IPv6.

1. Éditez le fichier `/etc/docker/daemon.json`, définissez la clé **ipv6** sur True et définissez la clé **fixed-cidr-v6** sur votre sous-réseau IPv6. Voici un exemple de fichier daemon.

```
{
  "ipv6": true,
  "fixed-cidr-v6": "2001:db8:1::/64",
```

```
"experimental": true,  
"ip6tables": true  
}
```

2. Rechargez la configuration Docker en exécutant la commande suivante.  
`systemctl reload docker`

**Remarque** : XClarity Administrator n'est pas exécuté en tant que conteneur avec privilèges.

## Procédure

Pour installer un conteneur XClarity Administrator à l'aide de Docker compose, procédez comme suit.

Etape 1. Téléchargez l'image de dispositif virtuel, le fichier d'environnement et le fichier YAML XClarity Administrator depuis [Page Web de téléchargements XClarity Administrator](#) sur un poste de travail client. Connectez-vous au site Web, puis utilisez la clé d'accès qui vous a été fournie pour télécharger l'image.

Etape 2. Importez l'image de conteneur XClarity Administrator dans votre hôte Docker en exécutant la commande suivante.

```
docker load -i lnvgv_sw_lxca_<ver>_anyos_noarch.tar.gz
```

Etape 3. Éditez le fichier `docker_compose.env`, puis mettez à jour les variables d'environnement suivantes.

- **CONTAINER\_NAME**. Nom de conteneur unique, utilisé pour créer des volumes Docker pour chaque instance XClarity Administrator (par exemple, `CONTAINER_NAME=LXCA-203`)
- **ADDRESS**. Adresse IPv4 statique du conteneur (par exemple, `ADDRESS=192.0.2.0`)
- **BACKUP\_MOUNT**. (Facultatif) Chemin pour le partage distant qui peut être utilisé pour stocker les sauvegardes XClarity Administrator. Cela doit être `/mnt/backup_share`.
- **FIRMWARE\_MOUNT**. (Facultatif) Chemin pour le partage distant pouvant être utilisé en tant que référentiel distant pour les mises à jour de microprogramme. Cela doit être `/mnt/fw_share`.

Voici un exemple de fichier d'environnement.

```
CONTAINER_NAME="LXCA-203"  
ADDRESS="192.0.2.0"  
BACKUP_MOUNT="/mnt/backup_share"  
FIRMWARE_MOUNT="/mnt/fw_share"
```

Etape 4. Éditez `docker_compose.yml` et mettez à jour les propriétés suivantes.

- Définissez la propriété de l'**image** sur le nom du fichier d'image d'installation utilisé lors de l'étape 2.

**Remarque** : Vous pouvez modifier le nom du fichier d'image (par exemple, « le plus récent ») à l'aide de la commande `docker tag`.

- Si vous souhaitez utiliser des partages distants en tant que référentiel de microprogramme distant et stocker des sauvegardes XClarity Administrator, définissez le point de montage hôte pour chaque partage distant dans la propriété **volumes**.
- Définissez la propriété **dns** sur l'adresse IP des serveurs DNS.
- Le conteneur fait partie du groupe de ressources du processeur et de la mémoire qui sont disponibles pour l'hôte. En option, vous pouvez définir des limites relatives à l'utilisation des ressources en définissant les propriétés **cpus** et **mémoire**.
- Définissez la propriété **parent** sur le nom de l'interface réseau du système hôte à utiliser en tant qu'interface parent pour l'interface macvlan du conteneur. Cette interface doit avoir un accès direct au sous-réseau affecté au conteneur.
- Définissez le **sous-réseau** et la **passerelle** en fonction de votre topologie de réseau. En général, le sous-réseau et la passerelle sont pour le réseau de gestion, auquel appartient `${ADDRESS}`.

- Si vous souhaitez prendre en charge le protocole IPv6, définissez la propriété **enable\_ipv6** sur True, définissez la propriété **ipv6\_address** sur l'adresse IPv6 et ajoutez un autre ensemble de propriétés de **sous-réseau** et de **passerelle** en fonction de votre topologie de réseau (généralement pour le réseau de gestion auquel l'adresse IPv6 appartient).

**Remarque** : XClarity Administrator utilise macvlan pour configurer le réseau du conteneur. Pour plus d'informations, voir le document [Utiliser la page Web des réseaux macvlan](#)

Ce qui suit est un exemple de fichier YML, avec IPv6 activé.

```
version: '3.8'

services:
  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.2.10
      - 192.0.2.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

volumes:
  data:
    name: ${CONTAINER_NAME}-data
  postgresql:
    name: ${CONTAINER_NAME}-postgresql
  log:
    name: ${CONTAINER_NAME}-log
  confluent-etc:
    name: ${CONTAINER_NAME}-confluent-etc
  confluent-log:
    name: ${CONTAINER_NAME}-confluent-log
  confluent:
    name: ${CONTAINER_NAME}-confluent
  propconf:
```

```

    name: ${CONTAINER_NAME}-propconf
ssh:
    name: ${CONTAINER_NAME}-ssh
xcat:
    name: ${CONTAINER_NAME}-xcat

networks:
  lan:
    name: lan
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: eth0
    ipam:
      config:
        - subnet: 192.0.0.0/19
          gateway: 192.0.30.1
        - subnet: "2001:8003:7d51:2000::/80"
          gateway: "2001:8003:7d51:2000::1"

```

Etape 5. Déployez la nouvelle dans Docker en exécutant la commande ci-après, `<ENV_FILENAME>` étant le nom du fichier des variables d'environnement créé lors de l'étape 2.

```
COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d
```

## Après avoir terminé

Connectez-vous et configurez XClarity Administrator (voir [Accès à l'interface Web Lenovo XClarity Administrator la première fois](#) et [Configuration des Lenovo XClarity Administrator](#)).

---

## Données séparées physiquement et réseaux de gestion

Dans cette topologie, le réseau de données et le réseau de gestion sont des réseaux séparés physiquement. Les communications de gestion entre Lenovo XClarity Administrator et le réseau se produisent via l'interface réseau Eth0 sur l'hôte. Les communications de données se produisent sur l'interface réseau Eth1.

### Avant de commencer

Vérifiez que tous les ports appropriés sont activés, y compris les ports requis par XClarity Administrator (voir [Disponibilité de port](#)).

Vérifiez que le microprogramme minimal requis est installé sur chaque appareil 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** : Configurez les appareils et les composants de manière à réduire au minimum les modifications d'adresse IP. Envisagez d'utiliser des adresses IP statiques au lieu du protocole DHCP (Dynamic Host Configuration Protocol). Si le protocole DHCP est utilisé, faites en sorte que les modifications d'adresse IP soient réduits au minimum.

### À propos de cette tâche

La figure suivante montre un moyen de configurer votre environnement lorsque les réseaux de gestion et de données sont physiquement différents. Les nombres indiqués dans la figure correspondent aux étapes numérotées dans les sections suivantes.

**Remarque :** Cette figure ne représente pas toutes les options de câblage qui peuvent être requises pour votre environnement. Au lieu de cela, cette figure affiche uniquement les exigences d'option de câblage pour les commutateurs Flex, les modules CMM et les serveurs rack, car ils concernent les réseaux de gestion et de données séparés physiquement.

**Conseil :** Au lieu de configurer deux commutateurs physiques connectés à chaque réseau pour la redondance (soit un total de quatre commutateurs), vous pouvez configurer un commutateur physique unique qui est connecté à chaque réseau (soit un total de deux commutateurs). Dans ce cas, chaque commutateur est connecté aux deux réseaux et vous implémentez deux VLAN : l'un pour le réseau de données et l'autre pour le réseau de gestion, afin d'isoler le trafic de données.

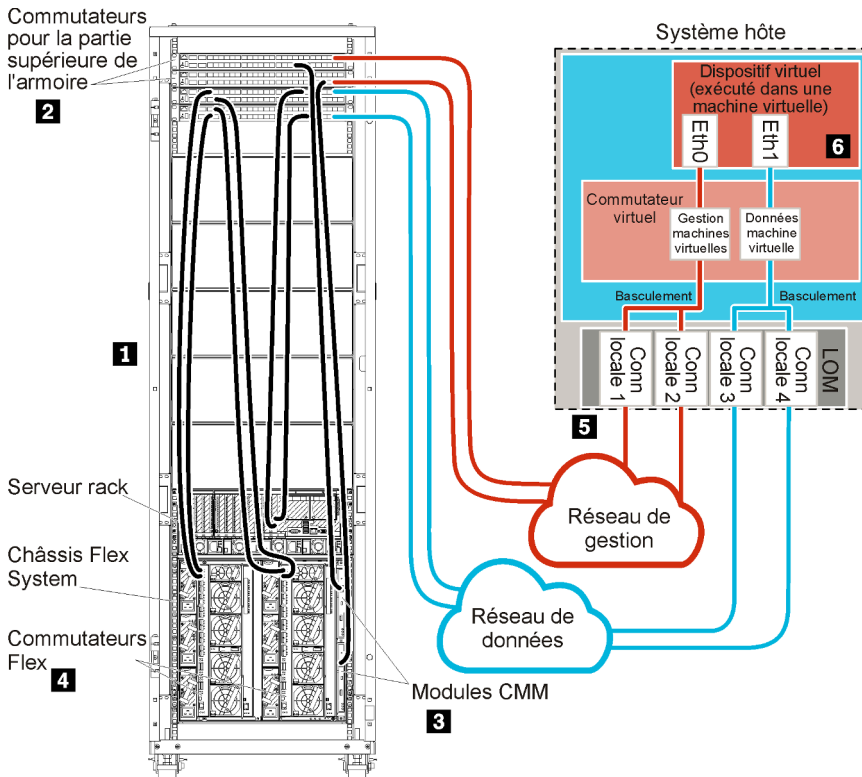


Figure 12. Exemple de données séparées physiquement et de topologie du réseau de gestion pour un dispositif virtuel

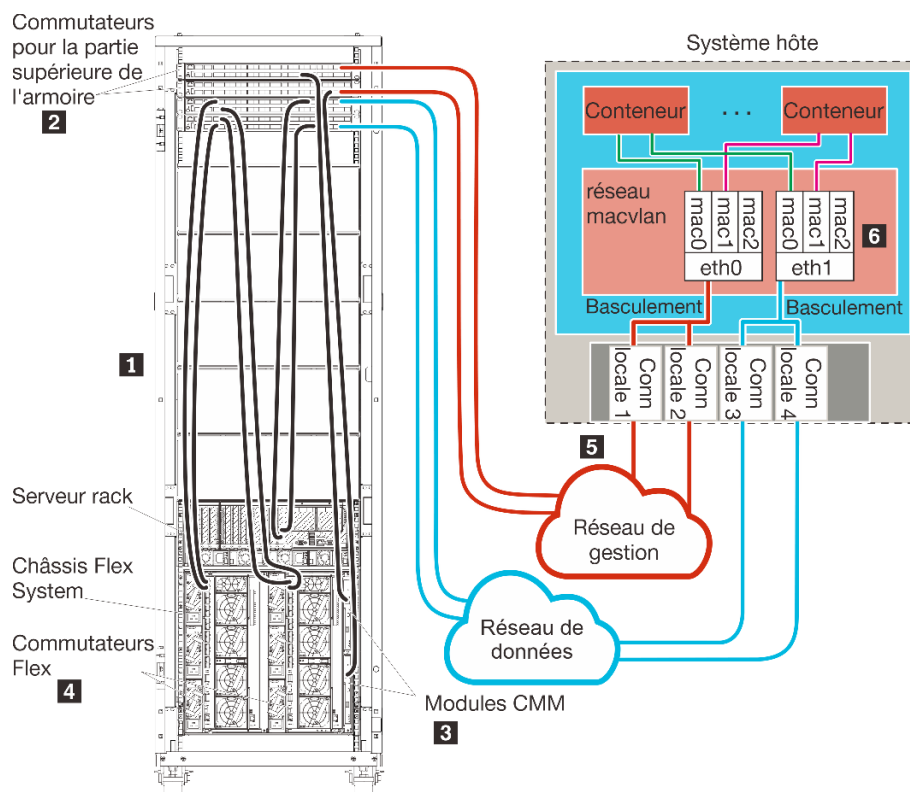


Figure 13. Exemple de données séparées physiquement et de topologie du réseau de gestion pour les conteneurs

Si vous prévoyez d'installer XClarity Administrator pour gérer des châssis et serveurs rack existants qui ont déjà été configurés, passez à [Étape 5 : installation et configuration de l'hôte](#).

Pour plus d'informations sur la planification pour cette topologie, notamment des informations sur les paramètres réseau et la configuration Eth1 et Eth0, voir [Réseau de données et réseau de gestion séparés physiquement](#).

## Étape 1 : Câblez le châssis, les serveurs rack et l'hôte Lenovo XClarity Administrator sur les commutateurs de la partie supérieure de l'armoire

Câblez le châssis, les serveurs rack et l'hôte XClarity Administrator aux commutateurs de la partie supérieure de l'armoire pour activer les communications entre les dispositifs et vos réseaux.

### Procédure

Câblez chaque commutateur Flex et module CMM dans chaque châssis, chaque serveur rack, et l'hôte XClarity Administrator aux commutateurs de la partie supérieure de l'armoire. Vous pouvez choisir n'importe quel port dans les commutateurs de la partie supérieure de l'armoire.

La figure suivante est un exemple qui montre le câblage du châssis (Commutateurs Flex et modules CMM), des serveurs rack et de l'hôte XClarity Administrator aux commutateurs de la partie supérieure de l'armoire.

**Remarque :** Cette figure ne représente pas toutes les options de câblage qui peuvent être requises pour votre environnement. Au lieu de cela, cette figure affiche uniquement les exigences d'option de câblage pour les commutateurs Flex, les modules CMM et les serveurs rack, car ils concernent les réseaux de gestion et de données séparés physiquement.

**Conseil :** Au lieu de configurer deux commutateurs physiques connectés à chaque réseau pour la redondance (soit un total de quatre commutateurs), vous pouvez configurer un commutateur physique unique qui est connecté à chaque réseau (soit un total de deux commutateurs). Dans ce cas, chaque commutateur est connecté aux deux réseaux et vous implémentez deux VLAN : l'un pour le réseau de données et l'autre pour le réseau de gestion, afin d'isoler le trafic de données.

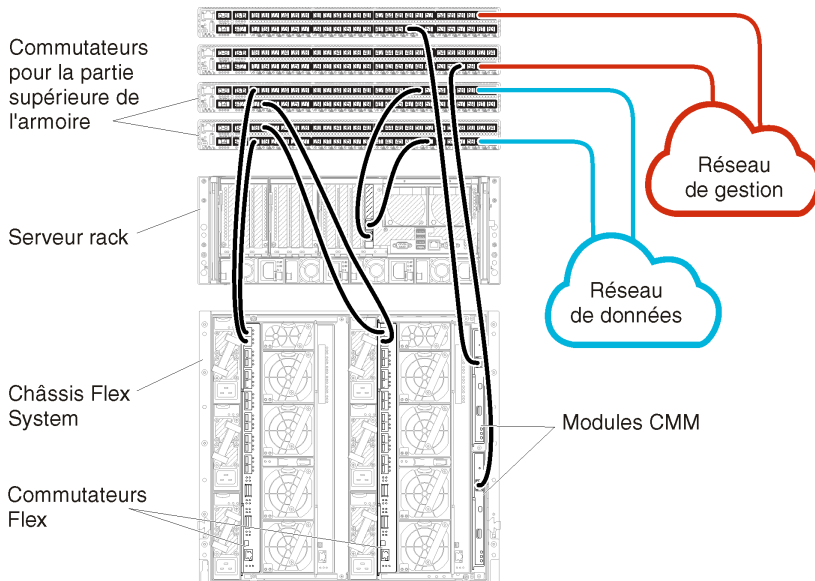


Figure 14. Exemple de câblage pour les réseaux de gestion et de données séparées physiquement

## Étape 2 : Configurer les commutateurs de la partie supérieure de l'armoire

Configurez les commutateurs de la partie supérieure de l'armoire.

### Avant de commencer

Outre les exigences de configuration type des commutateurs de la partie supérieure de l'armoire, vérifiez que tous les ports appropriés sont activés, y compris les ports externes sur les Commutateurs Flex, les serveurs rack, le réseau et les ports internes sur le module CMM, les serveurs rack et le réseau.

### Procédure

Les étapes de configuration peuvent varier, selon le type de commutateurs de type armoire qui sont installés.

Pour savoir comment configurer les commutateurs de la partie supérieure de l'armoire Lenovo, voir [Commutateurs d'armoire dans la documentation en ligne System x](#). Si un autre commutateur de la partie supérieure de l'armoire est installé, consultez la documentation fournie avec ce commutateur.

## Étape 3 : Configurer les Chassis Management Modules (modules CMM)

Configurez le module Chassis Management Module (CMM) principal dans votre châssis pour gérer tous les dispositifs du châssis.

### À propos de cette tâche



Pour obtenir des informations détaillées sur la configuration d'un module CMM, voir [Configuration des composants du châssis dans la documentation en ligne Flex System](#).

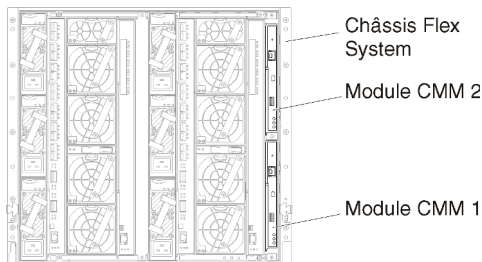
En outre, reportez-vous aux étapes 4.1 à 4.5 sur l'affiche d'instructions fournie avec votre châssis.

## Procédure

Pour configurer le module CMM, procédez comme suit.

Si deux modules CMM sont installés, configurez uniquement le module CMM *principale*, qui synchronise automatiquement la configuration avec le module CMM de secours.

Etape 1. Connectez un câble Ethernet du module CMM de la baie 1 à un poste de travail client pour créer une connexion directe.



Lors de la première connexion au module CMM, vous devrez peut-être modifier les propriétés du protocole Internet sur le poste de travail client.

**Important :** Vérifiez que le sous-réseau du poste de travail client est identique au sous-réseau CMM. (Le sous-réseau CMM par défaut est 255.255.255.0). L'adresse IP choisie pour le poste de travail client doit se trouver sur le même réseau que le module CMM (par exemple, 192.168.70.0 - 192.168.70.24).

Etape 2. Pour lancer l'interface de gestion du module CMM, ouvrez un navigateur Web sur le poste de travail client, et dirigez-le sur l'adresse IP du module CMM.

### Remarques :

- Veillez à utiliser une connexion sécurisée et à ajouter **https** dans l'URL (par exemple, <https://192.168.70.100>). Si vous n'ajoutez pas https, vous recevez une erreur de page introuvable.
- Si vous utilisez l'adresse IP par défaut, 192.168.70.100, l'interface de gestion du module CMM peut être disponible après quelques minutes. Ce délai est lié au fait que le module CMM tente d'obtenir une adresse DHCP pendant deux minutes avant de retomber à l'adresse statique par défaut.

Etape 3. Connectez-vous à l'interface de gestion du module CMM à l'aide de l'ID utilisateur `USERID` et du mot de passe `PASSWORD` par défaut. Après votre connexion, vous devez changer le mot de passe par défaut.

Etape 4. Exécutez l'assistant de configuration initiale du module CMM pour indiquer les détails de votre environnement. L'assistant de configuration initiale comporte les options suivantes :

- Affichez l'inventaire et la santé des châssis.
- Importez la configuration à partir d'un fichier de configuration existant.
- Configurez les paramètres du module CMM général.
- Configurez la date et l'heure du module CMM.

**Conseil :** Lorsque vous installez XClarity Administrator, vous configurez XClarity Administrator et tous les châssis gérés par XClarity Administrator pour utiliser un serveur NTP.

- Configurez les informations IP du module CMM.
- Configurez la stratégie de sécurité du module CMM.
- Configurez le Domain Name System (DNS).
- Configurez les réexpéditeurs d'événement.

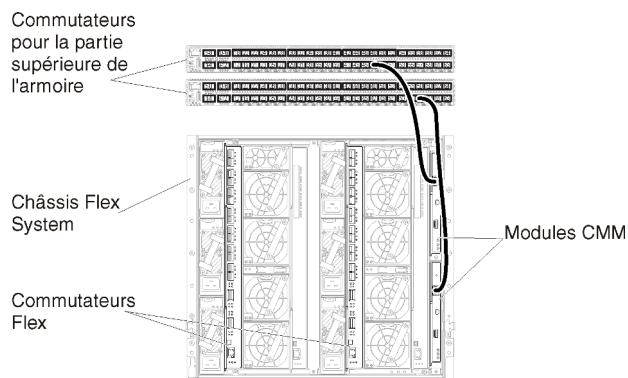
Etape 5. Après avoir sauvegardé les paramètres de l'assistant de configuration et appliqué les modifications, configurez les adresses IP de tous les composants du châssis.

Reportez-vous à l'étape 4.6 de l'affiche d'instructions fournie avec votre châssis.

**Remarque :** Vous devez réinitialiser le processeur de gestion du système pour chaque nœud de traitement et redémarrer les commutateurs Flex pour afficher la nouvelle adresse IP.

Etape 6. Redémarrez le module CMM à l'aide de l'interface de gestion CMM.

Etape 7. Lorsque le module CMM redémarre, connectez un câble du port Ethernet sur le module CMM à votre réseau.



Etape 8. Connectez-vous à l'interface de gestion du module CMM à l'aide de la nouvelle adresse IP.

## Après avoir terminé

Vous pouvez également configurer le module CMM pour prendre en charge la redondance. Utilisez le système d'aide du module CMM pour en savoir plus sur les zones disponibles sur chacune des pages suivantes.

