Lenovo XClarity Management Hub
Guide d’installation et d’utilisation

Version 2.1

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 Orchestrator.

Deuxième édition (Juillet 2024)

Table des matières

Chapitre 1. Planification pour Lenovo XClarity Management Hub

Passez en revue les remarques et les prérequis suivants pour vous aider à planifier l'installation de Lenovo XClarity Management Hub.

Logiciel et matériel pris en charge

Assurez-vous que votre environnement dispose de la configuration matérielle et logicielle requise pour Lenovo XClarity Management Hub.

Systèmes hôte

Exigences en matière d'hyperviseur

Les hyperviseurs suivants sont pris en charge pour l'installation de Lenovo XClarity Management Hub.
- VMware ESXi 7.0, U1, U2 et U3
- VMware ESXi 6.7, U1, U2[1] et U3

Pour VMware ESXi, le dispositif virtuel est un modèle OVF.

Important :

- Pour VMware ESXi 6.7 U2, vous devez utiliser l'image ISO VMware-ESXi-6.7.0.update02-13981272-LNV-20190630.iso ou ultérieure.

Configuration matérielle

Le tableau ci-après répertorie les configurations *minimales recommandées* pour XClarity Management Hub sur la base du nombre de périphériques clients Edge gérés. Selon votre environnement, des ressources supplémentaires peuvent s'avérer nécessaires afin d'optimiser les performances.

Nombre de périphériques clients Edge gérés	Processeurs	Mémoire	Stockage
0 - 100 appareils	6	32 Go	340 Go
100 - 200 appareils	8	34 Go	340 Go
200 - 400 appareils	10	36 Go	340 Go
400 - 600 appareils	12	40 Go	340 Go
600 - 800 appareils	14	44 Go	340 Go
800 – 1 000 appareils	16	48 Go	340 Go

1. Il s'agit de la quantité de stockage minimale pour l'utilisation par le dispositif virtuel XClarity Management Hub en tant que magasin de données SSD.

Configuration logicielle

Les logiciels suivants sont requis par XClarity Management Hub.

- **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 de gestionnaires de ressources et

d'appareils gérés soient synchronisés avec XClarity Management Hub. Assurez-vous que le serveur NTP est accessible via le réseau de gestion (généralement, l'interface Eth0).

Appareils pouvant être gérés

XClarity Management Hub peut gérer, surveiller et approvisionner un maximum de 10,000 appareils clients ThinkEdge (sans contrôleurs de gestion de la carte mère).

Vous trouverez une liste complète des appareils clients ThinkEdge et des options pris en charge (par exemple, des dispositifs d'E-S, des barrettes DIMM et des adaptateurs de stockage), des niveaux de microprogramme minimum requis, ainsi que des remarques concernant les limites à l'adresse Page Web des serveurs XClarity Management Hub.

Pour obtenir des informations générales sur les configurations matérielles et les options d'un appareil spécifique, voir page Web de Lenovo Server Proven.

Navigateurs Web

L'interface Web XClarity Management Hub fonctionne avec ces navigateurs Web.
- Chrome 80.0 ou version ultérieure
- Firefox ESR 68.6.0 ou version ultérieure
- Microsoft Edge 40.0 ou version ultérieure
- Safari 13.0.4 ou version ultérieure (s'exécute sur macOS 10.13 ou versions ultérieures)

Pare-feux et serveurs proxy

Certaines fonctions de maintenance et de support, y compris l'appel vers Lenovo et l'état de la garantie, nécessitent l'accès à Internet. Si vous avez des pare-feux dans votre réseau, configurez-les afin de permettre à XClarity Orchestrator et aux gestionnaires de ressources d'effectuer ces opérations. Si Lenovo XClarity Orchestrator et les gestionnaires de ressources ne disposent pas d'un accès direct à Internet, configurez-les pour l'utilisation d'un serveur proxy.

Pare-feux

Assurez-vous que les noms et ports DNS ci-après sont ouverts sur le pare-feu pour XClarity Orchestrator et les gestionnaires de ressources applicables (Lenovo XClarity Management Hub 2.0, Lenovo XClarity Management Hub et Lenovo XClarity Administrator), le cas échéant. Chaque DNS représente un système distribué de manière géographique avec une adresse IP dynamique.

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

Nom DNS	Les ports	Protocoles
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)		
download.lenovo.com	443	https
support.lenovo.com	443 et 80	https et http
Envoyer des données de maintenance au support Lenovo (appel vers Lenovo) - XClarity Orchestrator uniquement		
soaus.lenovo.com	443	https

Nom DNS	Les ports	Protocoles
esupportwebapi.lenovo.com (XClarity Orchestrator v2.0 et versions ultérieures) rsgw-eservice.motorola.com (XClarity Orchestrator v1.6) supportwebapi.lenovo.com:443/luf.luf-web.prd/BLL/Logupload.ashx (XClarity Orchestrator v1.5 et versions antérieures)	443	https
Envoi de données périodiques à Lenovo – XClarity Orchestrator uniquement		
esupportwebapi.lenovo.com (XClarity Orchestrator v2.0 et versions ultérieures) rsgw-eservice.motorola.com (XClarity Orchestrator v1.6) supportwebapi.lenovo.com:443/luf.luf-web.prd/BLL/uploadSnapshot.ashx (XClarity Orchestrator v1.5 et versions antérieures)	443	https
Obtenir les informations relatives à la garantie		
supportapi.lenovo.com	443	https et http

Serveur proxy

Si XClarity Orchestrator ou les gestionnaires de ressources n'ont pas d'accès direct à Internet, assurez-vous de bien les configurer pour l'utilisation d'un serveur proxy HTTP (voir Configuration du réseaudans la documentation en ligne de XClarity Orchestrator).

- 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.

Attention : XClarity Management Hub doit disposer d'un accès direct à Internet. Un serveur proxy HTTP n'est actuellement pas pris en charge.

Disponibilité de port

Lenovo XClarity Orchestrator et les gestionnaires de ressources exigent que certains ports soient ouverts afin de faciliter la communication. Si les ports requis sont bloqués ou utilisés par un autre processus, certaines fonctions peuvent ne pas fonctionner correctement.

XClarity Orchestrator, Lenovo XClarity Management Hub 2.0, Lenovo XClarity Management Hub et Lenovo XClarity Administrator sont des applications RESTful qui communiquent en toute sécurité via TCP sur le port 443.

XClarity Orchestrator

XClarity Orchestrator écoute et répond sur les ports répertoriés dans le tableau suivant. Si XClarity Orchestrator et toutes les ressources gérées sont derrière un pare-feu, et que vous avez l'intention d'accéder à ces ressources à partir d'un navigateur qui se trouve à *l'extérieur* du pare-feu, vous devez vous assurer que les ports requis sont ouverts.

Remarque : XClarity Orchestrator 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.

Service	**Sortant (ports ouverts sur des systèmes externes)**	**Entrant (ports ouverts sur appareil XClarity Orchestrator)**
Dispositif XClarity Orchestrator	• DNS - TCP/UDP sur le port **53**	• HTTPS - TCP sur le port **443**
Serveurs d'authentification externes	• LDAP – TCP sur le port **389**[1]	Sans objet
Services d'acheminement d'événement	• Serveur e-mail (SMTP) - UDP sur le port **25**[1] • Service Web REST (HTTP) – UPD sur le port **80**[1] • Splunk – UDP sur le port **8088**[11], **8089**[1] • Syslog - UDP sur le port **514**[1]	Sans objet
Services Lenovo (y compris Appel vers Lenovo)	• HTTPS (appel vers Lenovo) - TCP sur le port **443**	Sans objet

1. Il s'agit du port par défaut. Ce port est configurable à partir de l'interface utilisateur XClarity Orchestrator.

XClarity Management Hub 2.0

Lenovo XClarity Management Hub 2.0 nécessite l'ouverture de certains ports en vue de faciliter la communication. Si les ports requis sont bloqués ou utilisés par un autre processus, il est possible que certaines fonctions du concentrateur de gestion ne fonctionnent pas correctement.

Si des appareils pouvant être gérés sont protégés par un pare-feu, et que vous avez l'intention de gérer ces appareils à partir d'un concentrateur de gestion qui se trouve à l'extérieur de ce pare-feu, vous devez vous assurer que tous les ports impliqués dans des communications entre le concentrateur de gestion et le contrôleur de gestion de la carte mère de chaque appareil sont ouverts.

Service ou composant	**Sortant (ports ouverts vers des systèmes externes)**	**Entrant (ports ouverts vers les appareils cible)**
XClarity Management Hub 2.0	• DNS - UDP sur le port **53** • NTP - UDP sur le port **123** • HTTPS - TCP sur le port **443** • SSDP - UDP sur le port **1 900** • DHCP - UDP sur le port **67**	• HTTPS - TCP sur le port **443** • SSDP - UDP sur les ports **32768**-**65535**
Serveurs ThinkSystem et ThinkAgile	• HTTPS - TCP sur le port **443** • Reconnaissance SSDP – UDP sur le port **1900**	• HTTPS - TCP sur le port **443**

XClarity Management Hub

XClarity Management Hub écoute et répond sur les ports répertoriés dans le tableau suivant.

Service ou composant	Sortant (ports ouverts sur des systèmes externes)	Entrant (ports ouverts sur l'appareil XClarity Management Hub)
Dispositif XClarity Management Hub[1]	• DNS - TCP/UDP sur le port **53**[2]	• HTTPS - TCP sur le port **443** • MQTT – TCP sur le port **8883**
Appareils clients ThinkEdge[3]	Sans objet	• MQTT – TCP sur le port **8883**

1. Lors de l'utilisation de XClarity Management Hub pour gérer des appareils par le biais de XClarity Orchestrator, certains ports doivent être ouverts afin de faciliter la communication. Si les ports requis sont bloqués ou utilisés par un autre processus, certaines fonctions de XClarity Orchestrator peuvent ne pas fonctionner correctement.
2. XClarity Management Hub peut éventuellement être configuré pour établir des connexions sortantes vers des services externes. 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.
3. Si des appareils pouvant être gérés sont protégés par un pare-feu, et que vous avez l'intention de gérer ces appareils à partir d'un XClarity Management Hub qui se trouve à l'extérieur de ce pare-feu, vous devez vous assurer que tous les ports impliqués dans des communications entre le XClarity Management Hub et les appareils Edge sont ouverts.

XClarity Administrator

Lors de l'utilisation de Lenovo XClarity Administrator pour gérer des appareils par le biais de Lenovo XClarity Orchestrator, certains ports doivent être ouverts afin de faciliter la communication. Si les ports requis sont bloqués ou utilisés par un autre processus, certaines fonctions de XClarity Orchestrator peuvent ne pas fonctionner correctement.

Pour obtenir plus d'informations sur les ports qui doivent être ouverts pour XClarity Administrator, voir Disponibilité de port dans la documentation en ligne de XClarity Administrator.

Remarques sur le réseau

Vous pouvez vous configurer le Lenovo XClarity Management Hub afin d'utiliser une interface réseau unique (eth0) ou deux interfaces réseau séparées (eth0 et eth1) en vue de communiquer.

Lenovo XClarity Management Hub communique sur les réseaux suivants.

- Le *réseau de gestion* est utilisé pour communiquer entre le Lenovo XClarity Management Hub et les appareils gérés.
- Le *réseau de données* est utilisé pour communiquer entre les systèmes d'exploitation installés sur les serveurs et l'intranet de l'entreprise, Internet ou les deux.

Interface unique (eth0)

Lorsque vous utilisez une interface réseau unique (eth0), les communications de gestion, les communications de données et le déploiement du système d'exploitation se produisent sur le même réseau.

Lorsque vous configurez le Lenovo XClarity Management Hub, définissez l'interface réseau eth0 en tenant compte des remarques suivantes.

- L'interface réseau doit être configurée de manière à prendre en charge la détection et la gestion d'appareils (dont les mises à jour du microprogramme). Le Lenovo XClarity Management Hub doit être en mesure de communiquer avec tous ses appareils gérés depuis le réseau de gestion.Le Lenovo XClarity Management Hub doit être en mesure de communiquer avec tous ses appareils gérés depuis le réseau.

- Pour déployer les images SE, l'interface eth0 doit disposer d'une connectivité réseau IP à l'interface réseau du serveur qui sert à accéder au système d'exploitation hôte.
- **Important :** la mise en place d'un réseau de données et de gestion partagé peut entraîner des interruptions du trafic avec, par exemple, des modules ignorés ou des problèmes liés à la connectivité du réseau de gestion, en fonction de la configuration de votre 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.

Deux interfaces séparées (eth0 et eth1)

Lorsque vous utilisez deux interfaces réseau (eth0 et eth1), il est possible de configurer les réseaux comme suit : séparés physiquement ou séparés virtuellement.

Passez en revue les remarques suivantes lors de la définition des interfaces réseau eth0 et eth1.

- L'interface réseau eth0 doit être connectée au réseau de gestion. Elle doit en outre être configurée pour prendre en charge la détection et la gestion des appareils. Le Lenovo XClarity Management Hub doit être en mesure de communiquer avec tous ses appareils gérés depuis le réseau de gestion.
- L'interface réseau eth1 peut être configurée pour communiquer avec un réseau de données interne, un réseau de données public ou les deux.
- Si vous souhaitez déployer des images du système d'exploitation, l'interface réseau eth1 doit disposer d'une connectivité réseau IP à l'interface réseau du serveur qui sert à accéder au système d'exploitation hôte.
- Les fonctions peuvent être effectuées sur l'un ou l'autre réseau.
- Pour les réseaux séparés virtuellement, les modules du réseau de gestion et les modules du réseau de données sont envoyés par la même connexion physique. Utilisez un marquage VLAN sur tous les modules de données du réseau de gestion pour bien assurer la séparation entre les deux réseaux.

Remarques sur les adresses IP

Passez en revue les remarques suivantes sur les adresses IP avant de configurer le réseau.

- La modification de l'adresse IP du dispositif virtuel après l'exécution XClarity Management Hub va entraîner des problèmes de connectivité avec XClarity Orchestrator et tous les appareils gérés. Si vous devez modifier l'adresse IP, déconnectez XClarity Management Hub de XClarity Orchestrator, annulez la gestion de tous les appareils gérés avant de modifier l'adresse IP, puis appliquez à nouveau la gestion aux appareils et reconnectez XClarity Management Hub à XClarity Orchestrator une fois l'adresse IP modifiée
- 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, assurez-vous que les modifications des adresses IP sont réduites au minimum ; par exemple, en basant l'adresse DHCP sur une adresse MAC, ou en configurant le DHCP de sorte que le bail n'expire pas.Si l'adresse IP d'un appareil géré (autre qu'un appareil client ThinkEdge) est modifiée, vous devez annuler la gestion de l'appareil, puis le gérer à nouveau.
- La conversion d'adresses réseau (NAT), qui remappe un espace d'adresse IP dans un autre, n'est pas prise en charge.
- Les interfaces réseau doivent être configurées avec une adresse IPv4 afin de gérer les appareils suivants. Les adresses IPv6 ne sont pas prises en charge.
  - 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.

Remarques sur la haute disponibilité

Pour configurer la haute disponibilité pour Lenovo XClarity Orchestrator, utilisez les fonctions de haute disponibilité faisant partie du système d'exploitation hôte.

Microsoft Hyper-V

Utilisez la fonctionnalité de haute disponibilité fournie pour l'environnement Hyper-V.

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).

Chapitre 2. Configuration du XClarity Management Hub pour les appareils clients Edge

Lorsque vous accédez au Lenovo XClarity Management Hub pour la première fois, il existe plusieurs étapes à exécuter pour la configuration initiale du XClarity Management Hub.

Procédure

Procédez comme suit pour effectuer la configuration initiale du XClarity Management Hub.

Etape 1. Connectez-vous à l'interface Web du XClarity Management Hub.

Etape 2. Lisez et acceptez le contrat de licence.

Etape 3. Créer des comptes utilisateur supplémentaires.

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. Inscrivez le XClarity Management Hub auprès du serveur Orchestrator.