- Configurez le basculement pour le module CMM en cas de panne matérielle dans le module CMM principal. Dans l'interface de gestion du module CMM, cliquez sur **Gestion du module de gestion → Propriétés → Basculement avancé**.
- Configurez le basculement suite à un problème de réseau (liaison montante). Dans l'interface de gestion du module CMM, cliquez sur **Gestion du module de gestion → Réseau**, cliquez sur l'onglet **Ethernet**, puis cliquez sur **Ethernet avancé**. Au minimum, assurez-vous de sélectionner **Basculement en cas de perte de liaison réseau physique**.

## Étape 4 : Configurer Commutateurs Flex

Configurez les Commutateurs Flex dans chaque châssis.

### Avant de commencer

Vérifiez que tous les ports appropriés sont activés, y compris les ports externes du commutateur Flex au commutateur de la partie supérieure de l'armoire et les ports internes au module CMM.

Si les commutateurs Flex sont configurés de façon à obtenir des paramètres réseau dynamique (adresse IP, masque de réseau, passerelle et adresse DNS) sur DHCP, vérifiez que les commutateurs Flex possèdent des paramètres identiques (par exemple, vérifiez que les adresses IP sont dans le même sous-réseau que le module CMM).

**Important :** Pour chaque châssis Flex System, vérifiez que le type de matrice de la carte d'extension dans chaque serveur du châssis est compatible avec le type de matrice de tous les commutateurs Flex installés dans le même châssis. Par exemple, si des commutateurs Ethernet sont installés dans un châssis, tous les serveurs de ce châssis doivent disposer d'une connectivité Ethernet via le connecteur LAN-on-motherboard ou sur une carte d'extension Ethernet. Pour plus d'informations sur la configuration des commutateurs Flex, voir [Configuration des modules d'E-S dans la documentation en ligne Flex Systems](#).

## Procédure

Les étapes de configuration peuvent varier, selon le type de Commutateurs Flex qui sont installés. Pour plus d'informations sur chacun des Commutateurs Flex pris en charge, voir [Commutateurs réseau Flex System dans la documentation en ligne Flex Systems](#).

En général, vous devez configurer les commutateurs Flex dans les baies de commutateurs Flex 1 et 2.

**Astuce :** La baie de commutateur Flex 2 est la troisième baie de module lorsque l'on regarde à l'arrière du châssis.

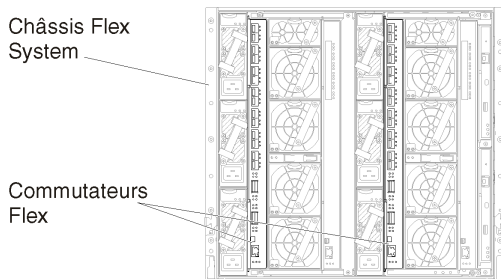


Figure 15. Emplacements Commutateur Flex dans un châssis

## Étape 5 : installation et configuration de l'hôte

Vous pouvez installer Docker sur tout serveur qui satisfait aux exigences de Lenovo XClarity Administrator

### Avant de commencer

Vous pouvez utiliser le centre de données Docker afin de définir un environnement haute disponibilité pour l'exécution des conteneurs XClarity Administrator dans le moteur Docker. Pour plus d'informations sur la haute disponibilité du centre de données Docker, voir [Page Web Architecture et applications haute disponibilité avec le centre de données Docker](#).

Vérifiez que l'hôte respecte les prérequis définis dans [Configurations matérielles et logicielles requises](#).

Vérifiez que le système hôte est dans le même réseau que les dispositifs à gérer.

**Important :** Vous pouvez configurer XClarity Administrator sur tout système qui satisfait aux exigences de XClarity Administrator, dont un serveur géré. Si vous utilisez un serveur géré pour l'hôte XClarity Administrator :

- Vous devez mettre en œuvre une topologie du réseau de gestion et de données séparées virtuellement ou une topologie du réseau de gestion et de donnée unique.

- Vous ne pouvez pas utiliser XClarity Administrator pour appliquer des mises à jour de microprogramme à ce serveur géré. Même dans ce cas, seule une partie du microprogramme est appliquée à l'activation immédiate et XClarity Administrator force le serveur cible à redémarrer, ce qui redémarrerait XClarity Administrator également. Une fois le microprogramme appliqué à l'activation reportée, seule une partie est appliquée lorsque l'hôte XClarity Administrator est redémarré.
- Si vous utilisez un serveur dans un châssis Flex System, vérifiez que le serveur est défini pour se mettre sous tension automatiquement. Vous pouvez définir cette option à partir de l'interface Web CMM en cliquant sur **Gestion de châssis** → **Nœuds de traitement**, puis en sélectionnant le serveur, et en sélectionnant **Alimentation automatique** pour **Mode de mise sous tension automatique**.

## Procédure

Installez et configurez Docker sur l'hôte à l'aide des instructions fournies avec votre distribution Docker.

## Étape 6 : installation et configuration de XClarity Administrator

Installez et configurez le conteneur Lenovo XClarity Administrator sur l'hôte Docker que vous venez d'installer.

### Avant de commencer

Vérifiez que le système hôte respecte les exigences logicielles et matérielles minimales (voir [Configurations matérielles et logicielles requises](#)).

Vérifiez que tous les ports appropriés sont activés, y compris les ports requis par XClarity Administrator (voir [Disponibilité de port](#)).

Vérifiez que le système hôte est dans le même réseau que les dispositifs à gérer.

Assurez-vous que le système d'exploitation hôte et XClarity Administrator utilisent le même serveur NTP.

XClarity Administrator permet un nom personnalisé pour le réseau à utiliser pour la gestion des données et du matériel, ainsi que le déploiement SE (voir [Configurations réseau](#)). Les exemples de la procédure ci-après utilisent eth0.

XClarity Administrator autorise un nom personnalisé pour le réseau à utiliser pour la gestion des données et du matériel et le réseau utilisé pour le déploiement SE (voir [Configurations réseau](#)). Les exemples de la procédure ci-après utilisent respectivement eth0 et eth1

Assurez-vous qu'un réseau macvlan est chargé dans le noyau sur le système hôte. Utilisez la commande **lsmod | grep macvlan** pour vérifier s'il est bien chargé. Exécutez la commande **modprobe macvlan** afin de charger macvlan dans le noyau.

Assurez-vous de bien utiliser un nom unique et une adresse IP pour chaque conteneur lors de l'exécution de plusieurs conteneurs XClarity Administrator dans le même hôte.

Si vous avez l'intention de gérer des appareils ThinkServer et d'autres appareils existants, assurez-vous que Docker est activé pour prendre en charge le protocole IPv6.

1. Éditez le fichier /etc/docker/daemon.json, définissez la clé **ipv6** sur True et définissez la clé **fixed-cidr-v6** sur votre sous-réseau IPv6. Voici un exemple de fichier daemon.

```
{
  "ipv6": true,
  "fixed-cidr-v6": "2001:db8:1::/64",
  "experimental": true,
  "ip6tables": true
}
```

```
}
```

2. Rechargez la configuration Docker en exécutant la commande suivante.  
`systemctl reload docker`

**Remarque** : XClarity Administrator *n'est pas* exécuté en tant que conteneur avec privilèges.

## Procédure

Pour installer un conteneur XClarity Administrator à l'aide de Docker compose, procédez comme suit.

- Etape 1. Téléchargez l'image de dispositif virtuel, le fichier d'environnement et le fichier YAML XClarity Administrator depuis [Page Web de téléchargements XClarity Administrator](#) sur un poste de travail client. Connectez-vous au site Web, puis utilisez la clé d'accès qui vous a été fournie pour télécharger l'image.
- Etape 2. Importez l'image de conteneur XClarity Administrator dans votre hôte Docker en exécutant la commande suivante.  
`docker load -i lnvgv_sw_lxca_<ver>_anyos_noarch.tar.gz`
- Etape 3. Éditez le fichier `docker_compose.env`, puis mettez à jour les variables d'environnement suivantes.
  - **CONTAINER\_NAME**. Nom de conteneur unique, utilisé pour créer des volumes Docker pour chaque instance XClarity Administrator (par exemple, `CONTAINER_NAME=LXCA-203`)
  - **ADDRESS**. Adresse IPv4 statique du conteneur (par exemple, `ADDRESS=192.0.2.0`)
  - **BACKUP\_MOUNT**. (Facultatif) Chemin pour le partage distant qui peut être utilisé pour stocker les sauvegardes XClarity Administrator. Cela doit être `/mnt/backup_share`.
  - **FIRMWARE\_MOUNT**. (Facultatif) Chemin pour le partage distant pouvant être utilisé en tant que référentiel distant pour les mises à jour de microprogramme. Cela doit être `/mnt/fw_share`.

Voici un exemple de fichier d'environnement.

```
CONTAINER_NAME="LXCA-203"  
ADDRESS="192.0.2.0"  
BACKUP_MOUNT="/mnt/backup_share"  
FIRMWARE_MOUNT="/mnt/fw_share"
```

- Etape 4. Éditez `docker_compose.yml` et mettez à jour les propriétés suivantes.
  - Définissez la propriété de l'**image** sur le nom du fichier d'image d'installation utilisé lors de l'étape 2.

**Remarque** : Vous pouvez modifier le nom du fichier d'image (par exemple, « le plus récent ») à l'aide de la commande `docker tag`.
  - Si vous souhaitez utiliser des partages distants en tant que référentiel de microprogramme distant et stocker des sauvegardes XClarity Administrator, définissez le point de montage hôte pour chaque partage distant dans la propriété **volumes**.
  - Définissez la propriété **dns** sur l'adresse IP des serveurs DNS.
  - Le conteneur fait partie du groupe de ressources du processeur et de la mémoire qui sont disponibles pour l'hôte. En option, vous pouvez définir des limites relatives à l'utilisation des ressources en définissant les propriétés **cpus** et **mémoire**.
  - Définissez la propriété **parent** sur le nom de l'interface réseau du système hôte à utiliser en tant qu'interface parent pour l'interface macvlan du conteneur. Cette interface doit avoir un accès direct au sous-réseau affecté au conteneur.
  - Définissez le **sous-réseau** et la **passerelle** en fonction de votre topologie de réseau. En général, le sous-réseau et la passerelle sont pour le réseau de gestion, auquel appartient `${ADDRESS}`.

- Si vous souhaitez prendre en charge le protocole IPv6, définissez la propriété **enable\_ipv6** sur True, définissez la propriété **ipv6\_address** sur l'adresse IPv6 et ajoutez un autre ensemble de propriétés de **sous-réseau** et de **passerelle** en fonction de votre topologie de réseau (généralement pour le réseau de gestion auquel l'adresse IPv6 appartient).

Ce qui suit est un exemple de fichier YAML, avec IPv6 activé.

```
version: '3.8'

services:
  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan1:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2000::2"
      lan2:
        ipv4_address: 192.0.1.3
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.40.10
      - 192.0.50.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

volumes:
  data:
    name: ${CONTAINER_NAME}-data
  postgresql:
    name: ${CONTAINER_NAME}-postgresql
  log:
    name: ${CONTAINER_NAME}-log
  confluent-etc:
    name: ${CONTAINER_NAME}-confluent-etc
  confluent-log:
    name: ${CONTAINER_NAME}-confluent-log
  confluent:
    name: ${CONTAINER_NAME}-confluent
  propconf:
```

```

    name: ${CONTAINER_NAME}-propconf
ssh:
  name: ${CONTAINER_NAME}-ssh
xcat:
  name: ${CONTAINER_NAME}-xcat

networks:
  lan1:
    name: lan1
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: eno1
    ipam:
      config:
        - subnet: 192.0.0.0/19
          gateway: 192.0.30.1
        - subnet: "2001:8003:7d51:2000::/80"
          gateway: "2001:8003:7d51:2000::1"
  lan2:
    name: lan2
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: virbr0
    ipam:
      config:
        - subnet: 192.0.122.0/24
          - subnet: "2001:8003:7d51:2005::/80"

```

Etape 5. Déployez la nouvelle dans Docker en exécutant la commande ci-après, `<ENV_FILENAME>` étant le nom du fichier des variables d'environnement créé lors de l'étape 2.

```
COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d
```

## Après avoir terminé

Connectez-vous et configurez XClarity Administrator (voir [Accès à l'interface Web Lenovo XClarity Administrator la première fois](#) et [Configuration des Lenovo XClarity Administrator](#)).

---

## Données séparées virtuellement et topologie du réseau de gestion

Dans cette topologie, le réseau de données et le réseau de gestion sont virtuellement distincts. Les modules du réseau de données et les modules du réseau de gestion sont envoyés sur la même connexion physique. Le marquage VLAN sur tous les modules de données du réseau de gestion est utilisé pour séparer le trafic entre les deux réseaux.

### Avant de commencer

Vérifiez que tous les ports appropriés sont activés, y compris les ports requis par XClarity Administrator (voir [Disponibilité de port](#)).

Vérifiez que le microprogramme minimal requis est installé sur chaque appareil 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.

Vérifiez que les ID VLAN sont configurés pour le réseau de données et le réseau de gestion. Facultativement, activez le marquage VLAN à partir des Commutateurs Flex si vous implémentez le marquage à partir des

Commutateurs Flex ou activez à partir des commutateurs de la partie supérieure de l'armoire si vous implémentez le marquage à partir de ces commutateurs.

Vérifiez que vous définissez les ports auxquels les modules CMM sont connectés comme appartenant au VLAN de gestion.

**Important :** Configurez les appareils et les composants de manière à réduire au minimum les modifications d'adresse IP. Envisagez d'utiliser des adresses IP statiques au lieu du protocole DHCP (Dynamic Host Configuration Protocol). Si le protocole DHCP est utilisé, faites en sorte que les modifications d'adresse IP soient réduits au minimum.

## À propos de cette tâche

La figure suivante montre un moyen de configurer votre environnement afin que le réseau de gestion soit séparé du réseau virtuel. Les nombres indiqués dans la figure correspondent aux étapes numérotées dans les sections suivantes.

**Remarque :** Cette figure ne représente pas toutes les options de câblage qui peuvent être requises pour votre environnement. Au lieu de cela, cette figure affiche uniquement les exigences d'option de câblage pour les commutateurs Flex, les modules CMM et les serveurs rack, car ils concernent les réseaux de gestion et de données séparés virtuellement.

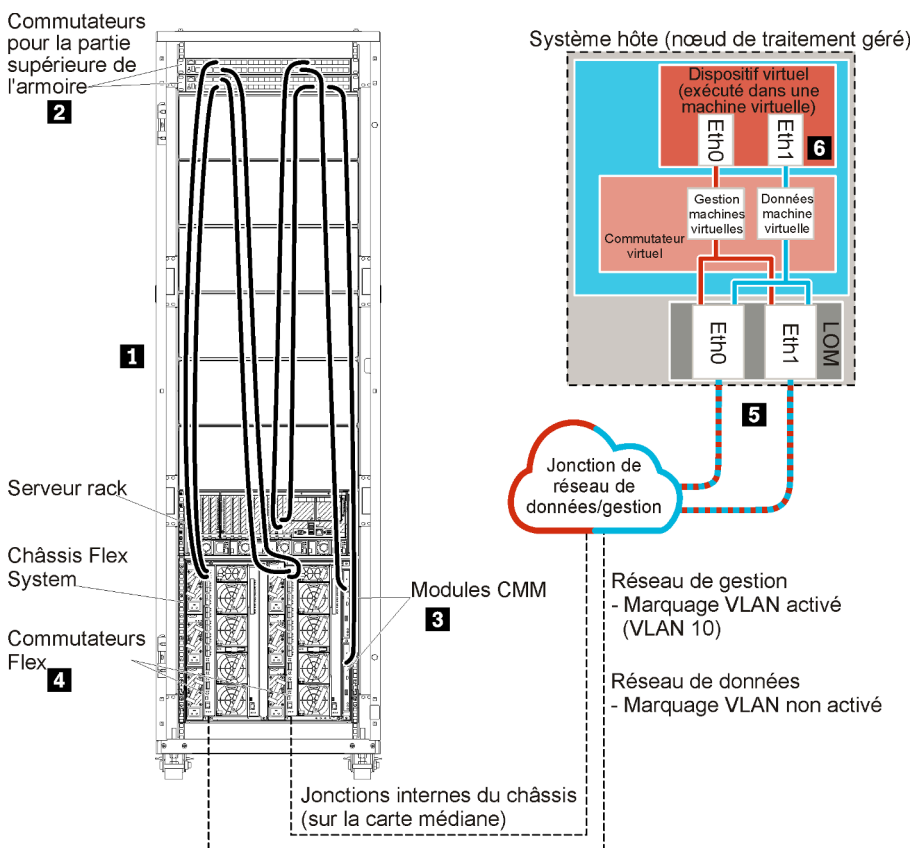


Figure 16. Exemple de données séparées virtuellement et de topologie du réseau de gestion pour un dispositif virtuel



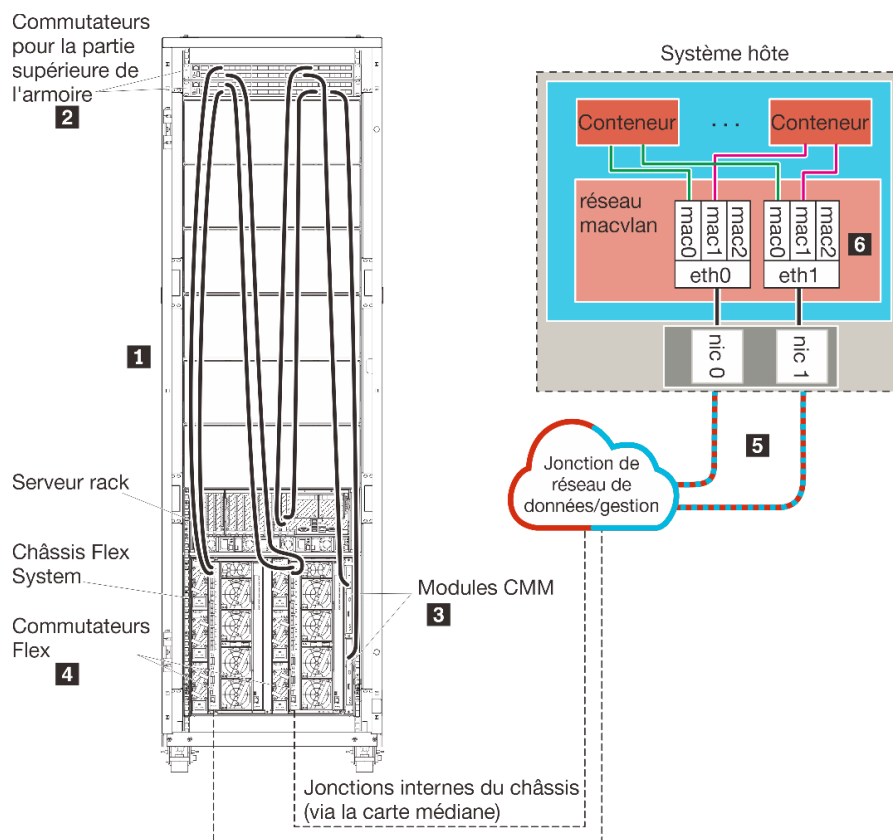


Figure 17. Exemple de données séparées virtuellement et de topologie du réseau de gestion pour les conteneurs

Dans ce scénario, XClarity Administrator est installé sur un serveur dans un châssis Flex System géré par XClarity Administrator.

**Important :** Vous pouvez configurer XClarity Administrator sur tout système qui satisfait aux exigences de XClarity Administrator, dont un serveur géré. Si vous utilisez un serveur géré pour l'hôte XClarity Administrator :

- Vous devez mettre en œuvre une topologie du réseau de gestion et de données séparées virtuellement ou une topologie du réseau de gestion et de donnée unique.
- Vous ne pouvez pas utiliser XClarity Administrator pour appliquer des mises à jour de microprogramme à ce serveur géré. Même dans ce cas, seule une partie du microprogramme est appliquée à l'activation immédiate et XClarity Administrator force le serveur cible à redémarrer, ce qui redémarrerait XClarity Administrator également. Une fois le microprogramme appliqué à l'activation reportée, seule une partie est appliquée lorsque l'hôte XClarity Administrator est redémarré.
- Si vous utilisez un serveur dans un châssis Flex System, vérifiez que le serveur est défini pour se mettre sous tension automatiquement. Vous pouvez définir cette option à partir de l'interface Web CMM en cliquant sur **Gestion de châssis → Nœuds de traitement**, puis en sélectionnant le serveur, et en sélectionnant **Alimentation automatique pour Mode de mise sous tension automatique**.

De plus, dans ce scénario, toutes les données sont envoyées sur les mêmes connexions physiques. La séparation du réseau de gestion à partir du réseau de données est accomplie via le marquage VLAN, dans lequel des balises spécifiques correspondant au réseau de gestion sont ajoutées aux paquets de données entrants pour assurer leur acheminement jusqu'aux interfaces appropriées. Les balises sont supprimées des modules de données sortants.

Le marquage VLAN peut être activé sur l'une des dispositifs suivants :

- **Commutateurs de la partie supérieure de l'armoire.** Les balises VLAN correspondant au réseau de gestion sont ajoutées aux paquets lorsqu'ils entrent dans le commutateur de la partie supérieure de l'armoire et passent via les Commutateurs Flex et sur les serveurs dans le châssis Flex System. Sur le chemin de retour, les étiquettes VLAN sont retirées au fur et à mesure qu'elles sont envoyées à partir du commutateur de la partie supérieure de l'armoire aux contrôleurs de gestion.
- **Commutateurs Flex.** Les balises VLAN correspondant au réseau de gestion sont ajoutées aux paquets lorsqu'ils entrent dans les Commutateurs Flex et sont transmis via les serveurs dans un châssis Flex System. Sur le chemin de retour, des étiquettes VLAN sont ajoutées par les serveurs, et transmises aux Commutateurs Flex, qui les suppriment lors du transfert aux contrôleurs de gestion.

Le choix d'implémenter le marquage VLAN s'appuie sur les besoins et la complexité de votre environnement.

Si vous prévoyez d'installer XClarity Administrator pour gérer des châssis et serveurs rack existants qui ont déjà été configurés, passez à [Étape 5 : installation et configuration de l'hôte](#).