Connexion à l'XClarity Management Hub pour les appareils clients Edge

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

Avant de commencer

Vérifiez que vous utilisez l'un des navigateurs Web pris en charge suivants.
- Chrome 80.0 ou version ultérieure
- Firefox ESR 68.6.0 ou version ultérieure
- Microsoft Edge 40.0 ou version ultérieure
- Safari 13.0.4 ou version ultérieure (s'exécute sur macOS 10.13 ou versions ultérieures)

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

Si vous configurez XClarity Management Hub 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 Management Hub à partir d'une autre machine virtuelle disposant d'une connectivité à XClarity Management Hub. Par exemple, vous pouvez accéder à XClarity Management Hub à partir d'une autre machine virtuelle sur l'hôte sur lequel XClarity Management Hub est installé.

XClarity Management Hub déconnecte automatiquement les sessions des utilisateurs après 60 minutes, quelle que soit leur activité.

Procédure

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

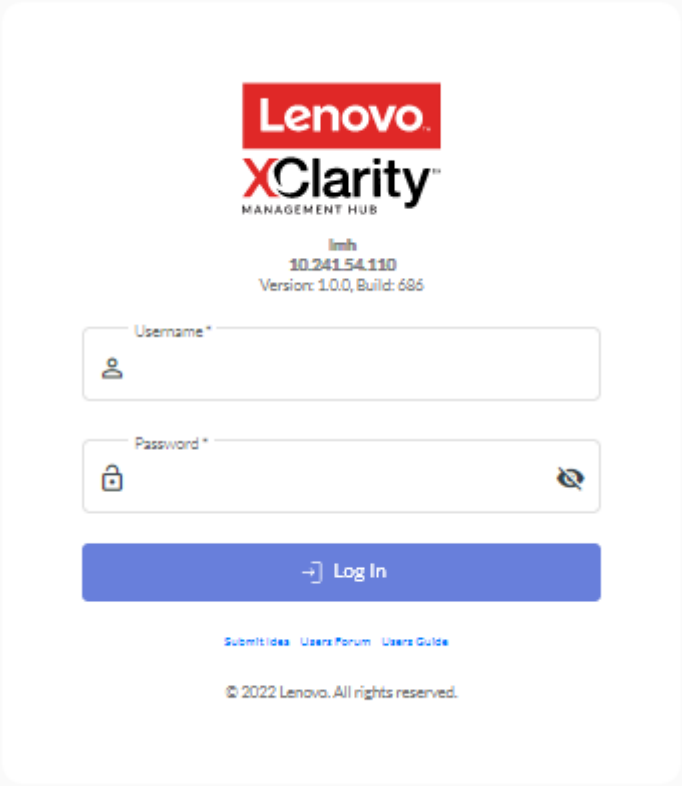
Etape 1. Faites pointer votre navigateur sur l'adresse IP de XClarity Management Hub.
`https://<IPv4_address>`

Par exemple :
`https://192.0.2.10`

L’adresse IP que vous utilisez dépend de l’installation de votre environnement.

- Si vous indiquez une adresse IPv4 dans eth0_config, utilisez cette adresse IPv4 pour accéder au XClarity Management Hub.
- Si un serveur DHCP est configuré dans le même domaine de diffusion que le XClarity Management Hub, utilisez l’adresse IPv4 qui s’affiche dans la console de la machine virtuelle XClarity Management Hub pour accéder au XClarity Management Hub.
- 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 le XClarity Management Hub 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 Management Hub par défaut.

La page de connexion initiale de XClarity Management Hub s'affiche :



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

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

Etape 3. Saisissez vos données d’identification et cliquez sur **Connexion**.

Si vous vous connectez à XClarity Management Hub pour la première fois, saisissez les données d’identification **USERID** et **PASSW0RD** par défaut (où 0 est zéro).

Etape 4. Lisez et acceptez le contrat de licence.

Etape 5. Si vous vous connectez pour la première fois à l’aide des données d’identification par défaut, vous serez invité(e) à changer le mot de passe. Par défaut, les mots de passe doivent contenir **8** à **256** caractères et doivent respecter les critères suivants.

Important : Nous vous recommandons d'utiliser des mots de passes forts, composés d'au moins 16 caractères.

- (1) Doit contenir au moins un caractère alphabétique en majuscule
- (2) Doit contenir au moins un caractère alphabétique en minuscule
- (3) Doit contenir au moins un nombre
- (4) Doit contenir au moins un caractère spécial
- (5) Doit être différent du nom d'utilisateur

Etape 6. Si vous vous connectez pour la première fois, vous êtes invité à choisir d'utiliser le certificat auto-signé actuel ou d'utiliser un certificat signé par une autorité de certification externe. Si vous décidez d'utiliser un certificat signé en externe, la page Certificat de serveur s'affiche.

Attention : Le certificat auto-signé n'est pas sécurisé. Il est conseillé de générer et d'installer votre propre certificat signé en externe.

Pour en savoir plus sur l'utilisation d'un certificat signé en externe, voir Installation d'un certificat de serveur fiable et signé de manière externe pour XClarity Management Hub pour les appareils clients Edge.

Après avoir terminé

Vous pouvez effectuer les actions suivantes depuis le menu **Compte utilisateur** ( ) situé dans le coin supérieur droit de l'interface Web de XClarity Management Hub.

- Pour vous déconnecter de la session en cours, cliquez sur **Déconnexion**. La page de connexion de XClarity Management Hub s'affiche.
- Posez vos questions et trouvez des réponses à l'aide du Site Web du forum de communauté Lenovo XClarity.
- Envoyez vos commentaires à propos de XClarity Management Hub en cliquant sur **Soumettre des idées** depuis le menu **Compte utilisateur** ( ) dans le coin supérieur droit de l'interface Web, ou en accédant directement à la section Site Web Lenovo XClarity Ideation.
- Consultez la documentation en ligne en cliquant sur **Guide d'utilisation**.
- Pour des informations sur la version de XClarity Management Hub, cliquez sur **À propos de**.
- Vous pouvez modifier la langue de l'interface utilisateur en cliquant sur **Modifier la langue**. Les langues suivantes sont prises en charge.
  - Anglais (en)
  - Chinois simplifié (zh-CN)
  - Chinois traditionnel (zh-TW)
  - Français (fr)
  - Allemand (de)
  - Italien (it)
  - Japonais (ja)
  - Coréen (ko)
  - Portugais (Brésil) (pt-BR)
  - Russe (ru)
  - Espagnol (es)
  - Thaï (th)

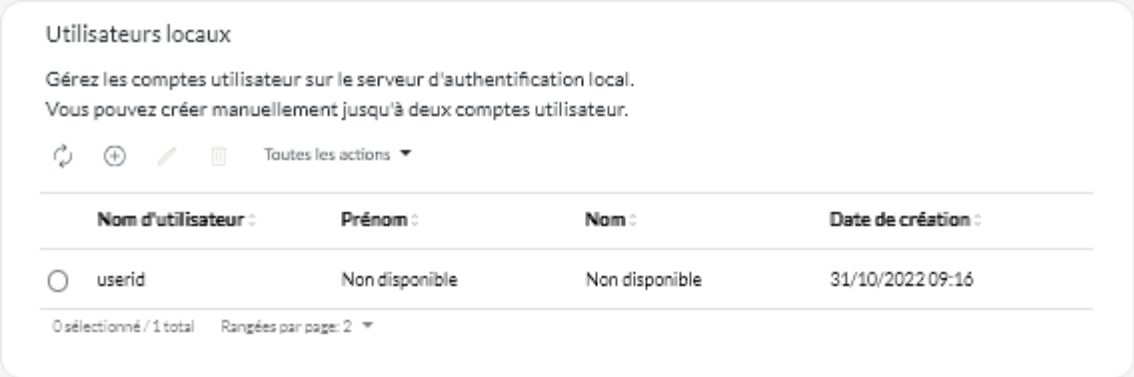
Création de comptes utilisateur pour Lenovo XClarity Management Hub pour les appareils clients Edge

Vous pouvez créer jusqu'à 10 comptes utilisateur pour le Lenovo XClarity Management Hub.

Procédure

Pour créer un compte utilisateur, procédez comme suit.

Etape 1. Dans la barre de menus Lenovo XClarity Management Hub, cliquez sur **Sécurité ( )** → **Utilisateurs locaux** pour afficher la carte Utilisateurs locaux.



Etape 2. Cliquez sur l'icône **Créer** ( ) pour créer un utilisateur. La boîte de dialogue Créer un nouvel utilisateur s'affiche.

Etape 3. Entrez les informations ci-après dans la boîte de dialogue.

- Entrez un nom d'utilisateur unique. Vous pouvez spécifier jusqu'à 32 caractères, y compris les caractères alphanumériques, le point (.), le tiret (-) et le trait de soulignement (_).

  Remarque : les noms d'utilisateur ne tiennent pas compte de la casse.
- Entrez les nouveaux mots de passe et confirmez-les. Par défaut, les mots de passe doivent contenir **8** à **256** caractères et doivent respecter les critères suivants.

  Important : Nous vous recommandons d'utiliser des mots de passes forts, composés d'au moins 16 caractères.
  - (1) Doit contenir au moins un caractère alphabétique en majuscule
  - (2) Doit contenir au moins un caractère alphabétique en minuscule
  - (3) Doit contenir au moins un nombre
  - (4) Doit contenir au moins un caractère spécial
  - (5) Doit être différent du nom d'utilisateur

Etape 4. Cliquez sur **Créer**.

Le compte utilisateur est ajouté au tableau.

Après avoir terminé

Sur la carte Utilisateurs locaux, vous pouvez effectuer les actions suivantes.

- Modifiez le mot de passe et les propriétés de votre compte utilisateur en cliquant sur l'icône **Éditer** ( ). Veuillez noter que les mots de passe n'expirent pas.
- Supprimer un utilisateur sélectionné en cliquant sur l'icône **Supprimer** ( ).

Configuration des paramètres réseau pour XClarity Management Hub les appareils clients Edge

Vous pouvez configurer une seule interface réseau IPv4 et des paramètres de routage Internet.

Avant de commencer

Avant de configurer le réseau, passez en revue les remarques relatives au réseau (voir Remarques sur le réseau).

Procédure

Pour configurer les paramètres réseau, cliquez sur **Administration (⚙) → Mise en réseau** depuis la barre de menus XClarity Management Hub, puis effectuez une ou plusieurs des étapes suivantes.

- **Configurer les paramètres IP**En ce qui concerne l'interface eth0, cliquez sur l'onglet **Interface eth0**, configurez les paramètres d'adresse IPv4 applicables, puis cliquez sur **Appliquer**.

  Attention :

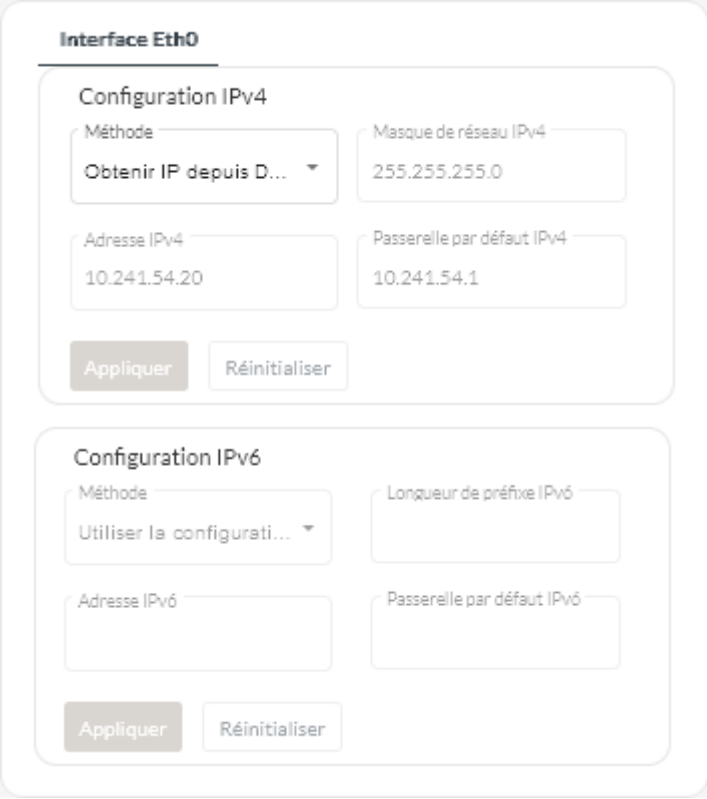
  – La modification de l'adresse IP du dispositif virtuel après l'exécution XClarity Management Hub va entraîner des problèmes de connectivité avec XClarity Orchestrator et tous les appareils gérés. Si vous devez modifier l'adresse IP, déconnectez XClarity Management Hub de XClarity Orchestrator, annulez la gestion de tous les appareils gérés avant de modifier l'adresse IP, puis appliquez à nouveau la gestion aux appareils et reconnectez XClarity Management Hub à XClarity Orchestrator une fois l'adresse IP modifiée

  A l'heure actuelle, seules les adresses IPv4 sont prises en charge.

  – **Paramètres IPv4**. Vous pouvez configurer la méthode d'affectation IP, l'adresse IPv4, le masque de réseau et la passerelle par défaut.Pour la méthode d'affectation IP, vous pouvez choisir d'utiliser une adresse IP attribuée de manière statique ou obtenir une adresse IP à partir d'un serveur DHCP. Lorsque vous utilisez une adresse IP statique, vous devez fournir une adresse IP, un masque de réseau et une passerelle par défaut.

    La passerelle par défaut doit être une adresse IP valide et utiliser le même masque de réseau (le même sous-réseau) que l'interface autorisée (eth0).

    Si l'une des interfaces utilise le protocole DHCP pour obtenir une adresse IP, la passerelle par défaut utilise également le DHCP.



- **Configurer des paramètres de routage Internet**Configurez éventuellement les paramètres DNS (Domain Name System) dans la carte Configuration DNS. Ensuite, cliquez sur **Appliquer**.

  A l'heure actuelle, seules les adresses IPv4 sont prises en charge.

  Vous pouvez changer l’adresse IP du serveur DNS.

  Le nom de domaine entièrement qualifié (FQDN) et le nom d’hôte du serveur DNS sont les mêmes que ceux du serveur XClarity Management Hub et ils ne peuvent pas être modifiés.

Configuration de la date et de l’heure pour le XClarity Management Hub appareils clients Edge

Vous devez configurer au moins un (quatre maximum) serveur NTP (Network Time Protocol) pour synchroniser les horodatages entre le XClarity Management Hub et tous les appareils gérés.

Avant de commencer

Chaque serveur NTP doit être accessible via le réseau. Pensez à configurer le serveur NTP sur le système local sur lequel XClarity Management Hub s'exécute.

Si vous modifiez l'heure sur le serveur NTP, un certain temps peut être nécessaire pour que XClarity Management Hub se synchronise avec la nouvelle heure.

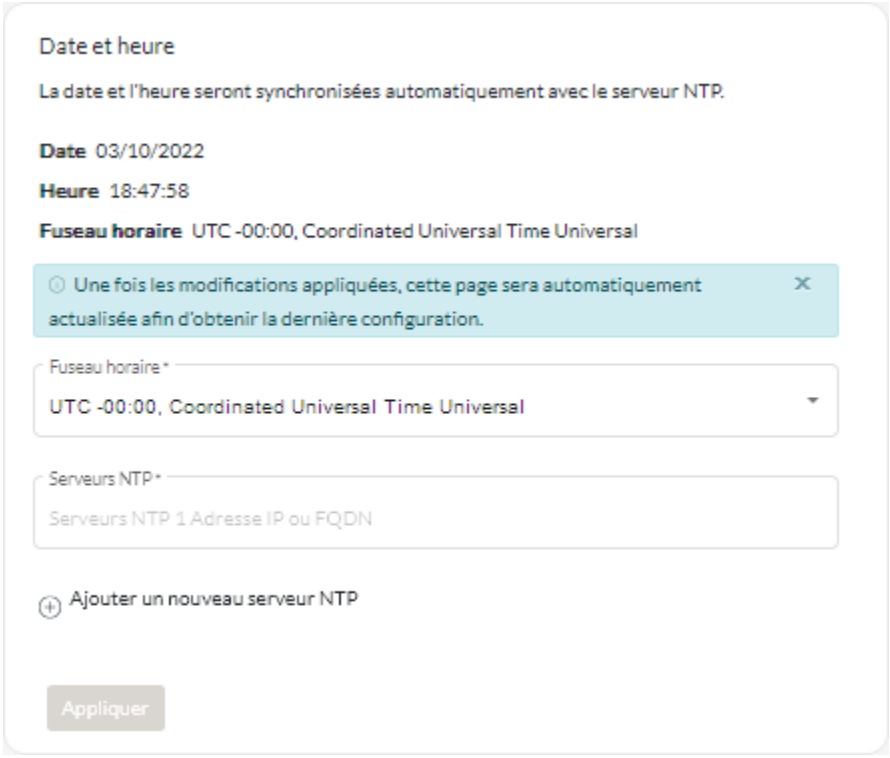
Attention : Le dispositif virtuel XClarity Management Hub et son hôte doivent être définis pour une synchronisation avec la même source temporelle afin d'éviter toute synchronisation involontaire entre XClarity Management Hub et son hôte. Généralement, l'hôte est configuré pour que les dispositifs virtuels se synchronisent avec lui. Si le XClarity Management Hub est défini pour être synchronisé avec une source différente de son hôte, vous devez désactiver la synchronisation des horloges de l'hôte entre les dispositifs virtuels du XClarity Management Hub et son hôte.