Pour plus d'informations sur la planification pour cette topologie, notamment des informations sur les paramètres réseau et la configuration Eth1 et Eth0, voir [Réseau de données et réseau de gestion séparés virtuellement](#).

## Étape 1 : Câblez le châssis et les serveurs rack sur les commutateurs de la partie supérieure de l'armoire

Câblez le châssis et les serveurs rack sur le même commutateur de la partie supérieure de l'armoire pour activer les communications entre les dispositifs.

### Procédure

Câblez chaque commutateur Flex et module CMM dans chaque châssis et chaque serveur rack aux commutateurs de la partie supérieure de l'armoire. Vous pouvez choisir n'importe quel port dans ce commutateur de la partie supérieure de l'armoire.

La figure suivante montre un exemple qui montre le câblage à partir du châssis (commutateurs Flex et modules CMM) et des serveurs rack aux commutateurs de la partie supérieure de l'armoire lorsque Lenovo XClarity Administrator est installé dans un châssis qui sera géré par XClarity Administrator.

**Remarque :** Cette figure ne représente pas toutes les options de câblage qui peuvent être requises pour votre environnement. Au lieu de cela, cette figure affiche uniquement les exigences d'option de câblage pour les commutateurs Flex, les modules CMM et les serveurs rack, car ils concernent les réseaux de gestion et de données séparés virtuellement.

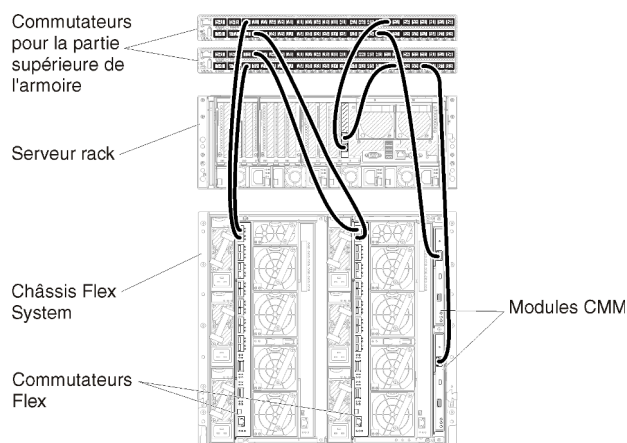


Figure 18. Exemple de câblage pour les réseaux de données séparées virtuellement et de gestion

## Étape 2 : Configurer les commutateurs de la partie supérieure de l'armoire

Configurez les commutateurs de la partie supérieure de l'armoire.

### Avant de commencer

Outre les exigences de configuration type des commutateurs de la partie supérieure de l'armoire, vérifiez que tous les ports appropriés sont activés, y compris les ports externes sur les Commutateurs Flex, les serveurs rack, le réseau et les ports internes sur le module CMM, les serveurs rack et le réseau.

Vous pouvez implémenter le marquage VLAN dans les commutateurs Flex ou les commutateurs de la partie supérieure de l'armoire, selon les besoins et la complexité de votre environnement. Si vous implémentez le balisage à partir des commutateurs de la partie supérieure de l'armoire, activez le marquage VLAN à partir des commutateurs de la partie supérieure de l'armoire.

Vérifiez que les ID VLAN sont configurés pour les réseaux de gestion et de données.

### Procédure

Les étapes de configuration peuvent varier, selon le type de commutateurs de type armoire qui sont installés.

La figure suivante montre un exemple de scénario qui montre le marquage VLAN qui est implémenté dans les commutateurs de la partie supérieure de l'armoire et activé uniquement sur le réseau de gestion. La gestion VLAN est configurée en tant que VLAN 10.

Dans ce scénario, vous devez définir les ports auxquels les modules CMM sont connectés comme appartenant au VLAN de gestion.

**Remarque :** Vous pouvez également activer le marquage VLAN sur le réseau de données pour configurer un VLAN de données.

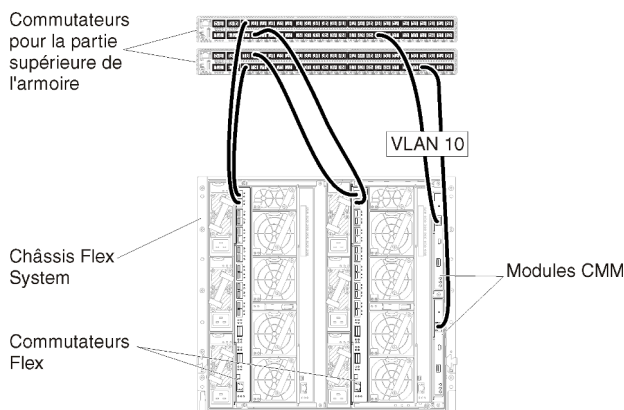


Figure 19. Exemple de configuration pour Commutateurs Flex sur des réseaux de données séparées virtuellement et de gestion (VMware ESXi) dans lesquels le marquage VLAN est activé sur le réseau de gestion.

Pour savoir comment configurer les commutateurs de la partie supérieure de l'armoire Lenovo, voir [Commutateurs d'armoire dans la documentation en ligne System x](#). Si un autre commutateur de la partie supérieure de l'armoire est installé, consultez la documentation fournie avec ce commutateur.

### Étape 3 : Configurer les Chassis Management Modules (modules CMM)

Configurez le module Chassis Management Module (CMM) principal dans votre châssis pour gérer tous les dispositifs du châssis.

#### À propos de cette tâche

Pour obtenir des informations détaillées sur la configuration d'un module CMM, voir [Configuration des composants du châssis dans la documentation en ligne Flex System](#).

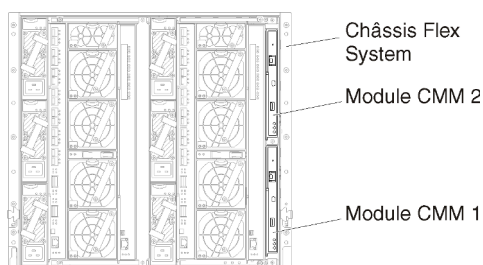
En outre, reportez-vous aux étapes 4.1 à 4.5 sur l'affiche d'instructions fournie avec votre châssis.

#### Procédure

Pour configurer le module CMM, procédez comme suit.

Si deux modules CMM sont installés, configurez uniquement le module CMM *principale*, qui synchronise automatiquement la configuration avec le module CMM de secours.

Étape 1. Connectez un câble Ethernet du module CMM de la baie 1 à un poste de travail client pour créer une connexion directe.



Lors de la première connexion au module CMM, vous devrez peut-être modifier les propriétés du protocole Internet sur le poste de travail client.

**Important :** Vérifiez que le sous-réseau du poste de travail client est identique au sous-réseau CMM. (Le sous-réseau CMM par défaut est 255.255.255.0). L'adresse IP choisie pour le poste de

travail client doit se trouver sur le même réseau que le module CMM (par exemple, 192.168.70.0 - 192.168.70.24).

Etape 2. Pour lancer l'interface de gestion du module CMM, ouvrez un navigateur Web sur le poste de travail client, et dirigez-le sur l'adresse IP du module CMM.

**Remarques :**

- Veillez à utiliser une connexion sécurisée et à ajouter **https** dans l'URL (par exemple, https://192.168.70.100). Si vous n'ajoutez pas https, vous recevez une erreur de page introuvable.
- Si vous utilisez l'adresse IP par défaut, 192.168.70.100, l'interface de gestion du module CMM peut être disponible après quelques minutes. Ce délai est lié au fait que le module CMM tente d'obtenir une adresse DHCP pendant deux minutes avant de retomber à l'adresse statique par défaut.

Etape 3. Connectez-vous à l'interface de gestion du module CMM à l'aide de l'ID utilisateur `USERID` et du mot de passe `PASSWORD` par défaut. Après votre connexion, vous devez changer le mot de passe par défaut.

Etape 4. Exécutez l'assistant de configuration initiale du module CMM pour indiquer les détails de votre environnement. L'assistant de configuration initiale comporte les options suivantes :

- Affichez l'inventaire et la santé des châssis.
- Importez la configuration à partir d'un fichier de configuration existant.
- Configurez les paramètres du module CMM général.
- Configurez la date et l'heure du module CMM.

**Conseil :** Lorsque vous installez XClarity Administrator, vous configurez XClarity Administrator et tous les châssis gérés par XClarity Administrator pour utiliser un serveur NTP.

- Configurez les informations IP du module CMM.
- Configurez la stratégie de sécurité du module CMM.
- Configurez le Domain Name System (DNS).
- Configurez les réexpéditeurs d'événement.

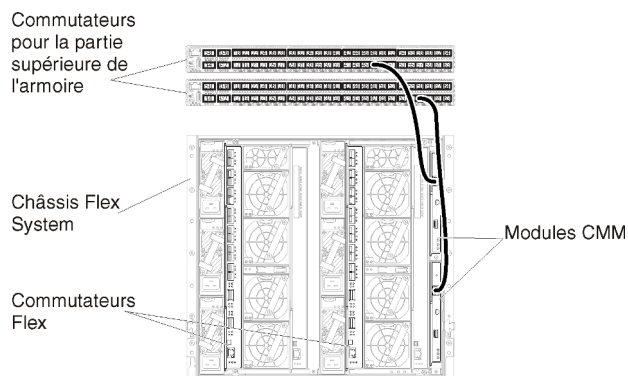
Etape 5. Après avoir sauvegardé les paramètres de l'assistant de configuration et appliqué les modifications, configurez les adresses IP de tous les composants du châssis.

Reportez-vous à l'étape 4.6 de l'affiche d'instructions fournie avec votre châssis.

**Remarque :** Vous devez réinitialiser le processeur de gestion du système pour chaque nœud de traitement et redémarrer les commutateurs Flex pour afficher la nouvelle adresse IP.

Etape 6. Redémarrez le module CMM à l'aide de l'interface de gestion CMM.

Etape 7. Lorsque le module CMM redémarre, connectez un câble du port Ethernet sur le module CMM à votre réseau.



Étape 8. Connectez-vous à l'interface de gestion du module CMM à l'aide de la nouvelle adresse IP.

## Après avoir terminé

Vous pouvez également configurer le module CMM pour prendre en charge la redondance. Utilisez le système d'aide du module CMM pour en savoir plus sur les zones disponibles sur chacune des pages suivantes.

- Configurez le basculement pour le module CMM en cas de panne matérielle dans le module CMM principal. Dans l'interface de gestion du module CMM, cliquez sur **Gestion du module de gestion → Propriétés → Basculement avancé**.
- Configurez le basculement suite à un problème de réseau (liaison montante). Dans l'interface de gestion du module CMM, cliquez sur **Gestion du module de gestion → Réseau**, cliquez sur l'onglet **Ethernet**, puis cliquez sur **Ethernet avancé**. Au minimum, assurez-vous de sélectionner **Basculement en cas de perte de liaison réseau physique**.

## Étape 4 : configuration de Commutateurs Flex

Configurez les Commutateurs Flex dans chaque châssis.

### Avant de commencer

Vérifiez que tous les ports appropriés sont activés, y compris les ports externes du commutateur Flex au commutateur de la partie supérieure de l'armoire et les ports internes au module CMM.

Vous pouvez implémenter le marquage VLAN dans les commutateurs Flex ou les commutateurs de la partie supérieure de l'armoire, selon les besoins et la complexité de votre environnement. Si vous implémentez le balisage à partir des commutateurs Flex, activez le marquage VLAN à partir des commutateurs Flex.

Vérifiez que les ID VLAN sont configurés pour les réseaux de gestion et de données.

**Important** : Pour chaque châssis Flex System, vérifiez que le type de matrice de la carte d'extension dans chaque serveur du châssis est compatible avec le type de matrice de tous les commutateurs Flex installés dans le même châssis. Par exemple, si des commutateurs Ethernet sont installés dans un châssis, tous les serveurs de ce châssis doivent disposer d'une connectivité Ethernet via le connecteur LAN-on-motherboard ou sur une carte d'extension Ethernet. Pour plus d'informations sur la configuration des commutateurs Flex, voir [Configuration des modules d'E-S dans la documentation en ligne Flex Systems](#).

### Procédure

Les étapes de configuration peuvent varier, selon le type de Commutateurs Flex qui sont installés. Pour plus d'informations sur chacun des Commutateurs Flex pris en charge, voir [Commutateurs réseau Flex System dans la documentation en ligne Flex Systems](#).

La figure suivante montre un exemple de scénario qui montre le marquage VLAN qui est implémenté dans les commutateurs Flex et activé uniquement sur le réseau de gestion. La gestion VLAN est configurée en tant que VLAN 10.

**Remarque :** Vous pouvez configurer un VLAN de données en activant le marquage VLAN sur le réseau de données.

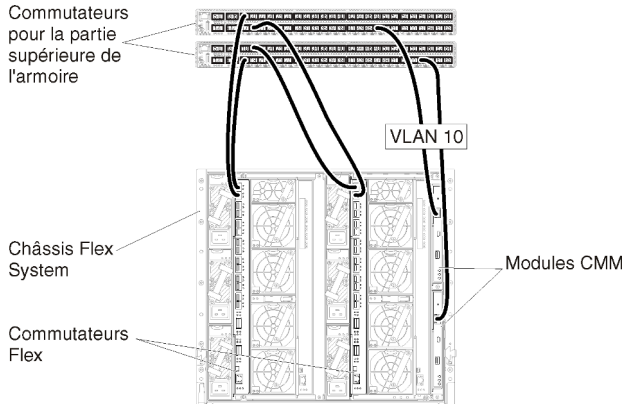


Figure 20. Exemple de configuration pour Commutateurs Flex sur des réseaux de données séparés virtuellement et de gestion (VMware ESXi) dans lesquels le marquage VLAN est activé sur le réseau de gestion.

Procédez comme suit pour configurer les commutateurs Flex pour ce scénario :

Étape 1. Configurez le commutateur Flex dans la baie du commutateur Flex 1 :

- a. Définissez le VLAN de gestion (dans l'exemple, nous avons choisi VLAN 10) pour qu'il contienne le port externe sur lequel le câble est acheminé vers le commutateur de gestion de la partie supérieure de l'armoire (Ext1).
- b. Définissez un port interne pour qu'il fasse partie du VLAN 10 (VLAN de gestion). Assurez-vous que l'acheminement VLAN est activé sur ce port.

Étape 2. Configurez le commutateur Flex dans la baie du commutateur Flex 2 :

**Astuce :** La baie de commutateur Flex 2 est la troisième baie de module lorsque l'on regarde à l'arrière du châssis :

- a. Définissez le VLAN de gestion (dans l'exemple, nous avons choisi VLAN 10) pour qu'il contienne le port externe sur lequel le câble est acheminé vers le commutateur de gestion de la partie supérieure de l'armoire.
- b. Définissez un port interne pour qu'il fasse partie du VLAN 10 (VLAN de gestion). Assurez-vous que l'acheminement VLAN est activé sur ce port.

## Étape 5 : installation et configuration de l'hôte

Vous pouvez installer Docker sur tout système qui satisfait aux exigences de Lenovo XClarity Administrator.

### Avant de commencer

Vous pouvez utiliser le centre de données Docker afin de définir un environnement haute disponibilité pour l'exécution des conteneurs XClarity Administrator dans le moteur Docker. Pour plus d'informations sur la haute disponibilité du centre de données Docker, voir [Page Web Architecture et applications haute disponibilité avec le centre de données Docker](#).

Vérifiez que l'hôte respecte les prérequis définis dans [Configurations matérielles et logicielles requises](#).

Vérifiez que le système hôte est dans le même réseau que les dispositifs à gérer.

**Important** : Vous pouvez configurer XClarity Administrator sur tout système qui satisfait aux exigences de XClarity Administrator, dont un serveur géré. Si vous utilisez un serveur géré pour l'hôte XClarity Administrator :

- Vous devez mettre en œuvre une topologie du réseau de gestion et de données séparées virtuellement ou une topologie du réseau de gestion et de donnée unique.
- Vous ne pouvez pas utiliser XClarity Administrator pour appliquer des mises à jour de microprogramme à ce serveur géré. Même dans ce cas, seule une partie du microprogramme est appliquée à l'activation immédiate et XClarity Administrator force le serveur cible à redémarrer, ce qui redémarrerait XClarity Administrator également. Une fois le microprogramme appliqué à l'activation reportée, seule une partie est appliquée lorsque l'hôte XClarity Administrator est redémarré.
- Si vous utilisez un serveur dans un châssis Flex System, vérifiez que le serveur est défini pour se mettre sous tension automatiquement. Vous pouvez définir cette option à partir de l'interface Web CMM en cliquant sur **Gestion de châssis → Nœuds de traitement**, puis en sélectionnant le serveur, et en sélectionnant **Alimentation automatique** pour **Mode de mise sous tension automatique**.

## Procédure

Installez et configurez Docker sur l'hôte à l'aide des instructions fournies avec votre distribution Docker.

## Étape6: installation et configuration de XClarity Administrator

Installez et configurez le conteneur Lenovo XClarity Administrator sur l'hôte Docker que vous venez d'installer.

### Avant de commencer

Vérifiez que le système hôte respecte les exigences logicielles et matérielles minimales (voir [Configurations matérielles et logicielles requises](#)).

Vérifiez que tous les ports appropriés sont activés, y compris les ports requis par XClarity Administrator (voir [Disponibilité de port](#)).

Vérifiez que le système hôte est dans le même réseau que les dispositifs à gérer.

Assurez-vous que le système d'exploitation hôte et XClarity Administrator utilisent le même serveur NTP.

XClarity Administrator permet un nom personnalisé pour le réseau à utiliser pour la gestion des données et du matériel, ainsi que le déploiement SE (voir [Configurations réseau](#)). Les exemples de la procédure ci-après utilisent eth0.

XClarity Administrator autorise un nom personnalisé pour le réseau à utiliser pour la gestion des données et du matériel et le réseau utilisé pour le déploiement SE (voir [Configurations réseau](#)). Les exemples de la procédure ci-après utilisent respectivement eth0 et eth1.

Assurez-vous qu'un réseau macvlan est chargé dans le noyau sur le système hôte. Utilisez la commande **lsmod | grep macvlan** pour vérifier s'il est bien chargé. Exécutez la commande **modprobe macvlan** afin de charger macvlan dans le noyau.

Assurez-vous de bien utiliser un nom unique et une adresse IP pour chaque conteneur lors de l'exécution de plusieurs conteneurs XClarity Administrator dans le même hôte.



Si vous avez l'intention de gérer des appareils ThinkServer et d'autres appareils existants, assurez-vous que Docker est activé pour prendre en charge le protocole IPv6.

1. Éditez le fichier `/etc/docker/daemon.json`, définissez la clé **ipv6** sur `True` et définissez la clé **fixed-cidr-v6** sur votre sous-réseau IPv6. Voici un exemple de fichier `daemon`.

```
{
  "ipv6": true,
  "fixed-cidr-v6": "2001:db8:1::/64",
  "experimental": true,
  "ip6tables": true
}
```

2. Rechargez la configuration Docker en exécutant la commande suivante.  
`systemctl reload docker`

**Remarque** : XClarity Administrator *n'est pas* exécuté en tant que conteneur avec privilèges.

## Procédure

Pour installer un conteneur XClarity Administrator à l'aide de Docker compose, procédez comme suit.

Étape 1. Téléchargez l'image de dispositif virtuel, le fichier d'environnement et le fichier YAML XClarity Administrator depuis [Page Web de téléchargements XClarity Administrator](#) sur un poste de travail client. Connectez-vous au site Web, puis utilisez la clé d'accès qui vous a été fournie pour télécharger l'image.

Étape 2. Importez l'image de conteneur XClarity Administrator dans votre hôte Docker en exécutant la commande suivante.

```
docker load -i lnvgv_sw_lxca_<ver>_angos_noarch.tar.gz
```

Étape 3. Éditez le fichier `docker_compose.env`, puis mettez à jour les variables d'environnement suivantes.

- **CONTAINER\_NAME**. Nom de conteneur unique, utilisé pour créer des volumes Docker pour chaque instance XClarity Administrator (par exemple, `CONTAINER_NAME=LXCA-203`)
- **ADDRESS**. Adresse IPv4 statique du conteneur (par exemple, `ADDRESS=192.0.2.0`)
- **BACKUP\_MOUNT**. (Facultatif) Chemin pour le partage distant qui peut être utilisé pour stocker les sauvegardes XClarity Administrator. Cela doit être `/mnt/backup_share`.
- **FIRMWARE\_MOUNT**. (Facultatif) Chemin pour le partage distant pouvant être utilisé en tant que référentiel distant pour les mises à jour de microprogramme. Cela doit être `/mnt/fw_share`.

Voici un exemple de fichier d'environnement.

```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

Étape 4. Éditez `docker_compose.yml` et mettez à jour les propriétés suivantes.

- Définissez la propriété de l'**image** sur le nom du fichier d'image d'installation utilisé lors de l'étape 2.

**Remarque** : Vous pouvez modifier le nom du fichier d'image (par exemple, « le plus récent ») à l'aide de la commande `docker tag`.

- Si vous souhaitez utiliser des partages distants en tant que référentiel de microprogramme distant et stocker des sauvegardes XClarity Administrator, définissez le point de montage hôte pour chaque partage distant dans la propriété **volumes**.
- Définissez la propriété **dns** sur l'adresse IP des serveurs DNS.

- Le conteneur fait partie du groupe de ressources du processeur et de la mémoire qui sont disponibles pour l'hôte. En option, vous pouvez définir des limites relatives à l'utilisation des ressources en définissant les propriétés **cpus** et **mémoire**.
- Définissez la propriété **parent** sur le nom de l'interface réseau du système hôte à utiliser en tant qu'interface parent pour l'interface macvlan du conteneur. Cette interface doit avoir un accès direct au sous-réseau affecté au conteneur.
- Définissez le **sous-réseau** et la **passerelle** en fonction de votre topologie de réseau. En général, le sous-réseau et la passerelle sont pour le réseau de gestion, auquel appartient `${ADDRESS}`.
- Si vous souhaitez prendre en charge le protocole IPv6, définissez la propriété **enable\_ipv6** sur `True`, définissez la propriété **ipv6\_address** sur l'adresse IPv6 et ajoutez un autre ensemble de propriétés de **sous-réseau** et de **passerelle** en fonction de votre topologie de réseau (généralement pour le réseau de gestion auquel l'adresse IPv6 appartient).

Ce qui suit est un exemple de fichier YAML, avec IPv6 activé.