- Pour ESXi, suivez les instructions dans VMware – Page Web Désactivation de la synchronisation des horloges.

Procédure

Pour définir la date et l'heure pour XClarity Management Hub, procédez comme suit.

Etape 1. Dans la barre de menus de XClarity Management Hub, cliquez sur **Administration (⚙) → Date et heure** pour afficher la carte Date et heure.



Etape 2. Choisissez le fuseau horaire correspondant à l'hôte pour XClarity Management Hub.

Si le fuseau horaire sélectionné observe l'heure d'été (DST), l'heure est automatiquement ajustée en fonction.

Etape 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.

Etape 4. Cliquez sur **Appliquer**.

Gestion des certificats de sécurité pour Lenovo XClarity Management Hub pour les appareils clients Edge

Le Lenovo XClarity Management Hub utilise des certificats SSL afin d'établir des communications sécurisées et approuvées entre le Lenovo XClarity Management Hub et ses appareils gérés, ainsi que des communications avec le Lenovo XClarity Management Hub par les utilisateurs ou avec différents services. Par défaut, le Lenovo XClarity Management Hub et XClarity Orchestrator utilisent des certificats générés par XClarity Orchestrator qui sont autosignés et émis par une autorité de certification interne.

Avant de commencer

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

À propos de cette tâche

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

- Générez une nouvelle paire de clés en regénérant l'autorité de certification interne et/ou le certificat du serveur final qui utilise des valeurs spécifiques à votre organisation.
- Générez une demande de signature de certificat (CSR) qui peut être envoyée à l'autorité de certification de votre choix pour signer un certificat personnalisé qui peut être téléchargé vers Lenovo XClarity Management Hub 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.

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

Lenovo XClarity Management Hub fait office de client lors de la communication avec des appareils gérés et des services externes. Lorsque cela se produit, l'appareil géré ou le service externe fourni son certificat de serveur en vue d'une vérification par le Lenovo XClarity Management Hub. Le Lenovo XClarity Management Hub conserve une liste des certificats de confiance. Si le *certificat sécurisé* fourni par l'appareil géré ou le service externe n'est pas répertorié, Lenovo XClarity Management Hub se déconnecte de l'appareil géré ou du service externe pour éviter d'échanger toutes les informations de sécurité sensibles avec une source non sécurisée.

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

- **Certificat de serveur**. Lors de l'amorçage initiale, une clé unique et un certificat auto-signé sont générés. Ils sont utilisés en tant qu'autorité de certification racine par défaut, qui peut être gérée sur la page de l'autorité de certification dans les paramètres de sécurité de Lenovo XClarity Management Hub. Il n'est pas nécessaire de regénérer ce certificat racine, sauf si la clé a été compromise ou si votre organisation dispose d'une règle indiquant que tous les certificats doivent être remplacés régulièrement (voir Régénération du certificat de serveur autosigné pour XClarity Management Hub pour les appareils clients Edge).De même, lors de la configuration initiale, une clé distincte est générée et un certificat de serveur est créé, puis signé par l'autorité de certification interne. Ce certificat est utilisé en tant que certificat de serveur Lenovo XClarity Management Hub par défaut. Il se regénère automatiquement à chaque fois que Lenovo XClarity Management Hub détecte que ses adresses de mise en réseau (adresses IP ou DNS) ont changé pour garantir que le certificat contient les adresses exactes pour le serveur. Il peut être personnalisé et généré à la demande (voir Régénération du certificat de serveur autosigné pour XClarity Management Hub pour les appareils clients Edge).

  Vous pouvez choisir d'utiliser un certificat de serveur à signature externe au lieu du certificat de serveur autosigné par défaut en générant une demande de signature de certificat (CSR), en faisant signer la CSR par une autorité de certification racine de certificat privée ou commerciale, puis en important l'intégralité de la chaîne de certificats dans Lenovo XClarity Management Hub (voir Installation d'un certificat de serveur fiable et signé de manière externe pour XClarity Management Hub pour les appareils clients Edge).

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

Régénération du certificat de serveur autosigné pour XClarity Management Hub pour les appareils clients Edge

Vous pouvez générer un nouveau certificat de serveur pour remplacer le serveur de certificat actuel auto-signé Lenovo XClarity Management Hub ou pour rétablir un certificat généré par XClarity Management Hub si XClarity Management Hub utilise actuellement un certificat de serveur à signature externe personnalisé. Le nouveau certificat de serveur auto-signé est utilisé par XClarity Management Hub pour l'accès HTTPS.

Avant de commencer

Attention : Si vous régénérez le XClarity Management Hub certificat du serveur à l'aide d'un nouveau certificat racine CA, XClarity Management Hub perd sa connexion aux appareils gérés et vous devez gérer ces derniers à nouveau. Si vous régénérez le XClarity Management Hub certificat du serveur sans modifier le certificat racine CA (par exemple, lorsque le certificat a expiré), il n'est pas nécessaire de gérer à nouveau les appareils.

À propos de cette tâche

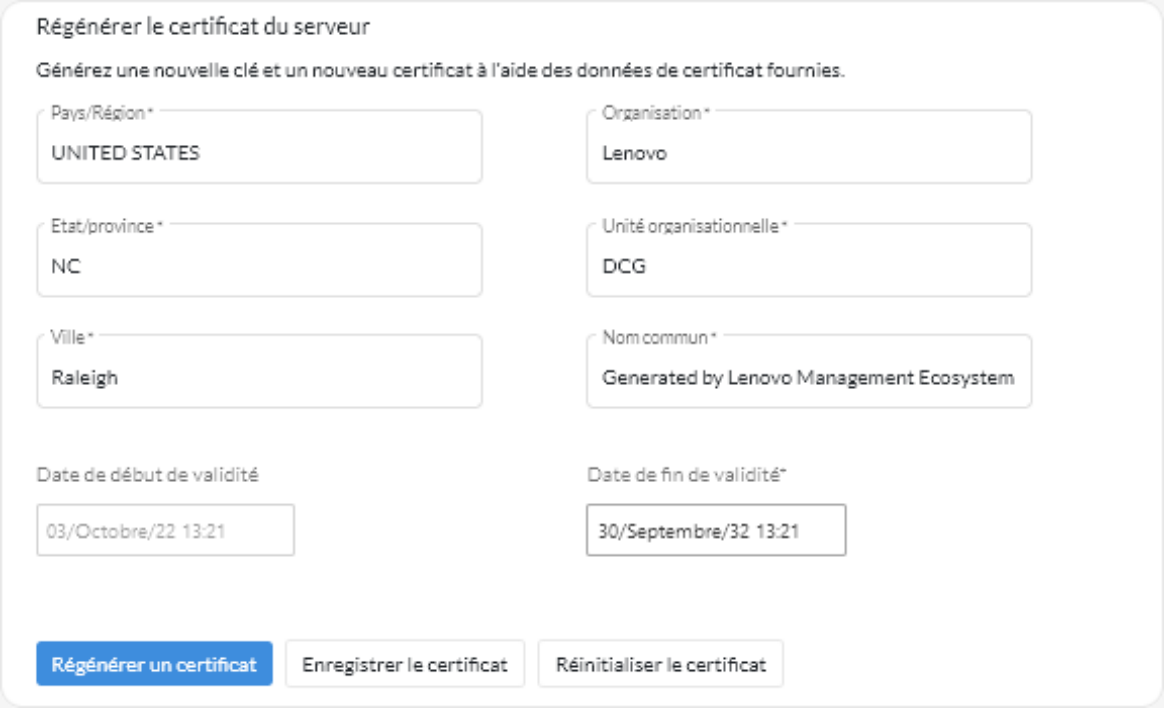
Le certificat de serveur qui est en cours d'utilisation, qu'il soit auto-signé ou à signature externe, reste en service jusqu'à ce que le nouveau certificat de serveur soit généré, signé et installé.