```

version: '3.8'

services:

  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan1:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2000::2"
      lan2:
        ipv4_address: 192.0.1.3
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.40.10
      - 192.0.50.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

volumes:
  data:
    name: ${CONTAINER_NAME}-data

```

```

postgresql:
  name: ${CONTAINER_NAME}-postgresql
log:
  name: ${CONTAINER_NAME}-log
confluent-etc:
  name: ${CONTAINER_NAME}-confluent-etc
confluent-log:
  name: ${CONTAINER_NAME}-confluent-log
confluent:
  name: ${CONTAINER_NAME}-confluent
propconf:
  name: ${CONTAINER_NAME}-propconf
ssh:
  name: ${CONTAINER_NAME}-ssh
xcat:
  name: ${CONTAINER_NAME}-xcat

networks:
  lan1:
    name: lan1
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: eno1
    ipam:
      config:
        - subnet: 192.0.0.0/19
          gateway: 192.0.30.1
        - subnet: "2001:8003:7d51:2000::/80"
          gateway: "2001:8003:7d51:2000::1"
  lan2:
    name: lan2
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: virbr0
    ipam:
      config:
        - subnet: 192.0.122.0/24
          gateway: 192.0.122.1
        - subnet: "2001:8003:7d51:2003::/80"
          gateway: "2001:8003:7d51:2003::1"

```

Etape 5. Déployez la nouvelle dans Docker en exécutant la commande ci-après, `<ENV_FILENAME>` étant le nom du fichier des variables d'environnement créé lors de l'étape 2.

```
COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d
```

## Après avoir terminé

Connectez-vous et configurez XClarity Administrator (voir [Accès à l'interface Web Lenovo XClarity Administrator la première fois](#) et [Configuration des Lenovo XClarity Administrator](#)).

---

## Topologie du réseau de gestion uniquement

Dans cette topologie, Lenovo XClarity Administrator ne possède que le réseau de gestion. Il ne possède pas le réseau de données.

## Avant de commencer

Vérifiez que tous les ports appropriés sont activés, y compris :

- Ports requis par XClarity Administrator (voir [Disponibilité de port](#))
- Ports externes sur le réseau
- Ports internes sur le module CMM

Vérifiez que le microprogramme minimal requis est installé sur chaque appareil 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 :** Configurez les appareils et les composants de manière à réduire au minimum les modifications d'adresse IP. Envisagez d'utiliser des adresses IP statiques au lieu du protocole DHCP (Dynamic Host Configuration Protocol). Si le protocole DHCP est utilisé, faites en sorte que les modifications d'adresse IP soient réduits au minimum.

## À propos de cette tâche

La figure suivante montre un moyen de configurer votre environnement si Lenovo XClarity Administrator ne possède que le réseau de gestion (et non le réseau de données). Les nombres indiqués dans la figure correspondent aux étapes numérotées dans les sections suivantes.

**Remarque :** Cette figure ne représente pas toutes les options de câblage qui peuvent être requises pour votre environnement. Au lieu de cela, cette figure affiche uniquement les exigences d'option de câblage pour les commutateurs Flex, les modules CMM et les serveurs rack, car ils concernent la configuration d'un réseau de gestion uniquement.

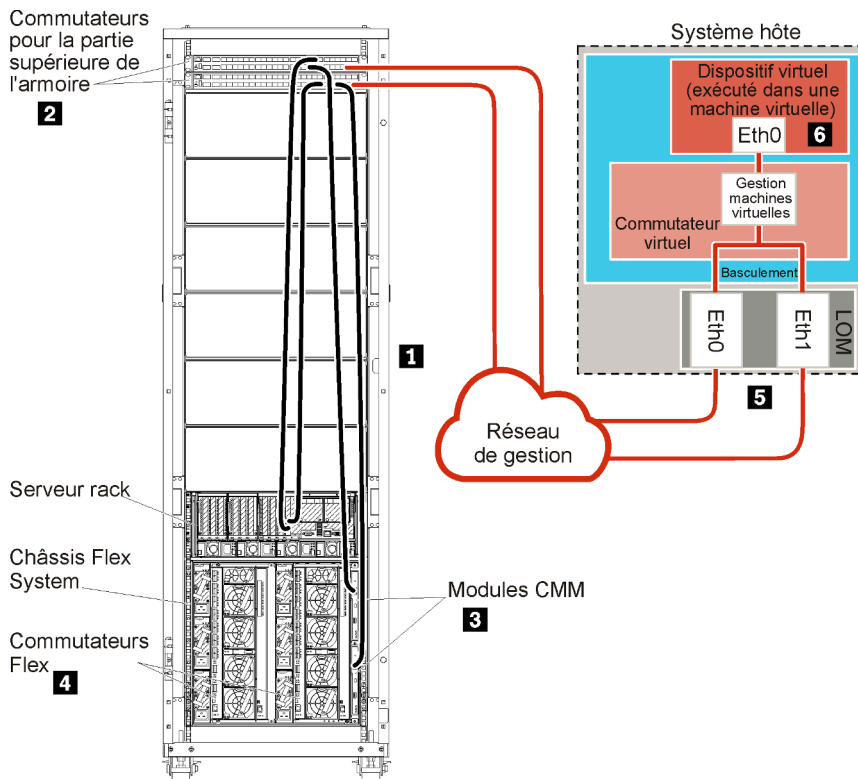


Figure 21. Exemple de topologie du réseau de gestion uniquement pour un dispositif virtuel

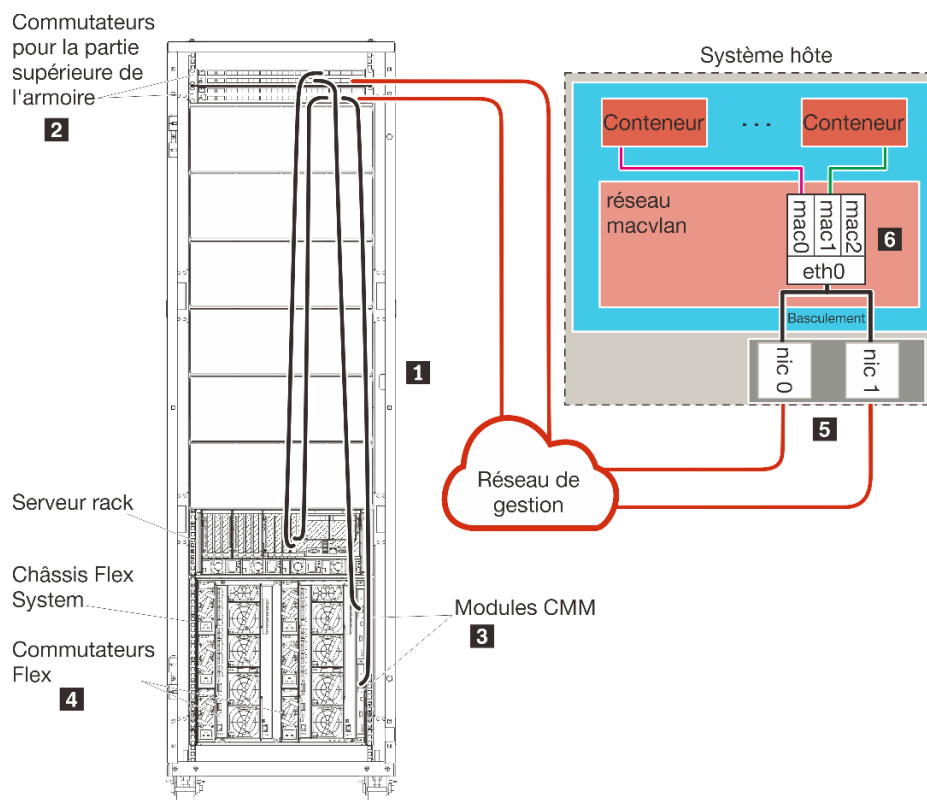


Figure 22. Exemple de topologie du réseau de gestion uniquement pour les conteneurs

Si vous prévoyez d'installer XClarity Administrator pour gérer des châssis et serveurs rack existants qui ont déjà été configurés, passez à [Étape 5 : installation et configuration de l'hôte](#).

Pour plus d'informations sur la planification pour cette topologie, notamment des informations sur les paramètres réseau et la configuration Eth1 et Eth0, voir [Réseau de gestion uniquement](#).

## Étape 1 : Câblez le châssis, les serveurs rack et l'hôte Lenovo XClarity Administrator sur les commutateurs de la partie supérieure de l'armoire

Câblez le châssis, les serveurs rack et l'hôte XClarity Administrator aux commutateurs de la partie supérieure de l'armoire pour activer les communications entre les dispositifs et votre réseau.

### Procédure

Câblez chaque commutateur Flex et module CMM dans chaque châssis, chaque serveur rack, et l'hôte XClarity Administrator aux commutateurs de la partie supérieure de l'armoire. Vous pouvez choisir n'importe quel port dans les commutateurs de la partie supérieure de l'armoire.

La figure suivante est un exemple qui montre le câblage du châssis (commutateurs Flex et modules CMM), des serveurs rack et de l'hôte XClarity Administrator aux commutateurs de la partie supérieure de l'armoire.

**Remarque :** Cette figure ne représente pas toutes les options de câblage qui peuvent être requises pour votre environnement. Au lieu de cela, cette figure affiche uniquement les exigences d'option de câblage pour les commutateurs Flex, les modules CMM et les serveurs rack, car ils concernent la configuration d'un réseau de gestion uniquement.

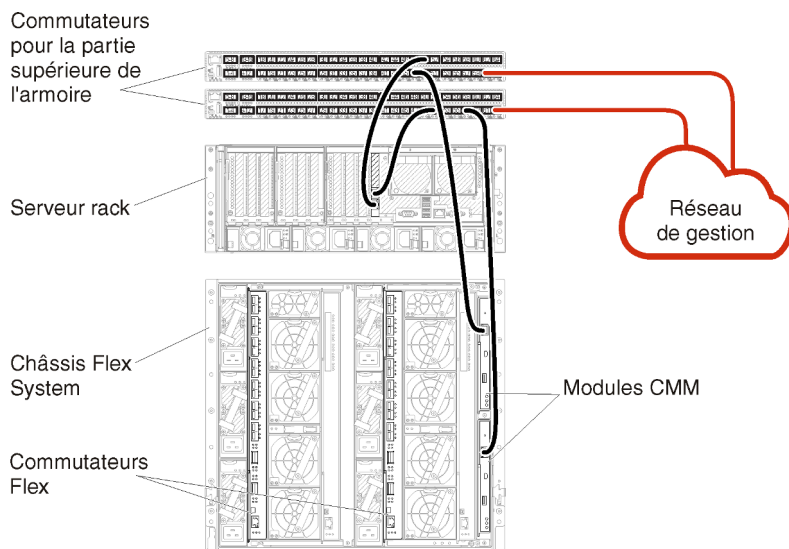


Figure 23. Exemple de câblage pour un réseau de gestion uniquement

## Étape 2 : Configurer les commutateurs de la partie supérieure de l'armoire

Configurez les commutateurs de la partie supérieure de l'armoire.

### Avant de commencer

Outre les exigences de configuration type des commutateurs de la partie supérieure de l'armoire, vérifiez que tous les ports appropriés sont activés, y compris les ports externes sur les Commutateurs Flex, les serveurs rack, le réseau et les ports internes sur le module CMM, les serveurs rack et le réseau.

### Procédure

Les étapes de configuration peuvent varier, selon le type de commutateurs de type armoire qui sont installés.

Pour savoir comment configurer les commutateurs de la partie supérieure de l'armoire Lenovo, voir [Commutateurs d'armoire dans la documentation en ligne System x](#). Si un autre commutateur de la partie supérieure de l'armoire est installé, consultez la documentation fournie avec ce commutateur.

## Étape 3 : Configurer les Chassis Management Modules (modules CMM)

Configurez le module Chassis Management Module (CMM) principal dans votre châssis pour gérer tous les dispositifs du châssis.

### À propos de cette tâche

Pour obtenir des informations détaillées sur la configuration d'un module CMM, voir [Configuration des composants du châssis dans la documentation en ligne Flex System](#).

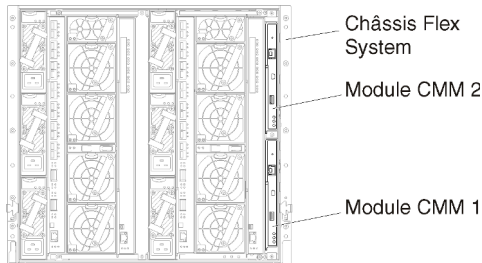
En outre, reportez-vous aux étapes 4.1 à 4.5 sur l'affiche d'instructions fournie avec votre châssis.

### Procédure

Pour configurer le module CMM, procédez comme suit.

Si deux modules CMM sont installés, configurez uniquement le module CMM *principal*, qui synchronise automatiquement la configuration avec le module CMM de secours.

Etape 1. Connectez un câble Ethernet du module CMM de la baie 1 à un poste de travail client pour créer une connexion directe.



Lors de la première connexion au module CMM, vous devrez peut-être modifier les propriétés du protocole Internet sur le poste de travail client.

**Important :** Vérifiez que le sous-réseau du poste de travail client est identique au sous-réseau CMM. (Le sous-réseau CMM par défaut est 255.255.255.0). L'adresse IP choisie pour le poste de travail client doit se trouver sur le même réseau que le module CMM (par exemple, 192.168.70.0 - 192.168.70.24).

Etape 2. Pour lancer l'interface de gestion du module CMM, ouvrez un navigateur Web sur le poste de travail client, et dirigez-le sur l'adresse IP du module CMM.

**Remarques :**

- Veillez à utiliser une connexion sécurisée et à ajouter **https** dans l'URL (par exemple, <https://192.168.70.100>). Si vous n'ajoutez pas https, vous recevez une erreur de page introuvable.
- Si vous utilisez l'adresse IP par défaut, 192.168.70.100, l'interface de gestion du module CMM peut être disponible après quelques minutes. Ce délai est lié au fait que le module CMM tente d'obtenir une adresse DHCP pendant deux minutes avant de retomber à l'adresse statique par défaut.

Etape 3. Connectez-vous à l'interface de gestion du module CMM à l'aide de l'ID utilisateur `USERID` et du mot de passe `PASSWORD` par défaut. Après votre connexion, vous devez changer le mot de passe par défaut.

Etape 4. Exécutez l'assistant de configuration initiale du module CMM pour indiquer les détails de votre environnement. L'assistant de configuration initiale comporte les options suivantes :

- Affichez l'inventaire et la santé des châssis.
- Importez la configuration à partir d'un fichier de configuration existant.
- Configurez les paramètres du module CMM général.
- Configurez la date et l'heure du module CMM.

**Conseil :** Lorsque vous installez XClarity Administrator, vous configurez XClarity Administrator et tous les châssis gérés par XClarity Administrator pour utiliser un serveur NTP.

- Configurez les informations IP du module CMM.
- Configurez la stratégie de sécurité du module CMM.
- Configurez le Domain Name System (DNS).
- Configurez les réexpéditeurs d'événement.

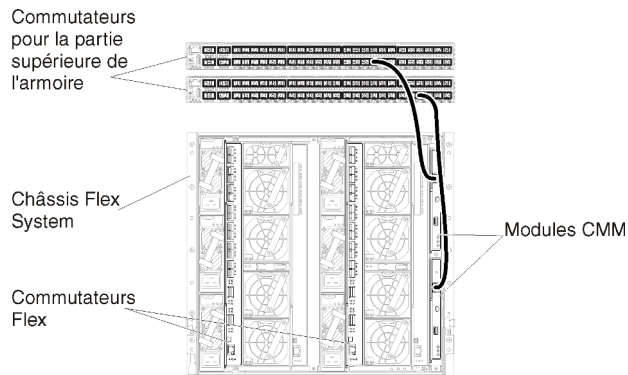
Etape 5. Après avoir sauvegardé les paramètres de l'assistant de configuration et appliqué les modifications, configurez les adresses IP de tous les composants du châssis.

Reportez-vous à l'étape 4.6 de l'affiche d'instructions fournie avec votre châssis.

**Remarque :** Vous devez réinitialiser le processeur de gestion du système pour chaque nœud de traitement et redémarrer les commutateurs Flex pour afficher la nouvelle adresse IP.

Etape 6. Redémarrez le module CMM à l'aide de l'interface de gestion CMM.

Etape 7. Lorsque le module CMM redémarre, connectez un câble du port Ethernet sur le module CMM à votre réseau.



Etape 8. Connectez-vous à l'interface de gestion du module CMM à l'aide de la nouvelle adresse IP.

## Après avoir terminé

Vous pouvez également configurer le module CMM pour prendre en charge la redondance. Utilisez le système d'aide du module CMM pour en savoir plus sur les zones disponibles sur chacune des pages suivantes.

- Configurez le basculement pour le module CMM en cas de panne matérielle dans le module CMM principal. Dans l'interface de gestion du module CMM, cliquez sur **Gestion du module de gestion → Propriétés → Basculement avancé**.
- Configurez le basculement suite à un problème de réseau (liaison montante). Dans l'interface de gestion du module CMM, cliquez sur **Gestion du module de gestion → Réseau**, cliquez sur l'onglet **Ethernet**, puis cliquez sur **Ethernet avancé**. Au minimum, assurez-vous de sélectionner **Basculement en cas de perte de liaison réseau physique**.

## Étape 4 : Configurer Commutateurs Flex

Configurez les Commutateurs Flex dans chaque châssis.

### Avant de commencer

Vérifiez que tous les ports appropriés sont activés, y compris les ports externes du commutateur Flex au commutateur de la partie supérieure de l'armoire et les ports internes au module CMM.

Si les commutateurs Flex sont configurés de façon à obtenir des paramètres réseau dynamique (adresse IP, masque de réseau, passerelle et adresse DNS) sur DHCP, vérifiez que les commutateurs Flex possèdent des paramètres identiques (par exemple, vérifiez que les adresses IP sont dans le même sous-réseau que le module CMM).

**Important :** Pour chaque châssis Flex System, vérifiez que le type de matrice de la carte d'extension dans chaque serveur du châssis est compatible avec le type de matrice de tous les commutateurs Flex installés dans le même châssis. Par exemple, si des commutateurs Ethernet sont installés dans un châssis, tous les serveurs de ce châssis doivent disposer d'une connectivité Ethernet via le connecteur LAN-on-motherboard



ou sur une carte d'extension Ethernet. Pour plus d'informations sur la configuration des commutateurs Flex, voir [Configuration des modules d'E-S dans la documentation en ligne Flex Systems](#).

## Procédure

Les étapes de configuration peuvent varier, selon le type de Commutateurs Flex qui sont installés. Pour plus d'informations sur chacun des Commutateurs Flex pris en charge, voir [Commutateurs réseau Flex System dans la documentation en ligne Flex Systems](#).

En général, vous devez configurer les commutateurs Flex dans les baies de commutateurs Flex 1 et 2.

**Astuce :** La baie de commutateur Flex 2 est la troisième baie de module lorsque l'on regarde à l'arrière du châssis.

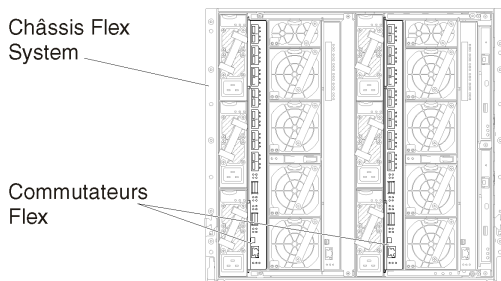


Figure 24. Emplacements Commutateur Flex dans un châssis

## Étape 5 : installation et configuration de l'hôte

Vous pouvez installer Docker sur tout système qui satisfait aux exigences de Lenovo XClarity Administrator.

### Avant de commencer

Vous pouvez utiliser le centre de données Docker afin de définir un environnement haute disponibilité pour l'exécution des conteneurs XClarity Administrator dans le moteur Docker. Pour plus d'informations sur la haute disponibilité du centre de données Docker, voir [Page Web Architecture et applications haute disponibilité avec le centre de données Docker](#).

Vérifiez que l'hôte respecte les prérequis définis dans [Configurations matérielles et logicielles requises](#).

Vérifiez que le système hôte est dans le même réseau que les dispositifs à gérer.

**Important :** Vous pouvez configurer XClarity Administrator sur tout système qui satisfait aux exigences de XClarity Administrator, dont un serveur géré. Si vous utilisez un serveur géré pour l'hôte XClarity Administrator :

- Vous devez mettre en œuvre une topologie du réseau de gestion et de données séparées virtuellement ou une topologie du réseau de gestion et de donnée unique.
- Vous ne pouvez pas utiliser XClarity Administrator pour appliquer des mises à jour de microprogramme à ce serveur géré. Même dans ce cas, seule une partie du microprogramme est appliquée à l'activation immédiate et XClarity Administrator force le serveur cible à redémarrer, ce qui redémarrerait XClarity Administrator également. Une fois le microprogramme appliqué à l'activation reportée, seule une partie est appliquée lorsque l'hôte XClarity Administrator est redémarré.
- Si vous utilisez un serveur dans un châssis Flex System, vérifiez que le serveur est défini pour se mettre sous tension automatiquement. Vous pouvez définir cette option à partir de l'interface Web CMM en

cliquant sur **Gestion de châssis** → **Nœuds de traitement**, puis en sélectionnant le serveur, et en sélectionnant **Alimentation automatique** pour **Mode de mise sous tension automatique**.

## Procédure

Installez et configurez Docker sur l'hôte à l'aide des instructions fournies avec votre distribution Docker.

## Étape 6 : installation et configuration de XClarity Administrator

Installez et configurez le conteneur Lenovo XClarity Administrator sur l'hôte Docker que vous venez d'installer.

### Avant de commencer

Vérifiez que le système hôte respecte les exigences logicielles et matérielles minimales (voir [Configurations matérielles et logicielles requises](#)).

Vérifiez que tous les ports appropriés sont activés, y compris les ports requis par XClarity Administrator (voir [Disponibilité de port](#)).

Vérifiez que le système hôte est dans le même réseau que les dispositifs à gérer.

Assurez-vous que le système d'exploitation hôte et XClarity Administrator utilisent le même serveur NTP.

XClarity Administrator permet un nom personnalisé pour le réseau à utiliser pour la gestion des données et du matériel, ainsi que le déploiement SE (voir [Configurations réseau](#)). Les exemples de la procédure ci-après utilisent eth0.

XClarity Administrator permet un nom personnalisé pour le réseau à utiliser pour la gestion des données et du matériel (voir [Configurations réseau](#)). Les exemples de la procédure ci-après utilisent eth0

Assurez-vous qu'un réseau macvlan est chargé dans le noyau sur le système hôte. Utilisez la commande **lsmod | grep macvlan** pour vérifier s'il est bien chargé. Exécutez la commande **modprobe macvlan** afin de charger macvlan dans le noyau.

Assurez-vous de bien utiliser un nom unique et une adresse IP pour chaque conteneur lors de l'exécution de plusieurs conteneurs XClarity Administrator dans le même hôte.

Si vous avez l'intention de gérer des appareils ThinkServer et d'autres appareils existants, assurez-vous que Docker est activé pour prendre en charge le protocole IPv6.

1. Éditez le fichier `/etc/docker/daemon.json`, définissez la clé **ipv6** sur `True` et définissez la clé **fixed-cidr-v6** sur votre sous-réseau IPv6. Voici un exemple de fichier `daemon.json`.

```
{
  "ipv6": true,
  "fixed-cidr-v6": "2001:db8:1::/64",
  "experimental": true,
  "ip6tables": true
}
```

2. Rechargez la configuration Docker en exécutant la commande suivante.  
`systemctl reload docker`

**Remarque** : XClarity Administrator *n'est pas* exécuté en tant que conteneur avec privilèges.

## Procédure

Pour installer un conteneur XClarity Administrator à l'aide de Docker compose, procédez comme suit.

Etape 1. Téléchargez l'image de dispositif virtuel, le fichier d'environnement et le fichier YAML XClarity Administrator depuis [Page Web de téléchargements XClarity Administrator](#) sur un poste de travail client. Connectez-vous au site Web, puis utilisez la clé d'accès qui vous a été fournie pour télécharger l'image.

Etape 2. Importez l'image de conteneur XClarity Administrator dans votre hôte Docker en exécutant la commande suivante.

```
docker load -i lnvggy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

Etape 3. Éditez le fichier `docker_compose.env`, puis mettez à jour les variables d'environnement suivantes.

- **CONTAINER\_NAME.** Nom de conteneur unique, utilisé pour créer des volumes Docker pour chaque instance XClarity Administrator (par exemple, `CONTAINER_NAME=LXCA-203`)
- **ADDRESS.** Adresse IPv4 statique du conteneur (par exemple, `ADDRESS=192.0.2.0`)
- **BACKUP\_MOUNT.** (Facultatif) Chemin pour le partage distant qui peut être utilisé pour stocker les sauvegardes XClarity Administrator. Cela doit être `/mnt/backup_share`.
- **FIRMWARE\_MOUNT.** (Facultatif) Chemin pour le partage distant pouvant être utilisé en tant que référentiel distant pour les mises à jour de microprogramme. Cela doit être `/mnt/fw_share`.

Voici un exemple de fichier d'environnement.

```
CONTAINER_NAME="LXCA-203"  
ADDRESS="192.0.2.0"  
BACKUP_MOUNT="/mnt/backup_share"  
FIRMWARE_MOUNT="/mnt/fw_share"
```

Etape 4. Éditez `docker_compose.yml` et mettez à jour les propriétés suivantes.

- Définissez la propriété de l'**image** sur le nom du fichier d'image d'installation utilisé lors de l'étape 2.

**Remarque :** Vous pouvez modifier le nom du fichier d'image (par exemple, « le plus récent ») à l'aide de la commande `docker tag`.

- Si vous souhaitez utiliser des partages distants en tant que référentiel de microprogramme distant et stocker des sauvegardes XClarity Administrator, définissez le point de montage hôte pour chaque partage distant dans la propriété **volumes**.
- Définissez la propriété **dns** sur l'adresse IP des serveurs DNS.
- Le conteneur fait partie du groupe de ressources du processeur et de la mémoire qui sont disponibles pour l'hôte. En option, vous pouvez définir des limites relatives à l'utilisation des ressources en définissant les propriétés **cpus** et **mémoire**.
- Définissez la propriété **parent** sur le nom de l'interface réseau du système hôte à utiliser en tant qu'interface parent pour l'interface `macvlan` du conteneur. Cette interface doit avoir un accès direct au sous-réseau affecté au conteneur.
- Définissez le **sous-réseau** et la **passerelle** en fonction de votre topologie de réseau. En général, le sous-réseau et la passerelle sont pour le réseau de gestion, auquel appartient `${ADDRESS}`.
- Si vous souhaitez prendre en charge le protocole IPv6, définissez la propriété **enable\_ipv6** sur `True`, définissez la propriété **ipv6\_address** sur l'adresse IPv6 et ajoutez un autre ensemble de propriétés de **sous-réseau** et de **passerelle** en fonction de votre topologie de réseau (généralement pour le réseau de gestion auquel l'adresse IPv6 appartient).

Ce qui suit est un exemple de fichier YML, avec IPv6 activé.

```
version: '3.8'
```

```

services:
  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.2.10
      - 192.0.2.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

volumes:
  data:
    name: ${CONTAINER_NAME}-data
  postgresql:
    name: ${CONTAINER_NAME}-postgresql
  log:
    name: ${CONTAINER_NAME}-log
  confluent-etc:
    name: ${CONTAINER_NAME}-confluent-etc
  confluent-log:
    name: ${CONTAINER_NAME}-confluent-log
  confluent:
    name: ${CONTAINER_NAME}-confluent
  propconf:
    name: ${CONTAINER_NAME}-propconf
  ssh:
    name: ${CONTAINER_NAME}-ssh
  xcat:
    name: ${CONTAINER_NAME}-xcat

networks:
  lan:
    name: lan
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: eth0

```

```
ipam:
  config:
    - subnet: 192.0.0.0/19
      gateway: 192.0.30.1
    - subnet: "2001:8003:7d51:2000::/80"
      gateway: "2001:8003:7d51:2000::1"
```

Etape 5. Déployez la nouvelle dans Docker en exécutant la commande ci-après, `<ENV_FILENAME>` étant le nom du fichier des variables d'environnement créé lors de l'étape 2.

```
COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d
```

## Après avoir terminé

Connectez-vous et configurez XClarity Administrator (voir [Accès à l'interface Web Lenovo XClarity Administrator la première fois](#) et [Configuration des Lenovo XClarity Administrator](#)).

---

## Mise en place de la haute disponibilité

Vous pouvez utiliser le centre de données Docker afin de définir un environnement haute disponibilité pour l'exécution des conteneurs Lenovo XClarity Administrator dans le moteur Docker.

Pour plus d'informations sur la haute disponibilité du centre de données Docker, voir [Page Web Architecture et applications haute disponibilité avec le centre de données Docker](#).



---

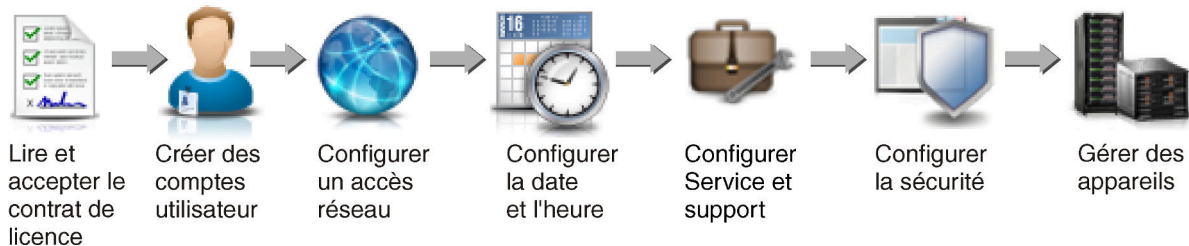
## Chapitre 4. Configuration des Lenovo XClarity Administrator

Lorsque vous accédez à Lenovo XClarity Administrator pour la première fois, il existe plusieurs étapes à exécuter pour la configuration initiale de XClarity Administrator.

**En savoir plus :**  [XClarity Administrator : configuration pour la première fois](#)

### Procédure

Procédez comme suit pour configurer XClarity Administrator pour la première fois.



Etape 1. Accès à l'interface Web de XClarity Administrator.

Etape 2. Lisez et acceptez le contrat de licence.

Etape 3. Créez des comptes utilisateurs qui disposent des droits de superviseur.

**Astuce :** Pensez à créer au moins deux comptes utilisateurs avec des droits de superviseur, afin de disposer d'un compte de secours en cas de besoin.

Etape 4. Configurez l'accès réseau, y compris les adresses IP pour les réseaux de données et de gestion.

Etape 5. Configurez la date et l'heure.

Etape 6. Configurez les paramètres de service et de support technique, y compris la déclaration de confidentialité, les données d'utilisation et matérielles, le support Lenovo (Appel vers Lenovo), la fonction de téléchargement Lenovo et la garantie du produit.

Etape 7. Configurez les paramètres de sécurité, y compris le serveur d'authentification, les groupes d'utilisateurs, les certificats du serveur et le mode de chiffrement.

Etape 8. Gérez votre châssis, serveurs, commutateurs et dispositifs de stockage.

---

### Accès à l'interface Web Lenovo XClarity Administrator la première fois

Vous pouvez lancer l'interface Web de XClarity Administrator à partir de n'importe quel ordinateur disposant d'une connectivité réseau à la machine virtuelle XClarity Administrator.

#### 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 accéder à l'interface Web de XClarity Administrator pour la première fois, 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 que XClarity 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 est 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`








Etape 2. Il est possible que vous receviez des avertissements relatifs à la sécurité ou au certificat la première fois que vous accédez à Lenovo XClarity Administrator. Vous pouvez les ignorer.

## Résultats

La page Configuration initiale s'affiche.

### Configuration initiale

Langue :

	<b>Lisez et acceptez le contrat de licence Lenovo® XClarity Administrator</b>	>
	<b>Créer un compte utilisateur</b>	>
	<b>Configurer l'accès au réseau</b> Configurer les paramètres IP pour la gestion et l'accès au réseau de données.	>
	<b>Configurer des préférences de date et heure</b> Définissez une date et une heure locales ou utilisez le serveur externe Network Time Protocol (NTP).	>
	<b>Configurer les paramètres de service et support</b> Accédez à la page de service et support pour configurer les paramètres.	>
	<b>Configurer des paramètres de sécurité supplémentaires</b> Passez à la page Sécurité afin modifier les valeurs par défaut des certificats, des groupes d'utilisateurs et du client LDAP.	>
	<b>Démarrer les systèmes de gestion</b> Passez à la page Reconnaître et gérer de nouveaux appareils, afin de sélectionner les systèmes à gérer.	>

## Après avoir terminé

Pour configurer XClarity Administrator, effectuez la procédure de configuration initiale (voir [Configuration des Lenovo XClarity Administrator](#)).

---

## Création de comptes utilisateur

Les comptes utilisateurs sont utilisés pour gérer l'autorisation et l'accès à Lenovo XClarity Administrator et aux appareils sous authentification gérée.

### 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 créer des comptes utilisateur, procédez comme suit.


Etape 1. Dans la boîte de dialogue Créer un nouvel utilisateur superviseur, renseignez les informations suivantes.

- 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 de rôles](#) dans la documentation en ligne de XClarity Administrator.

- (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 2. Cliquez sur **Créer**.

Etape 3. Cliquez sur l'icône **Créer** () et répétez les étapes précédentes pour créer des utilisateurs supplémentaires.

Etape 4. Cliquez sur **Revenir à la configuration initiale**.

---

## Configuration de l'accès réseau

Pour configurer l'accès réseau, vous pouvez configurer jusqu'à deux interfaces réseau, le nom d'hôte pour Lenovo XClarity Administrator, et les serveurs DNS à utiliser.

### 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 3. 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)	<p>Réseau de gestion</p> <ul style="list-style-type: none"> <li>• Reconnaissance et gestion</li> <li>• Configuration du serveur</li> <li>• Mises à jour du microprogramme</li> <li>• Collecte des données de maintenance</li> <li>• Notification de problèmes automatique (par exemple, l'Appel Lenovo et la fonction de mise à jour Lenovo)</li> <li>• Récupération des données relatives à la garantie</li> <li>• Déploiement SE</li> <li>• Mises à jour de pilote de périphériques SE</li> </ul>	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	<p>Réseau de gestion</p> <ul style="list-style-type: none"> <li>• Reconnaissance et gestion</li> <li>• Configuration du serveur</li> <li>• Mises à jour du microprogramme</li> <li>• Collecte des données de maintenance</li> <li>• Notification de problèmes automatique (par exemple, l'Appel Lenovo et la fonction de mise à jour Lenovo)</li> <li>• Récupération des données relatives à la garantie</li> <li>• Déploiement SE</li> <li>• Mises à jour de pilote de périphériques SE</li> </ul>	<p>Réseau de données</p> <ul style="list-style-type: none"> <li>• Aucun</li> </ul>
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	<p>Réseau de gestion</p> <ul style="list-style-type: none"> <li>• Reconnaissance et gestion</li> <li>• Configuration du serveur</li> <li>• Mises à jour du microprogramme</li> <li>• Collecte des données de maintenance</li> <li>• Notification de problèmes automatique (par exemple, l'Appel Lenovo et la fonction de mise à jour Lenovo)</li> <li>• Récupération des données relatives à la garantie</li> </ul>	<p>Réseau de données</p> <ul style="list-style-type: none"> <li>• Déploiement SE</li> <li>• Mises à jour de pilote de périphériques SE</li> </ul>

Tableau 3. 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 sans prise en charge pour le déploiement SE et les mises à jour de pilote de périphérique	<p>Réseau de gestion</p> <ul style="list-style-type: none"> <li>• Reconnaissance et gestion</li> <li>• Configuration du serveur</li> <li>• Mises à jour du microprogramme</li> <li>• Collecte des données de maintenance</li> <li>• Notification de problèmes automatique (par exemple, l'Appel Lenovo et la fonction de mise à jour Lenovo)</li> <li>• Récupération des données relatives à la garantie</li> </ul>	<p>Réseau de données</p> <ul style="list-style-type: none"> <li>• Aucun</li> </ul>
Réseau de gestion uniquement (le déploiement SE et les mises à jour de pilote de périphérique ne sont pas pris en charge)	<p>Réseau de gestion</p> <ul style="list-style-type: none"> <li>• Reconnaissance et gestion</li> <li>• Configuration du serveur</li> <li>• Mises à jour du microprogramme</li> <li>• Collecte des données de maintenance</li> <li>• Notification de problèmes automatique (par exemple, l'Appel Lenovo et la fonction de mise à jour Lenovo)</li> <li>• Récupération des données relatives à la garantie</li> </ul>	Aucun

Pour plus d'informations sur les interfaces réseau de XClarity Administrator, voir [Remarques sur le réseau](#).

## Procédure

Pour configurer l'accès réseau, procédez comme suit.

Etape 1. Sur la page Configuration initiale, cliquez sur **Configurer un accès réseau**. La page Éditer l'accès réseau s'affiche.

## Éditer l'accès réseau

Paramètres IP	Paramètres avancés	Paramètres Internet
---------------	--------------------	---------------------

**Paramètres IP**

Si vous utilisez le protocole DHCP et un certificat de sécurité externe, assurez-vous que les baux d'adresses du serveur de gestion sur le serveur DHCP soient permanents, afin d'éviter des problèmes de communication avec les ressources gérées lorsque l'adresse IP du serveur de gestion est modifiée.

Une interface réseau détectée :

Eth0 :  Activé - utilisée pour reconnaître et gérer le matériel, ainsi que pour gérer et déployer les images des sys... ?

	IPv4	IPv6
<b>Eth0:</b>	<p>Utiliser l'adresse IP affectée de manière stati... <span>?</span></p> <p>* Adresse IP : <input type="text" value="10.240.61.98"/></p> <p>Masque de réseau : <input type="text" value="255.255.252.0"/></p>	<p>Utiliser la configuration d'adresse avec état (...)</p> <p>Adresse IP : <input type="text"/></p> <p>Longueur de préfixe : <input type="text" value="64"/></p>
<b>Passerelle par défaut:</b>	<p>Passerelle: <input type="text" value="10.240.60.1"/></p>	<p>Passerelle: <input type="text" value="DHCP"/></p>

Étape 2. 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.

Étape 3. Indiquez 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 IP](#).

- 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 4. **Facultatif :** Configurez les paramètres avancés.

- a. Cliquez sur l'onglet **Routage avancé**.

**Éditer l'accès réseau**

Paramètres de route avancés					
Interface	Type de route	Destination	Masque/longueur de préfixe	Adresse de passerelle	
Eth0	Hôte	IPv4	255.255.255.255		+ X

- 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 5. Si vous le souhaitez, vous pouvez modifier les paramètres DNS et proxy.

- a. Cliquez sur l'onglet **DNS et proxy**.

#### Éditer l'accès réseau

Paramètres IP Paramètres avancés Paramètres Internet

Nom d'hôte et nom de domaine pour dispositif virtuel

Nom d'hôte : idxhwmgr

Nom de domaine : labs.lenovo.com

Serveurs DNS

Mode de fonctionnement DNS: Static

Commande	Adresse du serveur
1	10.240.0.10
2	10.240.0.11

Paramètres Internet

Accès à Internet : Connexion directe Proxy HTTP

- 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**.

Un 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 [Gestion des travaux](#) dans la documentation de XClarity Administrator).

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 6. Cliquez sur **Retour**.

Etape 7. Cliquez sur **Tester la connexion** pour vérifier les paramètres réseau.

---

## Configuration de la date et de l'heure

Vous pouvez définir manuellement la date et l'heure de Lenovo XClarity Administrator, mais une meilleure méthode consiste à configurer un serveur NTP (Network Time Protocol) qui permet de synchroniser les horodatages entre XClarity Administrator et tous les appareils gérés.

### 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

Pour configurer un serveur NTP pour XClarity Administrator, procédez comme suit.

Etape 1. Sur la page Configuration initiale, cliquez sur **Configurer des préférences de date et heure**. La page Éditer la date et l'heure s'affiche.

### Éditer la date et l'heure

La date et l'heure seront synchronisées automatiquement avec le serveur NTP.

Fuseau horaire

UTC -05:00, Heure normale de l'Est Amérique/New\_York

Effectue automatiquement le passage à l'heure d'été (DST).

Éditer les paramètres de l'horloge (format 12 ou 24 heures) :

24 12

Nom d'hôte ou adresse IP du serveur NTP :

us.pool.ntp.org

0.0.0.0

0.0.0.0

0.0.0.0

Authentification NTP v3 :

Requis

Aucun

\*

Clés d'authentification NTP (au moins une d'entre elles doit être renseignée)

Utiliser la clé M-MD5 :

Index de clé M-MD5 :

Clé M-MD5 :

Utiliser la clé SHA1 :

Index de clé SHA1 :

Clé SHA1 :

Etape 2. 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 3. Cliquez sur **Enregistrer**.

---

## Configuration du service et du support

Vous pouvez configurer les paramètres de service et de support technique, y compris les données d'usage, Support Lenovo (Appel vers Lenovo), la fonction de téléchargement Lenovo et la garantie du produit.

### Procédure

Procédez comme suit pour configurer la sécurité.

- Etape 1. Sur la page Configuration initiale, cliquez sur **Configurer les paramètres de service et support**. La page Service et support s'affiche.

## Téléchargement périodique des données

**i Attention** ×

---

Pour terminer le processus de configuration initiale, suivez toutes les étapes de ce panneau et à la fin, cliquez sur "Revenir à la configuration initiale"

Nous aimerions vous demander une faveur. Afin d'améliorer le produit ainsi que votre expérience, nous autoriseriez-vous à collecter des informations sur l'utilisation que vous faites de ce produit ?

### Déclaration de confidentialité de Lenovo

Non, merci

#### Matériel ?

J'accepte d'envoyer régulièrement à Lenovo des données d'inventaire matériel et d'événements système. Lenovo peut utiliser les données pour améliorer les futures expériences du support client (par exemple, pour stocker et déplacer les pièces pertinentes plus près de chez vous).

Pour télécharger un exemple de données, cliquez [ici](#).

#### Utilisation ?

J'accepte d'envoyer régulièrement des données d'utilisation à Lenovo afin de mieux comprendre comment le produit est utilisé. Toutes les données sont anonymes.

Pour télécharger un exemple de données, cliquez [ici](#).

Vous pouvez modifier ces paramètres à tout moment à partir de la page [Service](#) et de la page [d'assistance](#).

Appliquer

Etape 2. Lisez et acceptez le document suivant : [Déclaration de confidentialité de Lenovo](#)

**Remarque :** Vous ne pouvez pas collecter et envoyer des données à Lenovo sans accepter préalablement le document suivant : [Déclaration de confidentialité de Lenovo](#). Si vous choisissez de refuser la déclaration de confidentialité, vous pouvez consulter et accepter la déclaration de confidentialité ultérieurement à partir de la page **Service et support** → **Configuration de l'appel vers Lenovo**.

Etape 3. Si vous le souhaitez, vous pouvez choisir d'autoriser Lenovo XClarity Administrator en vue de collecter des informations sur la manière d'utilisation et matérielles. Cliquez ensuite sur **Appliquer**.