Important : Une fois que le certificat du serveur est modifié, le concentrateur de gestion redémarre et toutes les sessions utilisateur sont arrêtées. Les utilisateurs doivent se connecter à nouveau pour continuer à travailler dans l'interface Web.

Procédure

Pour générer un certificat de serveur autosigné XClarity Management Hub, procédez comme suit.

Etape 1. Dans la barre de menus XClarity Management Hub, cliquez sur **Sécurité (⚙) → Certificat de serveur** pour afficher la carte **Régénérer le certificat de serveur auto-signé**.



Etape 2. À partir de la carte **Régénérer le certificat de serveur auto-signé**, renseignez les zones correspondant à la demande.

- Code ISO 3166 à deux lettres du pays ou de la région d'origine à associer à l'organisation de certificat (par exemple, US pour les États-Unis).
- Nom complet de l'État ou de la province à associer au certificat (Californie ou Nouveau-Brunswick, par exemple).
- Nom complet de la ville à associer au certificat (par exemple, San Jose). La valeur ne doit pas comporter plus de 50 caractères.
- Organisation (société) possédant le certificat. Généralement, il s'agit du nom légal d'une entreprise. Celui-ci doit inclure tous les suffixes, tels que Ltd., Inc. ou Corp (par exemple, ACME International Ltd.). Cette valeur ne doit pas comporter plus de 60 caractères.
- (En option) Unité organisationnelle à laquelle appartient le certificat (par exemple, ABC Division). Cette valeur ne doit pas comporter plus de 60 caractères.
- Nom commun du propriétaire du certificat. En général, il s'agit du nom de domaine complet (FQDN) ou de l'adresse IP du serveur qui utilise le certificat (par exemple, `www.domainname.com` ou `192.0.2.0`). Cette valeur ne doit pas comporter plus de 63 caractères.

  Remarque : Cet attribut n'a actuellement aucun impact sur le certificat.
- Date et heure auxquelles le certificat du serveur n'est plus valide.

  Remarque : Ces attributs n'ont actuellement aucun impact sur le certificat.

Remarque : Vous ne pouvez pas modifier les autres noms de sujet lorsque vous regénérez le certificat du serveur.

Etape 3. Cliquez sur **Régénérer le certificat de serveur auto-signé** pour régénérer le certificat auto-signé, puis cliquez sur **Régénérer un certificat** pour confirmer.Le concentrateur de gestion redémarre et toutes les sessions utilisateur établies sont arrêtées.

Etape 4. Connectez-vous à nouveau au navigateur Web.

Après avoir terminé

Sur la carte Régénérer le certificat de serveur auto-signé, vous pouvez effectuer les actions suivantes.

- Enregistrez le certificat de serveur actuel sur votre système local au format PEM en cliquant **Enregistrer le certificat**.
- Regénérez le certificat du serveur à l'aide du paramètre par défaut en cliquant sur **Réinitialiser le certificat**. Lorsque vous y êtes invité, appuyez sur Ctrl + F5 pour actualiser le navigateur, puis établissez à nouveau votre connexion à l'interface Web.

Installation d'un certificat de serveur fiable et signé de manière externe pour XClarity Management Hub pour les appareils clients Edge

Vous pouvez choisir d'utiliser un certificat de serveur sécurisé qui a été signé par une autorité de certification privée ou commerciale (CA). Pour utiliser un certificat de serveur à signature externe, générez une demande de signature de certificat (CSR), puis importez le certificat de serveur qui en résulte afin de remplacer le certificat de serveur existant.

Avant de commencer

Attention :

- Si vous installez le Lenovo XClarity Management Hub certificat du serveur signé en externe à l'aide d'un nouveau certificat racine CA, XClarity Management Hub perd sa connexion aux appareils gérés et vous devez gérer ces derniers à nouveau. Si vous installez le Lenovo XClarity Management Hub certificat du serveur signé en externe sans modifier le certificat racine CA (par exemple, lorsque le certificat a expiré), il n'est pas nécessaire de gérer à nouveau les appareils.
- Si de nouveaux périphériques sont ajoutés après la génération CSR et avant l'importation du certificat de serveur signé, ces périphériques doivent être redémarrés afin de recevoir le nouveau certificat de serveur.

À propos de cette tâche

Il est recommandé de toujours utiliser des certificats signés v3.

Le certificat de serveur à signature externe doit être créé à partir de la dernière demande de signature de certificat générée, à l'aide du bouton **Générer un fichier CSR**.

Le contenu du certificat de serveur à signature externe doit être un groupe de certificats qui contient la chaîne de signature de l'autorité de certification entière, y compris le certificat racine de l'autorité de certification, tous les certificats intermédiaires et le certificat du serveur.

Si le nouveau certificat de serveur n'a pas été signé par un tiers de confiance, la prochaine fois que vous vous connecterez à Lenovo XClarity Management Hub, votre navigateur Web affichera un message de sécurité et une boîte de dialogue vous invitant à accepter le nouveau certificat dans le navigateur. Pour éviter les messages de sécurité, vous pouvez importer un certificat de serveur dans la liste de votre navigateur Web de certificats sécurisés (voir Importation du certificat de serveur dans un navigateur Web pour Lenovo XClarity Management Hub pour les appareils clients Edge).

XClarity Management Hub démarre à l'aide du nouveau certificat du serveur sans interrompre la session en cours. De nouvelles sessions sont établies avec le nouveau certificat. Pour utiliser le nouveau certificat en cours d'utilisation, redémarrez votre navigateur Web.

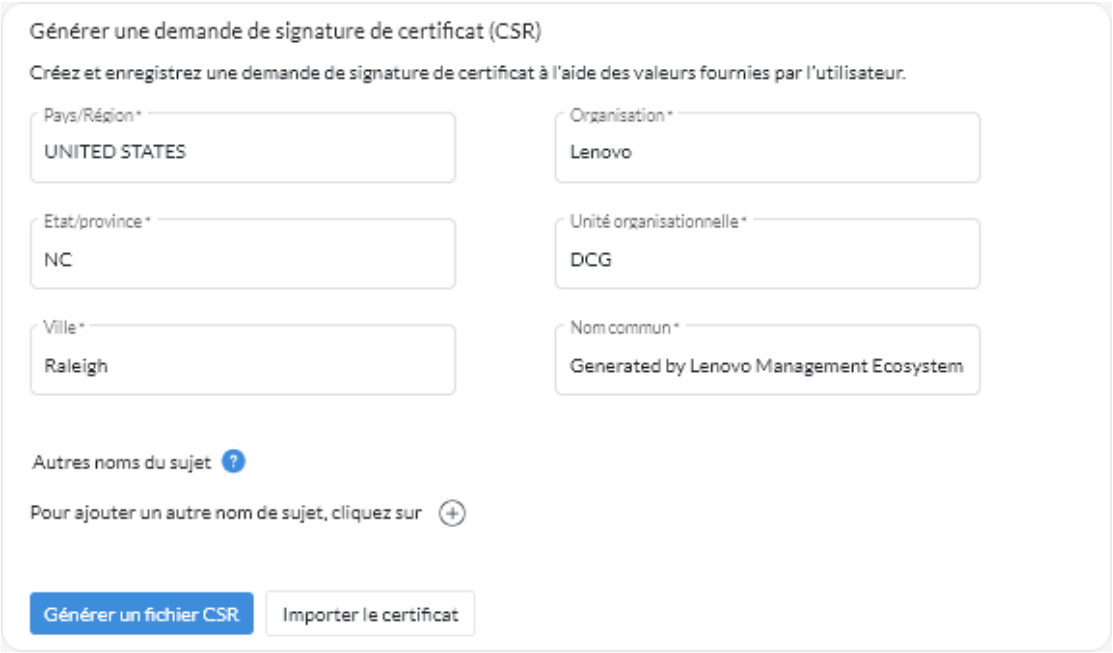
Important : Lorsque le certificat du serveur est modifié, toutes les sessions utilisateur établies doivent accepter le nouveau certificat en appuyant sur Ctrl+F5 pour actualiser le navigateur Web, puis en rétablissant la connexion à XClarity Management Hub.