Vous pouvez collecter et envoyer les types de données suivants à Lenovo.

- **Données d'utilisation**

Lorsque vous acceptez d'envoyer des données d'utilisation à Lenovo, les données suivantes sont collectées et envoyées chaque semaine. Ces données *sont anonymes*. Aucune donnée privée (y compris les numéros de série, les UUID, les noms d'hôte, les adresses IP et les noms d'utilisateur) n'est collectée ou envoyée à Lenovo.

- Journal des actions qui ont été effectuées
- Liste des événements qui ont été déclenchés et l'horodatage lors de leur déclenchement
- Liste des événements d'audit qui ont été déclenchés et l'horodatage lors de leur déclenchement
- Liste des travaux qui ont été exécutés, ainsi que les informations de réussite ou d'échec pour chaque travail

- Mesures XClarity Administrator, y compris l'utilisation de la mémoire, l'utilisation du processeur et l'espace disque
- Données d'inventaire limitées sur tous les appareils gérés

- **Données matérielles**

Lorsque vous acceptez d'envoyer des données matérielles à Lenovo, les données suivantes sont régulièrement collectées et envoyées. Ces données *ne sont pas anonymes*. Les données matérielles incluent des attributs, tels que des UUID et des numéros de série. Elles n'incluent pas les adresses IP ou les noms d'hôte.

- **Données matérielles quotidiennes.** Les données suivantes sont incluses dans chaque modification d'inventaire.
  - Événement de changement dans l'inventaire (FQXHMDM0001I)
  - Modifications apportées aux données d'inventaire pour l'appareil associé à cet événement
- **Données matérielles hebdomadaires.** Les données d'inventaire sont incluses pour tous les appareils gérés.

Lorsque des données d'utilisation et matérielles sont envoyées à Lenovo, un événement est enregistré dans le journal d'audit.

Vous pouvez modifier ce paramètre à tout moment et télécharger la dernière archive qui a été collectée et envoyée à Lenovo à l'aide de liens, en cliquant sur **Administration → Service et support**, puis en cliquant sur l'onglet **Téléchargement périodique des données**.

- Etape 4. Vous pouvez si vous le souhaitez cliquer sur **Configuration de l'appel vers Lenovo** pour configurer la notification automatique de problème au support Lenovo (Appel vers Lenovo). Cliquez ensuite sur **Appliquer et activer** pour créer le réexpéditeur de service Appel vers Lenovo par défaut, ou sur **Appliquer uniquement** pour enregistrer les informations de contact.

Pour plus d'informations sur la configuration de la notification de problèmes automatique au Support Lenovo, voir [Configuration de l'appel vers Lenovo](#) dans la documentation en ligne de XClarity Administrator.

- Etape 5. Vous pouvez si vous le souhaitez cliquer sur **Fonction de téléchargement Lenovo** pour configurer la notification automatique de problème à la fonction de téléchargement Lenovo. Cliquez ensuite sur **Appliquer et activer** pour créer le réexpéditeur de service Fonction de téléchargement Lenovo, ou sur **Appliquer uniquement** pour enregistrer les informations des paramètres.

Pour plus d'informations sur la configuration de la notification de problèmes automatique à 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.

- Etape 6. Vous pouvez si vous le souhaitez cliquer sur **Garantie** pour activer les connexions externes qui sont nécessaires pour collecter les informations relatives à la garantie de vos appareils gérés.

Pour plus d'informations sur la consultation de l'état de la garantie (y compris les garanties étendues) des appareils gérés, voir [Affichage des informations relatives à la garantie](#) dans la documentation en ligne de XClarity Administrator.

- Etape 7. De manière facultative, cliquez sur **Service de bulletin Lenovo** pour autoriser Lenovo à envoyer des bulletins de maintenance à XClarity Administrator, puis cliquez sur **Appliquer**.

Pour plus d'informations sur les types de bulletins de maintenance que Lenovo peut envoyer, voir [Obtention de bulletins de Lenovo](#) dans la documentation en ligne de XClarity Administrator.

Etape 8. Indiquez le mot de passe de récupération de service que vous pouvez utiliser pour collecter et télécharger les données et les journaux de maintenance si XClarity Administrator ne répond plus et ne peut pas être récupéré.

Pour plus d'informations sur le mot de passe de récupération de service, voir [Modification du mot de passe de récupération de service](#) dans la documentation en ligne de XClarity Administrator.

Etape 9. Cliquez sur **Revenir à la configuration initiale**.

---

## Configuration de la sécurité

Vous pouvez configurer la sécurité, y compris les groupes de rôles, le serveur d'authentification, les paramètres de sécurité de compte utilisateur, la cryptographie et les certificats.

### Procédure

Procédez comme suit pour configurer la sécurité.

Etape 1. Sur la page Configuration initiale, cliquez sur **Configurer des paramètres de sécurité supplémentaires**. La page Sécurité s'affiche.

Etape 2. Créez des groupes de rôles personnalisés pour gérer l'autorisation et l'accès aux ressources (voir [Création d'un groupe de rôles](#) dans la documentation en ligne de XClarity Administrator).

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

Etape 3. Configuration du serveur d'authentification (voir [Gestion du serveur d'authentification](#)) dans la documentation en ligne de XClarity Administrator.

Le *serveur d'authentification* est un serveur Microsoft Active Directory (LDAP) utilisé pour authentifier les données d'identification utilisateur. XClarity Administrator utilise un seul serveur d'authentification pour la gestion des utilisateurs centrale de tous les appareils gérés (sauf les commutateurs Flex). Lorsqu'un appareil est géré par XClarity Administrator, l'appareil géré et les composants qui sont installés dessus (à l'exception des commutateurs Flex) sont configurés pour utiliser le serveur d'authentification XClarity Administrator. Les comptes utilisateur définis sur le serveur d'authentification sont utilisés pour se connecter à XClarity Administrator, aux modules CMM et au contrôleur de gestion de la carte mère.

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

Etape 4. Configurez les paramètres de sécurité de compte utilisateur, qui contrôlent la complexité de mot de passe, le verrouillage du compte, et le délai d'inactivité de session Web (voir [Modification des paramètres de sécurité d'un compte utilisateur](#) dans la documentation en ligne de XClarity Administrator).

Etape 5. Configurez le paramètre de cryptographie qui définit les modes et protocoles de communication qui contrôlent la façon dont les communications sécurisées sont gérées entre XClarity Administrator et les appareils gérés (voir [Définition du mode de chiffrement et des protocoles de communication](#) dans la documentation en ligne de XClarity Administrator)

Etape 6. Si vous planifiez de gérer des serveurs rack par authentification locale plutôt que par XClarity Administrator authentification gérée, créez une ou plusieurs données d'identification stockées correspondant à des comptes utilisateur actifs sur l'appareil ou dans Active Directory pouvant être utilisés pour vous connecter aux appareils pendant le processus de gestion. Pour plus d'informations sur les données d'identification stockées, voir [Gestion de données d'identification stockées](#) dans la documentation en ligne de XClarity Administrator.

Etape 7. Si vous souhaitez utiliser un certificat de serveur personnalisé à signature externe comprenant vos propres informations ou utilisez un certificat à signature externe, générez et déployez le nouveau certificat avant de commencer à gérer des systèmes. Pour savoir comment générer votre propre certificat de sécurité, voir [Utilisation de certificats de sécurité](#) dans la documentation en ligne de XClarity Administrator.

Etape 8. Dans le menu vertical sur la page Sécurité, cliquez sur **Revenir à la configuration initiale**.

---

## Gestion des appareils

Lenovo XClarity Administrator peut gérer plusieurs types de systèmes, y compris le châssis Flex System, les serveurs rack et au format tour, les commutateurs RackSwitch et les dispositifs de stockage. Vous pouvez facilement détecter et gérer un grand nombre d'appareils présents dans votre environnement en important des informations sur vos appareils à l'aide d'un fichier d'importation en masse.

### Avant de commencer

#### Important :

- Vous pouvez gérer un maximum 300 appareils en même temps. N'incluez pas plus de 300 appareils dans un fichier d'importation en masse.
- Après avoir lancé une opération de gestion d'appareils, attendez que l'intégralité du travail de gestion se termine avant de lancer une autre opération de gestion d'appareils.

Les composants de châssis (tels que les modules CMM, les nœuds de traitement, les commutateurs et les dispositifs de stockage) 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.

Certains ports doivent être disponibles pour communiquer avec les modules CMM dans les contrôleurs de gestion de la carte mère et de châssis dans les serveurs. Vérifiez que ces ports sont disponibles avant de tenter de gérer des systèmes. Pour plus d'informations sur les ports, voir [Disponibilité de port](#).

Vérifiez que le microprogramme minimal requis est installé sur chaque système 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 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](#).

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).

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.

#### Important :

- 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](#).

- Le réacheminement SLP de multidiffusion doit être activé sur chaque dispositif de stockage pour qu'il puisse être reconnu par XClarity Administrator.
- Si vous souhaitez utiliser un certificat de serveur personnalisé à signature externe comprenant vos propres informations ou utilisez un certificat à signature externe, générez et déployez le nouveau certificat avant de commencer à gérer des systèmes. Pour savoir comment générer votre propre certificat de sécurité, voir [Utilisation de certificats de sécurité](#) dans la documentation en ligne de XClarity Administrator.
- 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.
- 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

## À propos de cette tâche

XClarity Administrator peut reconnaître des systèmes dans votre environnement en sondant des dispositifs gérables dans le même sous-réseau IP que XClarity Administrator, en utilisant une adresse IP ou une plage d'adresses IP spécifiée, ou en important des informations à partir d'un tableur.

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 [Gestion des serveurs](#) dans la documentation en ligne de XClarity Administrator).

**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.

Une fois que les systèmes sont gérés par XClarity Administrator, XClarity Administrator interroge régulièrement chaque système géré afin de collecter des informations, telles que l'inventaire, les données techniques essentielles et l'état. Vous pouvez afficher et surveiller chaque système 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).

Un système ne peut être géré que par une seule instance de XClarity Administrator à la fois. La gestion par plusieurs gestionnaires n'est pas prise en charge. Si un système 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 système sur l'instance de XClarity Administrator en cours. Ensuite, vous pouvez gérer le système avec une autre instance de XClarity Administrator. Pour plus d'informations sur l'annulation de la gestion d'un système, voir [Désactivation de la gestion d'un châssis](#), [Annulation de la gestion de serveurs](#), [Annulation de la gestion d'un commutateur RackSwitch](#) et [Annulation de la gestion d'un système de stockage Lenovo Storage](#) dans la documentation en ligne de XClarity Administrator.

**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 système géré (voir [Définition du mode de chiffrement et des protocoles de communication](#) dans la documentation en ligne de XClarity Administrator).

**Remarque** : XClarity Administrator peut être prérempli avec l'inventaire matériel pour un châssis de démonstration (comprenant un module CMM, des nœuds de traitement et des commutateurs) et un serveur de démonstration rack ou au format tour, qui simule le matériel réel. Les dispositifs de démonstration sont renseignés dans les pages de l'interface Web et peuvent être utilisés pour illustrer des opérations de gestion ; toutefois, les opérations de gestion échoueront. Par exemple, vous pouvez créer un modèle de configuration et déployer ce modèle sur un serveur de démonstration, mais le déploiement échouera. Vous pouvez retirer les dispositifs de démonstration en annulant leur gestion (voir [Désactivation de la gestion d'un châssis](#) et [Annulation de la gestion de serveurs](#) dans la documentation en ligne de XClarity Administrator). Une fois les dispositifs de démonstration supprimés, ils ne peuvent plus être gérés.

## Procédure

Pour détecter et gérer vos systèmes dans XClarity Administrator à l'aide d'un fichier d'importation en masse, procédez comme suit.

**Remarque** : Lors de la gestion des commutateurs à l'aide de l'importation en masse, HTTPS est activé sur le commutateur, et les clients NTP sur le commutateur sont configurés pour utiliser les paramètres NTP à partir du serveur de gestion. Pour modifier ces paramètres, vous devez gérer manuellement les commutateurs.

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.

**Remarques :**

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

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 [Reprise de la gestion de châssis avec un module CMM après une défaillance du serveur de gestion](#) et [Récupération de la gestion du serveur au format tour après une défaillance du serveur de gestion](#) dans la documentation en ligne de XClarity Administrator.

3. Cliquez sur **Importer en masse**. L'assistant Importer en masse s'affiche.

Importer en masse



**Importer le fichier de données**

Étape 1 : télécharger le fichier modèle au format [dans Excel](#) ou [dans CSV](#)

Étape 2 : entrer les informations dans le fichier modèle, puis l'enregistrer au format CSV

Étape 3 : télécharger le fichier CSV pour le traitement

template.csv    Parcourir    Télécharger

4. 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.

5. Remplissez la feuille de travail de données dans le modèle de fichier et enregistrez celui-ci au format CSV *délimité par des virgules*.

**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 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 appareils dans le fichier d'importation en masse, complétez les colonnes suivantes.

- (Colonne A à C) Pour la reconnaissance de base, vous devez indiquer le type de dispositif et l'adresse IP en cours ou le numéro de série de l'appareil. Les types suivants sont pris en charge :
  - **filler**. Marques de réservation pour un dispositif non géré. Dans la vue de l'armoire, ce dispositif est affiché sous la forme d'un graphique d'obturateur générique. Consultez la feuille de travail **Readme** dans le modèle Excel pour des types d'obturateur supplémentaires.
  - **flexchassis**. Châssis 10U Flex System :
  - **server**. Serveurs rack et au format tour pris en charge par XClarity Administrator
  - **rack**. Armoires 6U, 12U, 18U, 25U, 37U, 42U, 45U, 46U, 48U, 50U et 52U. Les autres hauteurs d'armoire ne sont pas prises en charge. 52U est utilisé par défaut.
  - **storage**. Dispositifs de stockage
  - **switch**. Commutateurs RackSwitch

**Remarque** : Les nœuds de traitement Flex System, les commutateurs et les dispositifs de stockage sont considérés comme faisant partie du processus de reconnaissance et de gestion du châssis.

- (Colonnes D - H) Si vous choisissez d'utiliser les données d'identification saisies manuellement au lieu des données d'identification stockées (Colonnes Z) ou l'identité (Colonnes AF – AJ), indiquez le nom d'utilisateur et le mot de passe en cours. Les données d'identification entrées manuellement sont utiles si elles sont différentes pour certains périphériques. Si vous ne spécifiez pas les données d'identification pour un ou plusieurs dispositifs dans le fichier d'importation en masse, ce sont les données d'identification globales spécifiées dans la boîte de dialogue Importer en masse qui sont utilisées. Pour plus d'informations sur les utilisateurs entrés manuellement et l'authentification gérée, voir [Gestion des comptes utilisateur](#) dans la documentation en ligne de XClarity Administrator.

#### Remarques :

- Pour utiliser les données d'identification saisies manuellement, vous devez sélectionner l'authentification gérée XClarity Administrator
- Certaines zones ne s'appliquent pas à certains dispositifs.
- (Pour les châssis) Si vous choisissez l'authentification gérée (dans la colonne AA ou dans la boîte de dialogue Importer en masse), vous devez spécifier le mot de passe `RECOVERY_ID` dans la colonne G du fichier d'importation en masse, ou dans la boîte de dialogue Importer en masse. Si vous choisissez l'authentification locale, le mot de passe de récupération n'est pas autorisé. Ne spécifiez pas le mot de passe de récupération dans la colonne G du fichier d'importation en masse, ou dans la boîte de dialogue Importer en masse.
- (Pour les serveurs rack) Si vous choisissez l'authentification gérée (dans la colonne AA ou dans la boîte de dialogue Importer en masse), vous pouvez également spécifier un mot de passe de récupération dans la colonne G du fichier d'importation en masse, ou dans la boîte de dialogue Importer en masse. Si vous choisissez l'authentification locale, le mot de passe de récupération n'est pas autorisé. Ne spécifiez pas le mot de passe de récupération dans la colonne G du fichier d'importation en masse, ou dans la boîte de dialogue Importer en masse.
- (Pour les commutateurs d'armoire) Les appareils RackSwitch prennent en charge uniquement les données d'identification stockées (dans la colonne Z) pour l'authentification auprès des commutateurs. Les données d'identification utilisateur manuelles ne sont pas prises en charge.

- (Colonnes I - U) Vous pouvez éventuellement fournir des informations supplémentaires si vous voulez appliquer des modifications au dispositif lorsque la gestion réussit.

**Remarque :** Certaines zones ne s'appliquent pas à certains dispositifs. Ces zones ne s'appliquent pas aux commutateurs RackSwitch.

- (Colonnes V - Z) Vous pouvez éventuellement fournir des informations pour la création et l'affectation de l'armoire, y compris le nom de l'armoire, emplacement, `sallelowestRackUnit` et la hauteur.

**Remarques :**

- Lors de la création d'une armoire, vous devez indiquer le nom et 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. Les autres hauteurs d'armoire ne sont pas prises en charge.
- Lors de la création d'un obturateur générique, vous devez indiquer le nom de l'armoire et la hauteur de l'obturateur. Les hauteurs d'obturateur suivantes sont prises en charge : 1U, 2U et 4U.
- Lors de la création d'un obturateur spécifique, la hauteur de l'obturateur est ignorée. XClarity Administrator connaît la hauteur de chaque obturateur spécifique. Consultez le modèle de tableur pour connaître les types et les hauteurs d'obturateur.
- Lors de l'affectation d'un appareil à l'armoire, la hauteur de l'appareil est ignorée. La hauteur de l'appareil est extraie de l'inventaire des appareils.
- (Colonne AA) Si la gestion n'a pas aboutie en raison d'une des conditions d'erreur suivantes, répétez cette procédure en utilisant l'option de gestion forcée.
  - 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 le XClarity Administrator défaillant, vous pouvez gérer à nouveau le périphérique à l'aide du compte et du mot de passe `RECOVERY_ID` (le cas échéant) et de l'option de gestion forcée.

- 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.

Les appareils peuvent être gérés 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 un XClarity Administrator, et que vous souhaitez le gérer avec un autre XClarity Administrator, vous devez d'abord annuler la gestion depuis le XClarity Administrator d'origine, puis le gérer avec le nouveau XClarity Administrator.

**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 gestion forcée.

- (Colonne AB) Vous pouvez également choisir d'utiliser les données d'identification stockées à la place de données d'identification entrées manuellement (colonnes D - H) ou l'identité (Colonnes AF – AJ) spécifiez un ID d'identification stocké. Vous trouverez l'ID d'identification stocké dans la page des données d'identification stockées en cliquant sur **Administration** → **Sécurité** dans le menu XClarity Administrator, puis en cliquant sur **Données d'identification stockées** dans le volet de navigation gauche. Pour plus d'informations sur les données d'identification normales et l'authentification locale, voir [Gestion de données d'identification stockées](#) dans la documentation en ligne de XClarity Administrator.

**Remarques :**



- Les appareils RackSwitch prennent en charge uniquement les données d'identification stockées pour l'authentification. Les données d'identification utilisateur manuelles (dans la colonne D) ne sont pas prises en charge.
- Si vous gérez un appareil en utilisant les données d'identification stockées et activez l'authentification gérée, vous ne pouvez pas éditer ces données d'identification.
- (Colonne AC) Pour les châssis et les serveurs rack, si vous avez choisi l'authentification gérée, vous devez spécifier le mot de passe RECOVERY\_ID, dans la colonne G du fichier d'importation en masse, ou dans la boîte de dialogue Importer en masse. Si vous choisissez l'authentification locale, le mot de passe de récupération n'est pas autorisé. Ne spécifiez pas le mot de passe de récupération dans la colonne G du fichier d'importation en masse, ou dans la boîte de dialogue Importer en masse.
- (Colonne AD) Pour les serveurs rack, vous pouvez également choisir d'utiliser l'authentification locale à la place de l'authentification gérée de XClarity Administrator en indiquant FALSE dans cette colonne. Pour plus d'informations sur l'authentification gérée et locale, voir [Gestion du serveur d'authentification](#) dans la documentation en ligne de XClarity Administrator.
- (Colonne AE) Vous pouvez éventuellement spécifier une liste de groupes de rôles autorisés à afficher et à gérer l'appareil. Vous pouvez indiquer seulement les groupes de rôles auxquels appartient l'utilisateur en cours.

**Remarque :** Si vous ajoutez des appareils à un châssis géré, les nouveaux appareils appartiennent aux mêmes groupes de rôles que le châssis.

- (Colonne AF – AJ) Si vous choisissez d'utiliser un système de gestion d'identité au lieu d'entrer manuellement les données d'identification (Colonnes D – H) ou les données d'identification stockées (Colonnes AB), indiquez l'adresse IP ou le nom d'hôte du serveur géré, le nom d'utilisateur, et éventuellement l'ID de l'application, du coffre-fort et du 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.

La figure suivante illustre un exemple de fichier d'importation en masse :

Required fields (Type + SN or IP)			Optional fields																
Type	Serial Number	Current IP	Current username	Current password	New password	Recovery password	Switch enable password	New IPv4	IPv4 subnet mask	IPv4 default gateway	IPv4 DNS1	IPv4 DNS2	New IPv6	IPv6 prefix	IPv6 gateway	IPv6 DNS1	IPv6 DNS2	Domain	
server		10.1.0.198																	
server	P67X30EL																		
flexchassis		10.1.0.213	USERID	passw0rdx	Pa55word@	abcd1234													
flexchassis	Z3499DD				Pa55word@	abcd1234		9.27.20.51	255.255.255.0	9.27.20.1	9.0.148.50	9.0.146.50							ebg.lenovo.com
server	35T88XP													2002:939	2002:939	2002:939	2002:939	2002:939	ebg.lenovo.com
server		10.1.0.214						10.1.2.213	255.255.255.0	10.1.2.1	9.0.148.50	9.0.146.50							ebg.lenovo.com
rack																			
rack																			
filler																			
filler																			
filler																			

IPv6 DNS2	Domain	Host name	User-defined name	Rack name	Location	Room	Lowest rack unit	Height	Force	Stored credentials ID	Stored credentials ID for RECOVERY_ID	Managed authentication	Role Groups	IdentityManagements systemEnabled	IMS type	IMS AppID	Folder	Safe
			chassis03	SH3G05A34				25	TRUE						CyberArk	LXCA		Test
	ebg.lenovo.com	chassis01	chassis01	SH3G05A34				5										
2002:9	ebg.lenovo.com	host4	c02node01	SH3G05B12				38		2	3	FALSE						
	ebg.lenovo.com	host5	web02	SH3G05B12				10										
			SG2R01A01					37										
			SH3G05A34					46										
			APC UPS	SH3G05A34				1	4									
			PC switch	SH3G05A34				40	2									
			KVM switch	SH3G05B12				22	1									

- 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.
- Cliquez sur **Télécharger** pour téléchargement et valider le fichier.
- Cliquez sur **Suivant** pour afficher la page de récapitulatif des entrées avec une liste des appareils à gérer.

## Importer en masse

### Récapitulatif d'entrée

La liste des appareils qui seront gérés est affichée. Vous pouvez, si vous le souhaitez, passer en revue les données avant de terminer l'Assistant. Vous pouvez toujours revenir en arrière et télécharger de nouveau un fichier correct si nécessaire.

Afficher uniquement les lignes d'éventuels problèmes

4 Nombre total d'appareils qui seront gérés : 1 Châssis, 1 Commutateurs, 2 Serveurs, 0 Stockage

CSV Row	Name	Current IP	Credentials	Type
2	Server_1	192.0.2.0	Entrée obligatoire	server
3	Chassis_1		Entrée obligatoire	flexchassis
4	Rack_2		Entrée obligatoire	rack
5	Filler		Entrée obligatoire	filler

- Passez en revue le récapitulatif des appareils que vous souhaitez gérer.

Sélectionnez **Afficher uniquement les lignes avec des problèmes potentiels** pour afficher la ligne avec des données incomplètes. Corrigez les problèmes dans le fichier d'importation en masse, puis cliquez sur **Retour** pour télécharger le fichier CSV corrigé.

### Remarques :

- Si les données requises ne sont pas fournies dans le fichier d'importation en masse, les appareils associés ne sont pas gérés.



- La page Récapitulatif des entrées indique les lignes qui ne comportent pas de données d'identification. Si vous ne spécifiez pas les données d'identification dans le fichier d'importation en masse, ce sont les données d'identification globales spécifiées dans l'assistant Importer en masse qui sont utilisées.

10. Cliquez sur **Suivant** pour afficher la page des données d'identification de l'appareil.

## Importer en masse

### Données d'identification d'appareil

Un ou plusieurs ensembles de données d'identification sont nécessaires pour pouvoir continuer à gérer ces appareils. Entrez ces données d'identification ici par type de dispositif. Une fois terminé, appuyez sur Gérer pour lancer le processus de gestion.

🔧 Châssis (1)
🔧 Serveur (2)
🔧 Commutateur (1)
🔧 Stockage
🔧 Reprise (3)

**Châssis**

Choisir d'utiliser l'authentification gérée ou non

Authentification gérée

Choisir le type de données d'identification

Utiliser des données d'identification saisies manuellement

Utiliser des données d'identification stockées

**Module CMM (Chassis Management Module)**

Données d'identification actuelles (globales)

nom d'utilisateur

mot de passe

Nouvelles données d'identification (globales)  
*(Remarque : utilisé uniquement si les données d'identification actuelles ont expirées)*

nouveau mot de passe

confirmation du mot de passe

Forcer la gestion, même si le système est géré par une autre instance de Lenovo® XClarity Administrator ou celle-ci  
Lorsque la gestion est forcée, la gestion Recovery-id doit être utilisée.

Appareils qui utiliseront ces données d'identification :

Chassis\_1

11. **Facultatif** : 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.

Si vous choisissez d'utiliser les données d'identification globales, les données d'identification pour un type de dispositif spécifique doivent être identiques pour tous les dispositifs du même type car les données d'identification ne sont pas entrées dans le fichier d'importation en masse. Par exemple, les données d'identification du module CMM doivent être identiques pour tous les châssis, et les données d'identification de gestion du stockage doivent être identiques pour tous les dispositifs de stockage. Si les données d'identification ne sont pas identiques, vous devez entrer les données d'identification dans le fichier d'importation en masse.

- **Châssis**. Spécifiez le mode d'authentification et le type de données d'identification. Indiquez les données d'identification actuelles pour la connexion à tous les châssis qui sont définis dans le fichier d'importation en masse. Indiquez le nouveau mot de passe à utiliser si les données d'identification CMM actuelles ont expiré.

Si vous forcez la gestion d'un châssis, spécifiez le compte RECOVERY\_ID et le mot de passe pour les données d'identification de l'appareil.

- **Serveurs.** Spécifiez le mode d'authentification et le type de données d'identification. Indiquez les données d'identification actuelles pour la connexion à tous les serveurs rack et au format tour qui sont définis dans le fichier d'importation en masse. Indiquez le nouveau mot de passe à utiliser si les données d'identification actuelles du contrôleur de gestion de la carte mère ont expiré.

Si vous forcez la gestion d'un serveur, spécifiez le compte RECOVERY\_ID et le mot de passe pour les données d'identification de l'appareil.

- **Commutateurs.** Indiquez les données d'identification stockées pour la connexion à tous les commutateurs RackSwitch qui sont définis dans le fichier d'importation en masse. S'il est défini, indiquez également le mot de passe « enable » qui est utilisé pour entrer en mode Exec Privileged sur le commutateur.
- **Stockage.** Indiquez les données d'identification actuelles pour la connexion à tous les dispositifs de stockage qui sont définis dans le fichier d'importation en masse.
- **Récupération.** Indiquez le mot de passe de récupération pour vous connecter à tous les serveurs et châssis qui sont définis dans le fichier d'importation en masse.

Vous pouvez choisir d'utiliser un compte utilisateur local ou des données d'identification de récupération stockées. Dans les deux cas, le nom d'utilisateur est toujours RECOVERY\_ID.

Lorsqu'un mot de passe est spécifié, le compte RECOVERY\_ID est créé sur l'appareil et tous les comptes utilisateur locaux sont désactivés.

- Pour le châssis, le mot de passe de récupération est requis.
- Pour les serveurs, 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.
- 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.

Les informations que vous spécifiez dans le fichier d'importation en masse remplacent des informations similaires que vous indiquez dans la page des données d'identification de l'appareil.

Vous pouvez éventuellement choisir de forcer la gestion de chaque type d'appareil si :

- Les dispositifs sont actuellement gérés par un autre système de gestion, comme une autre instance XClarity Administrator ou IBM Flex System Manager.
- XClarity Administrator est mis hors tension, mais la gestion des appareils n'a pas été annulée avant l'arrêt.
- La gestion des dispositifs n'a pas été annulée correctement et l'abonnement CIM n'a pas été effacé.

**Remarque :** Si le dispositif est géré par une autre instance XClarity Administrator, le dispositif semble être géré par l'instance initiale pendant un certain temps, une fois la gestion forcée effectuée. Vous pouvez annuler la gestion du dispositif afin de le retirer de l'instance XClarity Administrator initiale.

12. 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](#) dans la documentation en ligne XClarity Administrator.

Si XClarity Administrator ne peut pas se connecter à un dispositif utilisant les données d'identification spécifiées dans le fichier d'importation en masse ou les données d'identification globales spécifiées dans la boîte de dialogue, la gestion de ce dispositif échoue et XClarity Administrator passe au prochain dispositif dans le fichier d'importation en masse.

**Remarques** : 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 gérés 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.

13. Si le fichier d'importation en masse comprend un nouveau châssis, validez et modifiez 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 de serveurs à l'aide de XClarity Administrator](#) dans la documentation en ligne de XClarity Administrator.

## Après avoir terminé

Après avoir géré vos systèmes, vous pouvez effectuer les actions suivantes :

- Détecter et gérer les systèmes supplémentaires (voir [Gestion des châssis](#), [Gestion des armoires](#), [Gestion des serveurs](#), [Gestion des dispositifs de stockage](#) et [Gestion des commutateurs](#) dans la Lenovo XClarity Administrator documentation en ligne).
- Configurer les informations système, le stockage local, les cartes d'E-S, les paramètres d'amorçage et les paramètres de microprogramme en créant et en déployant des modèles de serveur (voir [Configuration de serveurs à l'aide de XClarity Administrator](#) dans la documentation en ligne de Lenovo XClarity Administrator).
- Déployer les images du système d'exploitation sur les serveurs qui n'ont pas déjà de système d'exploitation (voir [Déploiement d'une image du système d'exploitation](#) dans la documentation en ligne de XClarity Administrator).
- 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](#) dans la documentation en ligne de XClarity Administrator).
- Ajouter les systèmes récemment gérés dans l'armoire appropriée pour refléter l'environnement physique (voir [Gestion des armoires](#) dans la documentation en ligne de XClarity Administrator).
- Surveiller l'état et les détails du matériel (voir [Affichage de l'état d'un serveur géré](#)) dans la documentation en ligne de XClarity Administrator.

- Surveiller les événements et les alertes (voir [Utilisation des événements](#) et [Utilisation des alertes](#) dans la documentation en ligne de XClarity Administrator).
- 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 .

---

## Chapitre 5. Inscription de XClarity Administrator

En inscrivant votre instance de Lenovo XClarity Administrator, vous pouvez utiliser les fonctionnalités de base, sans recevoir des avertissements de manière régulière concernant l'expiration de la période d'essai ou des licences non conformes. Une fois l'inscription terminée, l'avertissement concernant la non-conformité des licences ne s'affiche plus. Toutefois, les fonctionnalités nécessitant une licence demeurent désactivées jusqu'à l'achat et l'installation des licences sur la base du nombre d'appareils gérés.

### À propos de cette tâche

L'inscription de votre instance XClarity Administrator ne nécessite aucun partage de vos coordonnées. Lenovo ne partage pas les informations fournies avec d'autres entités externes.

Si vous avez déjà installé des licences pour des fonctions avancées, vous n'avez pas besoin d'inscrire votre instance XClarity Administrator. Pour plus d'informations sur les licences et les fonctions avancées, voir [Installation de la licence d'activation de l'ensemble des fonctionnalités](#).

### Procédure

Pour inscrire XClarity Administrator, procédez comme suit.

- Si XClarity Administrator est connecté à Internet
  1. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Administration → Inscription** pour afficher la page Inscription.
  2. Cliquez sur **Inscrire** pour inscrire une nouvelle instance de XClarity Administrator.
  3. Renseignez le nom de l'entreprise, le nombre d'appareils devant être gérés par XClarity Administrator, puis le pays dans lequel XClarity Administrator se trouve.
  4. Cliquez sur **Soumettre**.
- Si XClarity Administrator n'est pas connecté à Internet
  1. Inscrivez XClarity Administrator.
    - a. Dans un navigateur Web, ouvrez le [Portail Web d'inscription Lenovo XClarity](#).
    - b. Renseignez le nom de l'entreprise, le nombre d'appareils devant être gérés par XClarity Administrator, puis le pays dans lequel XClarity Administrator se trouve.
    - c. Cliquez sur **Soumettre** pour recevoir un jeton d'inscription.
  2. Dans la barre de menus de Lenovo XClarity Administrator, cliquez sur **Administration → Inscription** pour afficher la page Inscription.
  3. Cliquez sur **Importer** pour importer le jeton d'inscription.
  4. Saisissez le jeton d'inscription reçu lors de l'étape 1.
  5. Cliquez sur **Soumettre**.



---

## Chapitre 6. Installation de la licence d'activation de l'ensemble des fonctionnalités

À l'issue de l'évaluation gratuite de 90 jours, vous devez acheter et installer les licences Lenovo XClarity Pro pour tous les appareils gérés prenant en charge des fonctions avancées pour continuer à utiliser un déploiement de système d'exploitation et les fonctionnalités de configuration de l'appareil dans Lenovo XClarity Administrator. Vous devez disposer de licences Lenovo XClarity Pro pour *tous* les appareils gérés afin de bénéficier du service et du support XClarity Administrator.

**En savoir plus :**  [XClarity Administrator : installation de la licence](#)

### Avant de commencer

Consultez les remarques relatives aux licences suivantes.

- Une licence *n'est pas* liée à un appareil spécifique.
- Une licence de châssis fournit des licences pour 14 appareils.
- Pour les serveurs complexes évolutifs System x3850 X6 (6241), chaque serveur a besoin d'une licence distincte, quelle que soit la partition.
- Pour les serveurs complexes évolutifs System x3950 X6 (6241), s'ils ne sont pas partitionnés, chaque serveur a besoin d'une licence séparée. S'ils sont partitionnés, chaque partition a besoin d'une licence distincte.
- Les appareils ci-après *ne prennent pas en charge* les fonctions avancées et, par conséquent, *ne nécessitent pas* de licences pour ces fonctions ; toutefois, une licence doit être achetée pour chacun de ces appareils pour obtenir le service et le support XClarity Administrator.
  - Serveurs ThinkServer
  - Serveurs System x M4
  - Serveurs System x X5
  - Serveurs System x3850 X6 et x3950 X6 (3837)
  - Dispositifs de stockage
  - Commutateurs

Vous devez disposer de droits **lxc-supervisor** ou **lxc-security-admin** pour installer les licences.

### À propos de cette tâche

XClarity Administrator prend en charge la licence suivante.

- **Lenovo XClarity Pro.** Chaque licence fournit les droits suivants pour un seul appareil.
  - Service et support pour Lenovo XClarity Integrator
  - Service et support pour XClarity Administrator
  - Fonctions avancées dans XClarity Administrator :
    - Configuration des serveurs à l'aide de modèles de configuration
    - Déploiement des systèmes d'exploitation
    - Signalement de problèmes liés à XClarity Administrator à l'aide de l'appel vers Lenovo (l'appel vers Lenovo pour les alertes matérielles n'est pas affecté).

La période d'activation de la licence démarre lorsque la licence est achetée et que le code d'autorisation est créé.

La conformité de licence est déterminée en fonction du nombre d'appareils gérés qui prennent en charge les fonctions avancées. Le nombre d'appareils gérés ne doit pas dépasser le nombre total de licences de toutes les clés de licences actives. Si XClarity Administrator n'est pas conforme aux licences installées (par exemple, si des licences expirent ou si la gestion d'appareils supplémentaires dépasse le nombre total de licences actives), vous disposez d'un délai autorisé de 90 jours pour installer des licences appropriées. Chaque fois que XClarity Administrator devient non compatible, le délai autorisé se réinitialise à 90 jours. Si la période de grâce (y compris l'essai gratuit) se termine avant que les licences ne soient conformes, les fonctions avancées sont désactivées pour tous les appareils.


Par exemple, si vous gérez un serveur ThinkSystem 100 supplémentaire et 20 commutateurs rack dans une instance XClarity Administrator existante, vous avez 90 jours pour acheter et installer 100 licences supplémentaires avant que les fonctions avancées ne soient désactivées dans l'interface utilisateur (pour tous les appareils). Il n'est pas nécessaire que les 20 commutateurs rack disposent d'une licence pour utiliser les fonctions avancées. Toutefois, celles-ci sont nécessaires si vous souhaitez bénéficier du service et du support. Si des fonctions avancées sont désactivées, celles-ci sont réactivées une fois que suffisamment de licences auront été activées pour être en conformité.

Si vous utilisez une licence d'évaluation gratuite ou que vous disposez d'un délai autorisé pour devenir conforme et que vous effectuez une mise à niveau vers une version ultérieure de XClarity Administrator, la licence d'évaluation ou le délai autorisé se réinitialise à 90 jours.

#### Remarques :

- La configuration du serveur et les fonctions de déploiement du système d'exploitation sont désactivées à l'expiration du délai autorisé.
- La fonction Appel vers Lenovo concernant les problèmes de XClarity Administrator (fonction logicielle Appel vers Lenovo) est désactivée lorsque les licences ne sont pas conformes. Aucun délai autorisé n'est disponible pour cette fonctionnalité. Toutefois, la fonctionnalité Appel vers Lenovo pour les alertes matérielles n'est pas affectée.

Si les licences sont déjà installées, aucune nouvelle licence *n'est* requise lors de la mise à niveau vers une nouvelle édition de XClarity Administrator.

Vous pouvez déterminer l'état de la licence, y compris le nombre de jours restants dans la période d'évaluation, en cliquant sur le menu d'action utilisateur (  ) dans la barre de titre de XClarity Administrator, puis en cliquant sur **À propos de**.

#### Obtenir de l'aide

- Si vous rencontrez des problèmes et vous êtes passé par un partenaire commercial, contactez ce dernier afin de vérifier la transaction et l'autorisation.
- Si vous n'avez pas reçu votre preuve d'achat électronique, des codes d'autorisation ou des clés d'activation, ou s'ils ont été envoyés à une personne incorrecte, contactez l'un des représentants régionaux, selon votre région.
  - [ESDNA@lenovo.com](mailto:ESDNA@lenovo.com) (Pays d'Amérique du Nord)
  - [ESDAP@lenovo.com](mailto:ESDAP@lenovo.com) (pays d'Asie-Pacifique)
  - [ESDEMEA@lenovo.com](mailto:ESDEMEA@lenovo.com) (Pays d'Europe/Moyen-Orient/Afrique)
  - [ESDLA@lenovo.com](mailto:ESDLA@lenovo.com) (Pays d'Amérique Latine)
  - [ESDChina@Lenovo.com](mailto:ESDChina@Lenovo.com) (Chine)
- Si des informations concernant l'autorisation ne sont pas correctes, contactez le support Lenovo à l'adresse [SW\\_override@lenovo.com](mailto:SW_override@lenovo.com) et incluez les informations suivantes :
  - Numéro de commande
  - Vos informations de contact, y compris l'adresse e-mail.
  - Votre adresse physique
  - Modifications que vous souhaitez effectuer



- Si vous avez des problèmes ou des questions sur le téléchargement de la licence, contactez le support Lenovo à l'adresse [-eSupport\\_-\\_Ops@lenovo.com](mailto:-eSupport_-_Ops@lenovo.com).

---

## Installation de licences d'activation de l'ensemble des fonctionnalités à l'aide de l'interface Web XClarity Administrator

Si XClarity Administrator dispose d'un accès Internet, vous pouvez utiliser l'interface Web XClarity Administrator pour utiliser et récupérer des licences d'autorisation existantes, puis importer et installer les licences utilisées.

### Avant de commencer

Contactez votre représentant Lenovo ou partenaire commercial agréé pour obtenir des licences Lenovo XClarity Pro selon les fonctions que vous souhaitez activer et le nombre d'appareils que vous souhaitez gérer. Après avoir acheté des licences, vous recevrez un code d'autorisation dans un e-mail contenant votre *preuve d'achat électronique*. Le code d'autorisation est une chaîne alphanumérique de 22 caractères, dont vous avez besoin pour utiliser et installer les licences. Si vous ne recevez pas d'e-mail et que vous avez acheté les licences via un partenaire commercial, contactez votre partenaire commercial pour lui demander le code d'autorisation.

Vous pouvez également extraire vos codes d'autorisation du [Portail Web Features on Demand](#) en cliquant sur **Obtention d'un code d'autorisation**.

### Procédure

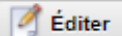
Pour installer les licences Lenovo XClarity Pro dans le serveur de gestion, procédez comme suit.

- **Utiliser et installer toutes ou une partie des licences restantes depuis un seul code d'autorisation**








Il est possible d'utiliser toutes ou une partie des licences disponibles depuis un seul code d'autorisation, et ce, afin de créer une clé d'activation de licence, c'est-à-dire un fichier qui contient chaque information au sujet d'une licence utilisée. Vous pouvez ensuite installer les licences utilisées à l'aide de ce fichier de clé d'activation de licence.

1. Dans la barre de menu de XClarity Administrator, cliquez sur **Administration** → **Licences** pour afficher la page Gestion de licences.


## Gestion des licences

La période d'avertissement est de : 90 jours. 

Clés actives : utilisation de 213 sur 1401 autorisations actives, 75 dont l'expiration a lieu bientôt

   |   |  |  | Toutes les actions ▾ |

<input type="checkbox"/>	Description de la clé de licence	Nombre de licences	Date de début	Date d'expiration	État
<input type="checkbox"/>	XClarity Pro	100	01/05/2022	12/31/2022	 Valide
<input type="checkbox"/>	XClarity Pro	126	01/05/2022	12/30/2023	 Valide
<input type="checkbox"/>	XClarity Pro	1100	01/05/2022	12/31/2022	 Valide
<input type="checkbox"/>	XClarity Pro	75	01/05/2022	01/31/2022	 Expire bientôt : 23 jours restants

2. Cliquez sur l'icône **Demander une clé d'activation** () pour afficher la boîte de dialogue Demander une clé d'activation.
3. Cliquez sur **Code d'autorisation unique**.
4. Saisissez le code d'autorisation composé de 22 caractères, puis cliquez sur **Rechercher** pour récupérer les informations sur les licences achetées pour le code d'autorisation indiqué depuis le site Web Features on Demand.

Si le code d'autorisation reçu n'est pas accepté, contactez le support Lenovo.

5. Saisissez votre numéro de client Lenovo composé de 10 numéros dans le champ **Numéro de client Lenovo**.
6. Entrez le nombre de licences que vous souhaitez obtenir dans le champ **Obtenir la quantité**, puis cliquez sur **Continuer**.

Pour utiliser toutes les licences disponibles dans le code d'autorisation, faites correspondre le nombre figurant dans le champ **Licences disponibles**.

Si vous utilisez un sous-ensemble de licences disponibles, vous pouvez utiliser les licences restantes ultérieurement, à l'aide du même code d'autorisation.


**Astuce** : chaque XClarity Administrator prend en charge jusqu'à 1 000 appareils gérés. Par conséquent, une seule clé d'activation de licence que vous pouvez installer dans une instance XClarity Administrator ne peut pas comporter plus de 1 000 licences.