Procédure

Pour générer et installer un certificat de serveur à signature externe, procédez comme suit.

Etape 1. Créez une demande de signature de certificat et enregistrez le fichier sur votre système local.

1. Dans la barre de menus XClarity Management Hub, cliquez sur **Sécurité** ( ) → **Certificat de serveur** pour afficher la carte Générer une demande de signature de certificat.



2. À partir de la carte Générer une demande de signature de certificat, renseignez les zones correspondant à la demande.
   - Code ISO 3166 à deux lettres du pays ou de la région d'origine associée à l'organisation de certificat (par exemple, US pour les États-Unis).
   - Nom complet de l'État ou de la province à associer au certificat (Californie ou Nouveau-Brunswick, par exemple).
   - Nom complet de la ville à associer au certificat (par exemple, San Jose). La valeur ne doit pas comporter plus de 50 caractères.
   - Organisation (société) possédant le certificat. Généralement, il s'agit du nom légal d'une entreprise. Celui-ci doit inclure tous les suffixes, tels que Ltd., Inc. ou Corp (par exemple, ACME International Ltd.). Cette valeur ne doit pas comporter plus de 60 caractères.
   - (En option) Unité organisationnelle à laquelle appartient le certificat (par exemple, ABC Division). Cette valeur ne doit pas comporter plus de 60 caractères.
   - Nom commun du propriétaire du certificat. Il doit s'agit du nom d'hôte du serveur qui utilise le certificat. Cette valeur ne doit pas comporter plus de 63 caractères.

Remarque : Cet attribut n'a actuellement aucun impact sur le certificat.

- (Facultatif) Les autres noms du sujet qui sont personnalisés, supprimés et ajoutés à l'extension X.509 « subjectAltName » lorsque le fichier CSR est généré. Les autres noms du sujet spécifiés sont validés (sur la base du type spécifié) et ajoutés au CSR seulement après la génération du CSR. Par défaut, XClarity Management Hub définit automatiquement les autres noms de sujet (SAN) pour la CSR basé sur l'adresse IP et le nom d'hôte qui sont reconnus par les interfaces réseau du système d'exploitation XClarity Management Hub invité.

  Attention : Les autres noms du sujet doivent inclure le nom de domaine complet (FQDN) ou l'adresse IP du concentrateur de gestion. En outre, le nom de sujet doit être défini sur le FQDN du concentrateur de gestion. Vérifiez que ces zones obligatoires sont bien présentes et corrigez-les avant de commencer le processus de CSR afin de vérifier que le certificat résultant est terminé. Les données manquantes du certificat peuvent entraîner des connexions qui ne sont pas fiables lors de la tentative de connexion du concentrateur de gestion à Lenovo XClarity Orchestrator.

  Le nom que vous spécifiez doit être valide pour le type sélectionné.
  - **DNS** (utilisez le FQDN, par exemple, hostname.labs.company.com)
  - **Adresse IP** (par exemple, 192.0.2.0)
  - **e-mail** (par exemple, example@company.com)

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

Etape 3. Importez le certificat du serveur à signature externe et le certificat de l'autorité de certification dans XClarity Management Hub, puis remplacez le certificat du serveur actuel.

1. Sur la carte Générer une demande de signature de certificat (CSR), cliquez sur **Importer le certificat** pour afficher la boîte de dialogue Importer un certificat.
2. Copiez et collez le certificat du serveur et le certificat de l'autorité de certification au format PEM. Vous devez fournir la totalité de la chaîne de certificats, en commençant par le certificat du serveur et en finissant par le certificat racine de l'autorité de certification.
3. Cliquez sur **Importer** pour stocker le certificat du serveur dans le fichier de clés certifiées XClarity Management Hub.

Etape 4. Acceptez le nouveau certificat en appuyant sur Ctrl + F5 pour actualiser le navigateur, puis en recréant votre connexion à l'interface Web. Cette opération doit être effectuée par toutes les sessions utilisateur établies.

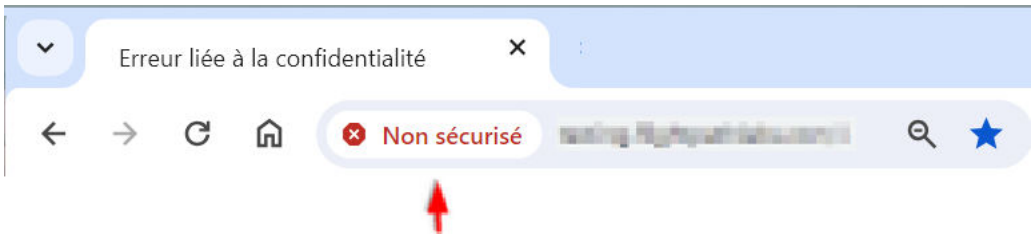
Importation du certificat de serveur dans un navigateur Web pour Lenovo XClarity Management Hub pour les appareils clients Edge

Vous pouvez enregistrer une copie du certificat du serveur en cours, au format PEM, sur votre système local. Vous pouvez ensuite importer le certificat dans la liste de certificats sécurisés de votre navigateur Web ou dans d'autres applications pour éviter les messages d'avertissement de sécurité de votre navigateur Web lorsque vous accédez au Lenovo XClarity Management Hub.

Procédure

Pour importer le certificat de serveur dans votre navigateur Web, procédez comme suit.

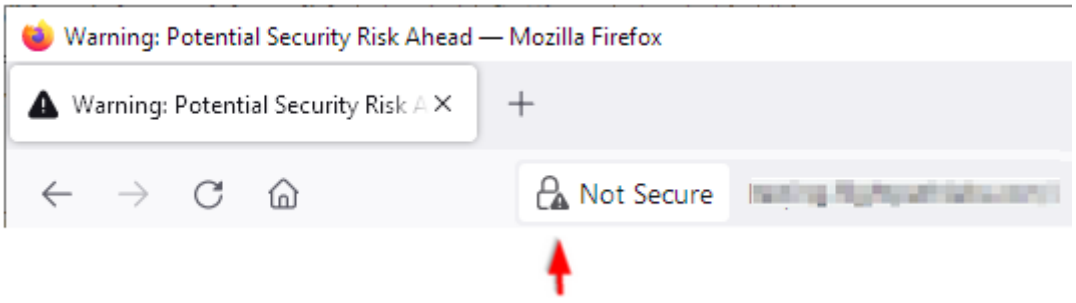
- **Chrome**
  1. Exportez le certificat du serveur Lenovo XClarity Management Hub.
     a. Cliquez sur l'icône d'avertissement « Non sécurisé » dans la barre d'adresses supérieure, par exemple :



b. Cliquez sur **Le certificat n'est pas valide** pour afficher la boîte de dialogue Certificat.
c. Cliquez sur l'onglet **Détails**.
d. Cliquez sur **Exporter**.
e. Indiquez le nom et l'emplacement du fichier de certificat, puis **Enregistrer** pour exporter le certificat.
f. Fermez la boîte de dialogue Visionneuse de certificats.

2. Importez le certificat de serveur Lenovo XClarity Management Hub dans la liste des certificats d'autorité racine de confiance pour votre navigateur.
   a. Dans votre navigateur Chrome, cliquez sur les trois points dans l'angle supérieur droit de la fenêtre, puis cliquez sur **Paramètres** pour ouvrir la page Paramètres.
   b. Cliquez sur **Confidentialité et sécurité**, puis sur **Sécurité** pour afficher la page Sécurité.
   c. Faites défiler l'écran dans la section **Avancé**, puis cliquez sur **Gérer les certificats de l'appareil**.
   d. Cliquez sur **Importer**, puis sur **Suivant**.
   e. Sélectionnez le fichier de certificat que vous avez précédemment exporté et cliquez sur **Suivant**.
   f. Choisissez l'emplacement de stockage du certificat, puis cliquez sur **Suivant**.
   g. Cliquez sur **Terminer**.
   h. Fermez et rouvrez le navigateur Chrome, puis ouvrez Lenovo XClarity Management Hub.