7. Si besoin, passez en revue les informations de contact et procédez à des modifications.
8. Cliquez sur **Soumettre une demande** pour utiliser les licences et créer une clé d'activation de licence.
9. Sélectionnez la clé d'activation de licence qui contient les licences à installer.
10. Cliquez sur **Installer** pour installer les licences dans le serveur de gestion.
11. Cliquez sur **Fermer**.

- **Utiliser et installer toutes les licences restantes depuis plusieurs codes d'autorisation**


Il est possible d'utiliser toutes les licences restantes pour plusieurs codes d'autorisation. Une clé d'activation de licence est créée pour chaque code d'autorisation. Vous pouvez ensuite installer les

licences utilisées à l'aide des fichiers de clé d'activation de licence. Les codes d'autorisation doivent être fournis dans un fichier au format CSV, à l'aide du modèle fourni.

1. Dans la barre de menu de XClarity Administrator, cliquez sur **Administration** → **Licences** pour afficher la page Gestion de licences.
2. Cliquez sur l'icône **Demander une clé d'activation** () pour afficher la boîte de dialogue Demander une clé d'activation.
3. Cliquez sur **Plusieurs codes d'autorisation**.
4. Cliquez sur le lien **Télécharger un modèle** pour ouvrir un fichier Excel. Ajoutez chaque code d'autorisation au fichier, puis enregistrez-le au format CSV sur votre système local.
5. Cliquez sur **Parcourir** pour trouver et sélectionner le fichier CSV du code d'autorisation. Ensuite, cliquez sur **Rechercher** pour trouver des informations au sujet du code d'autorisation sur le site Web du support Lenovo.
6. Passez en revue les informations au sujet de la licence achetée et les clés d'activation de licence disponibles associées à chaque code d'autorisation.
7. Saisissez votre numéro de client Lenovo composé de 10 numéros dans le champ **Numéro de client Lenovo**.
8. Si besoin, passez en revue les informations de contact et procédez à des modifications. Cliquez ensuite sur **Continuer**.
9. Sélectionnez **Oui, je souhaite utiliser tous les codes d'autorisation valides**, puis cliquez sur **Soumettre une demande** pour générer les clés d'activation de licence.
10. Sélectionnez les clés d'activation de licence à installer.
11. Cliquez sur **Installer** pour installer les clés d'activation de licence dans le serveur de gestion.
12. Cliquez sur **Fermer**.


- **Récupérer et installer les licences utilisées**

Il est possible de télécharger des clés d'activation de licence vers le système local depuis une instance XClarity Administrator qui a accès à [Portail Web Features on Demand](#), puis d'importer et d'installer ces clés d'activation de licence vers une autre instance XClarity Administrator. Cela est utile lorsque vous souhaitez installer des licences sur une instance XClarity Administrator qui ne dispose pas d'un accès Internet ou lorsque vous avez réinstallé XClarity Administrator et que vous devez restaurer les licences installées.


1. Dans la barre de menu de XClarity Administrator, cliquez sur **Administration** → **Licences** pour afficher la page Gestion de licences.
2. Cliquez sur l'icône **Consultation de l'historique** () pour afficher la boîte de dialogue Consultation de l'historique.
3. Saisissez votre numéro de client Lenovo ou le code d'autorisation composé de 22 caractères.
4. Cliquez sur **Rechercher** pour extraire des informations sur les licences disponibles et utilisées.  
Si le code d'autorisation reçu n'est pas accepté, contactez le support Lenovo.
5. Sélectionnez les fichiers de clé de licence à installer.
6. Cliquez sur **Installer** pour installer les clés d'activation de licence dans XClarity Administrator.
7. Cliquez sur **Fermer**.

- **Importer et installer des licences utilisées sur une autre instance XClarity Administrator**

Si vous avez utilisé des licences à l'aide d'une instance XClarity Administrator et que vous souhaitez installer ces licences sur une autre instance XClarity Administrator, ou si une erreur survient et que vous devez restaurer les licences installées, il est possible d'importer le fichier de clé de licence depuis le système local vers l'autre instance XClarity Administrator.

1. Depuis une instance XClarity Administrator disposant d'un accès à [Portail Web Features on Demand](#), récupérez les clés d'activation de licence de [Portail Web Features on Demand](#), puis enregistrez les clés d'activation de licence en tant que fichier sur votre système local.
  - a. Dans la barre de menu de XClarity Administrator, cliquez sur **Administration** → **Licences** pour afficher la page Gestion de licences.
  - b. Cliquez sur l'icône **Consultation de l'historique**  pour afficher la boîte de dialogue Consultation de l'historique.
  - c. Saisissez le code d'autorisation composé de 22 caractères.
  - d. Cliquez sur **Rechercher** pour récupérer des informations au sujet des licences disponibles et utilisées pour ce code d'autorisation.

Si le code d'autorisation reçu n'est pas accepté, contactez le support Lenovo.


- e. Sélectionnez les fichiers de clé d'activation de licence à installer.
  - f. Cliquez sur **Télécharger** pour enregistrer les fichiers de clé de licence sur le système local.
2. Depuis l'instance XClarity Administrator sur laquelle vous souhaitez installer les clés d'activation de licence :
    - a. Dans la barre de menu de XClarity Administrator, cliquez sur **Administration** → **Licences** pour afficher la page Gestion de licences.
    - b. Cliquez sur l'icône **Importer et appliquer**  pour importer et installer les licences.
    - c. Cliquez sur **Parcourir** pour sélectionner les fichiers de clé d'activation de licence pour les licences que vous souhaitez installer.

Pour importer plusieurs clés d'activation de licence, compressez les fichiers .KEY dans un fichier ZIP, puis sélectionnez-le pour l'importation.
    - d. Cliquez sur **Accepter la licence** pour importer et appliquer les licences.


Une fois l'installation terminée, les clés d'activation de licence sont répertoriées dans le tableau contenant le nombre de licences installées et la période d'activation (dates de début et de fin).

## Après avoir terminé

Sur la page Licences, vous pouvez effectuer les actions suivantes.

- Téléchargez une ou plusieurs clés d'activation de licence spécifiques sur le système local en cliquant sur l'icône **Exporter** .

**Remarque** : Lorsque vous exportez plusieurs clés d'activation de licence, les fichiers sont téléchargés sous la forme d'un fichier ZIP unique.

- Supprimez une clé d'activation de licence spécifique en cliquant sur l'icône **Supprimer** .
- Configurez la période d'avertissement de licence en cliquant sur le bouton **Éditer** en haut de la page. La période d'avertissement de licence correspond au nombre de jours avant l'expiration des licences lorsque XClarity Administrator déclenche un avertissement.

## Obtenir de l'aide

- Si vous rencontrez des problèmes et vous êtes passé par un partenaire commercial, contactez ce dernier afin de vérifier la transaction et l'autorisation.
- Si vous n'avez pas reçu votre preuve d'achat électronique, des codes d'autorisation ou des clés d'activation, ou s'ils ont été envoyés à une personne incorrecte, contactez l'un des représentants régionaux, selon votre région.
  - [ESDNA@lenovo.com](mailto:ESDNA@lenovo.com) (Pays d'Amérique du Nord)

- [ESDAP@lenovo.com](mailto:ESDAP@lenovo.com) (pays d'Asie-Pacifique)
  - [ESDEMEA@lenovo.com](mailto:ESDEMEA@lenovo.com) (Pays d'Europe/Moyen-Orient/Afrique)
  - [ESDLA@lenovo.com](mailto:ESDLA@lenovo.com) (Pays d'Amérique Latine)
  - [ESDChina@Lenovo.com](mailto:ESDChina@Lenovo.com) (Chine)
- Si des informations concernant l'autorisation ne sont pas correctes, contactez le support Lenovo à l'adresse [SW\\_override@lenovo.com](mailto:SW_override@lenovo.com) et incluez les informations suivantes :
    - Numéro de commande
    - Vos informations de contact, y compris l'adresse e-mail.
    - Votre adresse physique
    - Modifications que vous souhaitez effectuer
  - Si vous avez des problèmes ou des questions sur le téléchargement de la licence, contactez le support Lenovo à l'adresse [-eSupport\\_-\\_Ops@lenovo.com](mailto:-eSupport_-_Ops@lenovo.com).

---

## Installation de licences d'activation de l'ensemble des fonctionnalités à l'aide du portail Web Features on Demand

Si XClarity Administrator n'a pas accès à Internet, vous pouvez utiliser et récupérer les licences pour des codes d'autorisation existants à l'aide de la fonction [Portail Web Features on Demand](#) d'autres systèmes disposant d'un accès réseau à XClarity Administrator. Vous pouvez ensuite utiliser l'interface Web XClarity Administrator pour importer et installer les licences utilisées.

### Procédure

Pour installer les licences Lenovo XClarity Pro dans le serveur de gestion, procédez comme suit.

Étape 1. Achetez une licence Lenovo XClarity Pro pour chaque appareil géré.

Contactez votre représentant Lenovo ou partenaire commercial agréé pour obtenir des licences Lenovo XClarity Pro selon les fonctions que vous souhaitez activer et le nombre d'appareils que vous souhaitez gérer. Après avoir acheté des licences, vous recevrez un code d'autorisation dans un e-mail contenant votre *preuve d'achat électronique*. Le code d'autorisation est une chaîne alphanumérique de 22 caractères, dont vous avez besoin pour utiliser et installer les licences. Si vous ne recevez pas d'e-mail et que vous avez acheté les licences via un partenaire commercial, contactez votre partenaire commercial pour lui demander le code d'autorisation.

Vous pouvez également extraire vos codes d'autorisation du [Portail Web Features on Demand](#) en cliquant sur **Obtention d'un code d'autorisation**.

Étape 2. Utilisez toutes ou une partie des licences à l'aide du code d'autorisation. Lorsque des licences sont utilisées, un fichier clé d'activation de licence est générée.

1. Ouvrez les [Portail Web Features on Demand](#) à partir d'un navigateur Web et connectez-vous au portail à l'aide de votre ID utilisateur, à savoir votre adresse e-mail.
2. Cliquez sur **Demander une clé d'activation**.
3. Sélectionnez **Saisie d'un code d'autorisation unique**.
4. Entrez le code d'autorisation de 22 caractères, puis cliquez sur **Continuer**.
5. Entrez votre numéro de client Lenovo dans le champ **Numéro de client Lenovo**.
6. Entrez le nombre de licences que vous souhaitez obtenir dans le champ **Obtenir la quantité**, puis cliquez sur **Continuer**.

Pour utiliser toutes les licences disponibles dans ce code d'autorisation, faites correspondre le nombre figurant dans le champ **Licences disponibles**.

Si vous utilisez un sous-ensemble de licences disponibles, vous pouvez utiliser les licences restantes dans une autre clé d'activation de licence à l'aide du même code d'autorisation.


**Astuce** : chaque XClarity Administrator prend en charge jusqu'à 1 000 appareils gérés. Par conséquent, une seule clé d'activation de licence que vous installez dans une instance XClarity Administrator ne doit pas comporter plus de 1 000 licences.

7. Suivez les invites pour saisir les détails du produit et les informations de contact, puis cliquez sur **Continuer** pour générer la clé d'activation de licence.
8. Si vous le souhaitez, vous pouvez indiquer des destinataires supplémentaires, qui recevront les clés d'activation de licence.
9. Cliquez sur **Envoyer** pour envoyer les clés d'activation de licence.

La personne affectée à la commande d'achat et les destinataires supplémentaires reçoivent un e-mail contenant la clé d'activation de licence. La clé est un fichier au format .KEY.

**Remarque** : De plus, vous pouvez télécharger des clés d'activation de licence (individuellement ou non) depuis [Portail Web Features on Demand](#) en cliquant sur **Consultation de l'historique** et en utilisant votre numéro client Lenovo afin de trouver vos clés d'activation de licence. Vous pouvez ensuite télécharger toutes vos clés, ou seulement une partie. Ensuite, cliquez sur **E-mail** pour envoyer les clés par e-mail ou cliquez sur **Télécharger** pour télécharger les clés sur votre système local.

Etape 3. Importez et installez les licences dans XClarity Administrator.

1. Dans la barre de menu de XClarity Administrator, cliquez sur **Administration → Licences** pour afficher la page Gestion de licences.
2. Cliquez sur l'icône **Importer et appliquer** () pour installer les licences.
3. Cliquez sur **Parcourir** pour sélectionner le fichier de clé d'activation de licence pour les licences que vous souhaitez installer.


**Astuce** : pour importer plusieurs clés d'activation de licence, compressez les fichiers .KEY dans un fichier ZIP, puis sélectionnez-le pour l'importation.

4. Cliquez sur **Accepter la licence** pour importer et appliquer les licences.


Une fois l'installation terminée, la clé d'activation de licence est répertoriée dans le tableau contenant le nombre de licences installées et la période d'activation (dates de début et de fin).

## Après avoir terminé

Sur la page Licences, vous pouvez effectuer les actions suivantes.

- Téléchargez une ou plusieurs clés d'activation de licence spécifiques sur le système local en cliquant sur l'icône **Exporter** ()

**Remarque** : Lorsque vous exportez plusieurs clés d'activation de licence, les fichiers sont téléchargés sous la forme d'un fichier ZIP unique.

- Supprimez une clé d'activation de licence spécifique en cliquant sur l'icône **Supprimer** ()
- Configurez la période d'avertissement de licence en cliquant sur le bouton **Éditer** en haut de la page. La période d'avertissement de licence correspond au nombre de jours avant l'expiration des licences lorsque XClarity Administrator déclenche un avertissement.

## Obtenir de l'aide

- Si vous rencontrez des problèmes et vous êtes passé par un partenaire commercial, contactez ce dernier afin de vérifier la transaction et l'autorisation.

- Si vous n'avez pas reçu votre preuve d'achat électronique, des codes d'autorisation ou des clés d'activation, ou s'ils ont été envoyés à une personne incorrecte, contactez l'un des représentants régionaux, selon votre région.
  - [ESDNA@lenovo.com](mailto:ESDNA@lenovo.com) (Pays d'Amérique du Nord)
  - [ESDAP@lenovo.com](mailto:ESDAP@lenovo.com) (pays d'Asie-Pacifique)
  - [ESDEMEA@lenovo.com](mailto:ESDEMEA@lenovo.com) (Pays d'Europe/Moyen-Orient/Afrique)
  - [ESDLA@lenovo.com](mailto:ESDLA@lenovo.com) (Pays d'Amérique Latine)
  - [ESDChina@Lenovo.com](mailto:ESDChina@Lenovo.com) (Chine)
- Si des informations concernant l'autorisation ne sont pas correctes, contactez le support Lenovo à l'adresse [SW\\_override@lenovo.com](mailto:SW_override@lenovo.com) et incluez les informations suivantes :
  - Numéro de commande
  - Vos informations de contact, y compris l'adresse e-mail.
  - Votre adresse physique
  - Modifications que vous souhaitez effectuer
- Si vous avez des problèmes ou des questions sur le téléchargement de la licence, contactez le support Lenovo à l'adresse [-eSupport\\_-\\_Ops@lenovo.com](mailto:-eSupport_-_Ops@lenovo.com).





---

## Chapitre 7. Mise à jour de XClarity Administrator en tant que

Lors de l'exécution de Lenovo XClarity Administrator en tant que conteneur, suivez cette procédure de mise à jour pour installer le logiciel le plus récent comme nouveau conteneur et lier les volumes du conteneur d'origine au nouveau conteneur.

### Avant de commencer

Vous pouvez mettre à jour XClarity Administrator version 4.0 ou ultérieure uniquement à partir d'une instance XClarity Administrator version 3.0 ou ultérieure. Si vous utilisez une version de XClarity Administrator antérieure à la version 3.0, vous devez passer à la version 3.0 ou une version ultérieure avant de procéder à la mise à niveau à la version 4.0.

Pour gérer des instances XClarity Administrator de version 4.0 ou ultérieure à l'aide de Lenovo XClarity Orchestrator, XClarity Orchestrator version 2.0 ou ultérieure est requis. Si vous mettez à jour XClarity Administrator à la version 4.0 ou une version ultérieure, assurez-vous que XClarity Orchestrator est déjà à la version 2.0 ou ultérieure.

### À propos de cette tâche

Le fichier `docker-compose.yml` utilise les variables d'environnement suivantes, que vous avez définies lors de l'installation du conteneur *d'origine*. Ces variables d'environnement sont également utilisées par le nouveau conteneur.

- **CONTAINER\_NAME.** Nom de conteneur unique, utilisé pour créer des volumes Docker pour chaque instance XClarity Administrator (par exemple, `CONTAINER_NAME=LXCA-203`)

XClarity Administrator utilise le nom de conteneur pour créer les volumes du conteneur. Si vous utilisez le même nom de conteneur pour le nouveau conteneur, la nouvelle instance XClarity Administrator va utiliser les mêmes volumes et, par conséquent, aura accès aux mêmes données du système et paramètres de l'instance XClarity Administrator d'origine (conteneur).

Si vous modifiez le nom de conteneur, de nouveaux volumes sont créés pour le conteneur. La nouvelle instance XClarity Administrator n'aura pas accès aux mêmes données système et aux paramètres de l'instance XClarity Administrator d'origine (conteneur). Si vous devez modifier le nom de conteneur ou l'adresse IP, effectuez une sauvegarde des données système et des paramètres de l'instance XClarity Administrator d'origine avant d'installer le nouveau conteneur. Ensuite, utilisez cette sauvegarde pour restaurer les données du système et les paramètres vers le nouveau conteneur.

- **ADDRESS.** Adresse IPv4 ou IPv6 statique pour le conteneur (par exemple, `ADDRESS=192.0.2.0`)

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.

- **BACKUP\_MOUNT** et **FIRMWARE\_MOUNT.** (Facultatif) Chemins pour les partages distants pouvant être utilisés pour stocker les sauvegardes XClarity Administrator ou utilisés en tant que référentiel distant pour les mises à jour de microprogramme. Les chemins doivent respectivement être `/mnt/backup_share` et `/mnt/fw_share`.

**Remarque :** XClarity Administrator *n'est pas* exécuté en tant que conteneur avec privilèges.

### Procédure

Pour mettre à jour un conteneur XClarity Administrator, procédez comme suit.

- Etape 1. Téléchargez l'image du conteneur XClarity Administrator depuis le site [Page Web de téléchargements XClarity Administrator](#) vers un poste de travail client. Connectez-vous au site Web, puis utilisez la clé d'accès qui vous a été fournie pour télécharger l'image.
- Etape 2. Importez l'image de conteneur XClarity Administrator dans votre hôte Docker en exécutant la commande suivante.
- ```
docker load -i lnvgy_sw_lxca_110-3.5.0_anyos_noarch
```
- Etape 3. Modifiez le même fichier `docker-compose.yml` utilisé pour le conteneur d'origine. Mettez à jour la propriété d'image en haut du fichier pour pointer vers la nouvelle image Docker de l'étape 2. Vous pouvez modifier l'étiquette d'image à l'aide de la commande `docker tag`.

Ce qui suit est un exemple de fichier `yml`, avec IPv6 activé.

```
version: '3.8'

services:
  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.2.10
      - 192.0.2.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

volumes:
  data:
    name: ${CONTAINER_NAME}-data
  postgresql:
    name: ${CONTAINER_NAME}-postgresql
  log:
    name: ${CONTAINER_NAME}-log
  confluent-etc:
    name: ${CONTAINER_NAME}-confluent-etc
  confluent-log:
    name: ${CONTAINER_NAME}-confluent-log
```

```

confluent:
  name: ${CONTAINER_NAME}-confluent
propconf:
  name: ${CONTAINER_NAME}-propconf
ssh:
  name: ${CONTAINER_NAME}-ssh
xcat:
  name: ${CONTAINER_NAME}-xcat

networks:
  lan:
    name: lan
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: eth0
    ipam:
      config:
        - subnet: 192.0.0.0/19
          gateway: 192.0.30.1
        - subnet: "2001:8003:7d51:2000::/80"
          gateway: "2001:8003:7d51:2000::1"

```

Etape 4. Arrêtez le conteneur *d'origine* en exécutant la commande suivante.

```
docker-compose -p ${CONTAINER_NAME} down
```

Etape 5. Déployez la *nouvelle* image dans Docker en exécutant la commande ci-après, `<ENV_FILENAME>` étant le nom du fichier des variables d'environnement.

```
COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d
```



---

## Chapitre 8. Désinstallation de XClarity Administrator

Procédez comme suit pour désinstaller un dispositif virtuel Lenovo XClarity Administrator ou un conteneur.

### Procédure

Pour désinstaller le dispositif virtuel XClarity Administrator, procédez comme suit.

- Etape 1. Annulez la gestion de tous les appareils actuellement gérés par XClarity Administrator (voir [Gestion des châssis](#), [Gestion des serveurs](#) et [Gestion des commutateurs](#) dans la documentation en ligne XClarity Administrator).
- Etape 2. Désinstallez XClarity Administrator, selon le système d'exploitation :
- **Docker-compose** Exécutez la commande ci-après pour arrêter le conteneur et retirer les réseaux et les volumes.  
`docker-compose down -v`
  - **CentOS, Red Hat, Rocky et Ubuntu**
    1. Connectez-vous à l'hôte à l'aide du gestionnaire de machine virtuelle.
    2. Cliquez avec le bouton droit de la souris sur la machine virtuelle, puis cliquez sur **Arrêter** → **Forcer l'arrêt**.
    3. Cliquez à nouveau avec le bouton droit de la souris sur la machine virtuelle, puis cliquez sur **Supprimer**. La boîte de dialogue Confirmation de la suppression s'affiche.
    4. Sélectionnez toutes les cases à cocher et cliquez sur **Supprimer**.
  - **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** → **Mettre hors tension**.
    3. Cliquez à nouveau avec le bouton droit de la souris sur la machine virtuelle, puis cliquez sur **Supprimer du disque**.
  - **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, puis cliquez sur **Arrêter**.
    4. Cliquez à nouveau avec le bouton droit de la souris sur la machine virtuelle, puis cliquez sur **Supprimer**.