- **Firefox**
  1. Exportez le certificat du serveur Lenovo XClarity Management Hub.
     a. Cliquez sur l'icône d'avertissement « Non sécurisé » dans la barre d'adresses supérieure, par exemple :



     b. Cliquez sur **Connexion non sécurisée**, puis sur **Informations complémentaires**.
     c. Cliquez sur **Afficher le certificat**.
     d. Faites défiler vers le bas, jusqu'à la section **Divers**, puis cliquez sur le lien **PEM (cert)** afin d'enregistrer le fichier sur le système local.
  2. Importez le certificat de serveur Lenovo XClarity Management Hub dans la liste des certificats d'autorité racine de confiance pour votre navigateur.
     a. Ouvrez le navigateur et cliquez sur **Outils → Paramètres**, puis cliquez sur **Confidentialité et sécurité**.
     b. Faites défiler jusqu'à la section **Sécurité**.

c. Cliquez sur **Afficher les certificats** pour afficher la boîte de dialogue Gestionnaire de certificats.
d. Cliquez sur l'onglet **Vos certificats**.
e. Cliquez sur **Importer** et accédez à l'emplacement où le certificat a été téléchargé.
f. Sélectionnez le certificat, puis cliquez sur **Ouvrir**.
g. Fermez la boîte de dialogue Gestionnaire de certificats.

Connexion de XClarity Management Hub pour les appareils clients Edge à XClarity Orchestrator

Après votre inscription (connexion) de Lenovo XClarity Management Hub avec Lenovo XClarity Orchestrator, vous pouvez commencer la gestion et la surveillance de vos appareils.

Avant de commencer

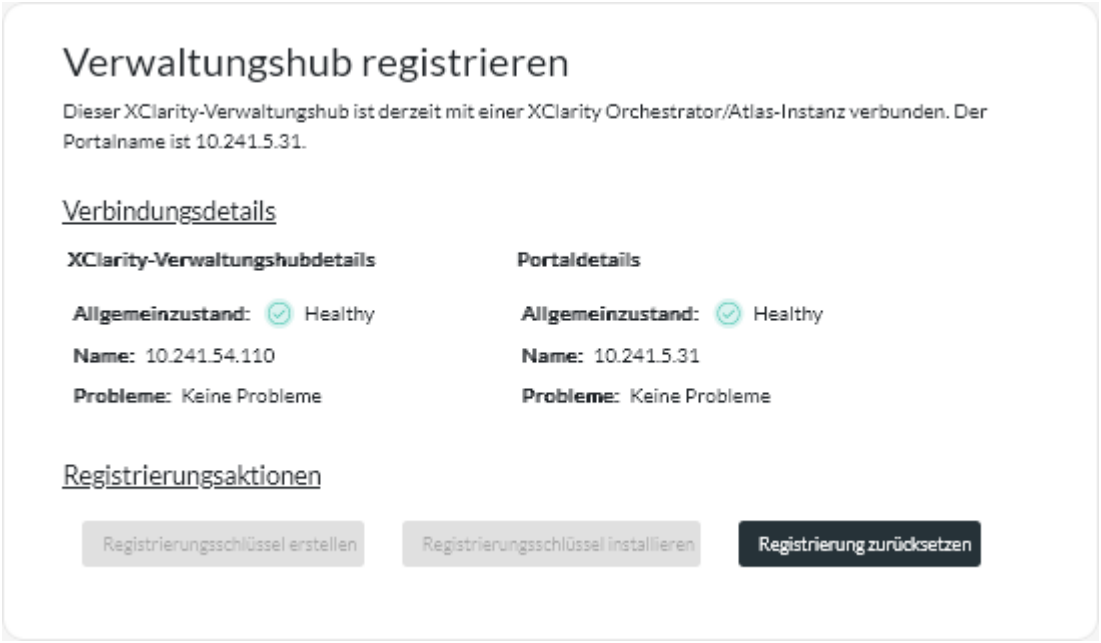
Assurez-vous que le XClarity Management Hub est accessible sur le réseau depuis XClarity Orchestrator et que XClarity Orchestrator est accessible sur le réseau depuis XClarity Management Hub.

Procédure

Pour inscrire XClarity Management Hub, procédez comme suit.

Etape 1. Créez la clé d'inscription du concentrateur de gestion.

1. Dans la barre de menus du Management Hub, cliquez sur **Inscription** pour afficher la page Inscription.

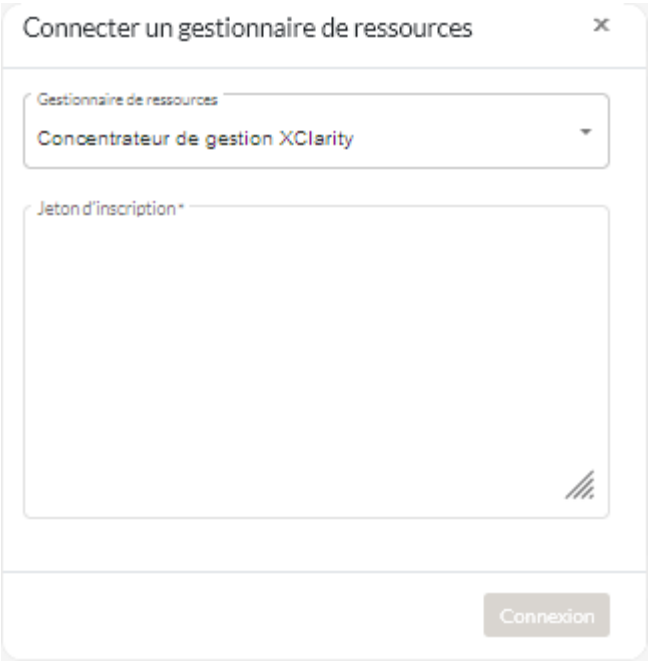


2. Cliquez sur **Créer une clé d'inscription**.
3. Cliquez sur **Copier dans le presse-papiers** pour copier la clé d'inscription, puis fermez la boîte de dialogue.

Etape 2. Ajoutez la clé d'inscription du concentrateur de gestion à XClarity Orchestrator.

1. Dans la barre de menus de XClarity Orchestrator, cliquez sur **Ressources** (⚙) → **Gestionnaires de ressources** pour afficher la carte Gestionnaires de ressources.

2. Cliquez sur l'icône **Se connecter** ( ) pour afficher gestionnaire de ressources. La boîte de dialogue Connecter un gestionnaire de ressources.



3. Sélectionnez **XClarity Management Hub** en tant que gestionnaire de ressources.
4. Copiez la clé d'inscription dans la zone **Jeton d'inscription**.
5. Cliquez sur **Connecter** pour afficher la boîte de dialogue Connecter un gestionnaire de ressources qui contient la clé d'inscription du XClarity Orchestrator.
6. Cliquez sur **Copier dans le presse-papiers** pour copier la clé d'inscription, puis fermez la boîte de dialogue.

Etape 3. Ajoutez la clé d'inscription XClarity Orchestrator au concentrateur de gestion.

1. Dans la barre de menus du Management Hub, cliquez sur **Inscription** pour afficher la page Inscription.
2. Cliquez sur **Installer une clé d'inscription**.
3. Copiez la clé d'inscription dans la zone **Jeton d'inscription**.
4. Cliquez sur **Connecter**.

Après avoir terminé

- Gérez des appareils à l'aide du concentrateur de gestion (voir Gestion d'appareils clients ThinkEdge dans la documentation en ligne de XClarity Orchestrator).
- Supprimez la clé d'inscription du concentrateur de gestion actuel en cliquant sur **Réinitialiser l'inscription**.

Chapitre 3. Désinstallation de XClarity Management Hub pour les appareils clients Edge

Procédez comme suit pour désinstaller un dispositif virtuel XClarity Management Hub.

Procédure

Pour désinstaller le dispositif virtuel XClarity Management Hub, procédez comme suit.

Etape 1. Annulez la gestion de tous les appareils actuellement gérés par le XClarity Management Hub.

Etape 2. Désinstallez le XClarity Management Hub, selon le système d'exploitation.

- **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**.

Lenovo