Lenovo

XClarity Controller 3
Guide d’utilisation

Remarque : Avant d'utiliser le présent document, prenez connaissance des informations générales figurant à la section Annexe B « Consignes » à la page 187.

Première édition (Octobre 2024)

Table des matières

Chapitre 1. Introduction

Lenovo XClarity Controller 3 (XCC3) est un contrôleur de gestion nouvelle génération destiné aux serveurs Lenovo ThinkSystem.

Le contrôleur consolide les fonctionnalités de processeur de service, de Super I/O, de contrôleur vidéo et de présence à distance dans une seule puce sur la carte mère du serveur. Il propose les fonctions suivantes :

- Choix entre une connexion Ethernet dédiée ou partagée pour la gestion des systèmes
- Prise en charge de HTML5
- Prise en charge de l'accès via XClarity Mobile
- XClarity Provisioning Manager
- Configuration à distance à l'aide de l'interface de ligne de commande XClarity Essentials ou XClarity Controller.
- Possibilité pour les applications et les outils d'accéder à XClarity Controller en local ou à distance
- Fonctions d'intervention à distance améliorées.
- Prise en charge de l'API REST (schéma Redfish) pour des services et des applications logicielles Web supplémentaires.

Remarques :

- XClarity Controller prend en charge actuellement la spécification d'API Redfish Scalable Platforms Management 1.16.0 et le schéma 2022.2
- Dans l'interface Web XClarity Controller, BMC est utilisé en référence à XCC.
- Il se peut qu'un port réseau dédié à la gestion des systèmes ne soit pas disponible sur certains serveurs ThinkSystem ; pour ces serveurs, l'accès à XClarity Controller est uniquement disponible via un port réseau qui est partagé avec le système d'exploitation du serveur.

Ce document explique comment utiliser les fonctions de XClarity Controller sur un serveur ThinkSystem. XClarity Controller fonctionne avec XClarity Provisioning Manager et UEFI pour fournir une fonction de gestion des systèmes pour les serveurs ThinkSystem.

Pour vérifier la disponibilité de mises à jour du microprogramme, procédez comme suit.

Remarque : La première fois que vous accédez au portail du support, vous devez choisir la catégorie du produit, la famille du produit et les numéros de modèle de votre serveur. La prochaine fois que vous accédez au portail de support, les produits sélectionnés initialement sont préchargés par le site Web et seuls les liens correspondant à vos produits sont affichés. Pour modifier ou ajouter des éléments à votre liste de produits, cliquez sur le lien **Gérer mes listes de produits**. Le site Web est régulièrement mis à jour. La procédure de recherche des microprogrammes et des publications peut être légèrement différente de celle qui est décrite dans le présent document.

1. Accédez à http://datacentersupport.lenovo.com.
2. Sous **Support**, sélectionnez **Data Center (Centre de données)**.
3. Lorsque le contenu est chargé, sélectionnez **Servers (Serveurs)**.
4. Sous **Select Series (Sélectionner une série)**, sélectionnez d'abord la gamme matérielle du serveur, puis sous **Select SubSeries (Sélectionner une sous-série)**, sélectionnez la sous-série du produit serveur particulier ; enfin, sous **Select Machine Type (Sélectionner un type de machine)**, sélectionnez le type de machine.

Fonctionnalités de niveau standard et Premier de XClarity Controller

XClarity Controller se décline dans plusieurs niveaux de fonctionnalités : standard et Premier. Pour plus d'information sur le niveau XClarity Controller installé sur votre serveur, consultez la documentation de votre serveur. Tous les niveaux offrent les fonctionnalités suivantes :

- Accès à distance et gestion en continu de votre serveur
- Gestion à distance indépendante du statut du serveur géré
- Contrôle à distance du matériel et des systèmes d'exploitation

Fonctionnalités de niveau standard de XClarity Controller

Les fonctionnalités de niveau standard de XClarity Controller sont les suivantes :

Interfaces de gestion des normes de l'industrie

- Interface IPMI 2.0
- Redfish
- DCMI 1.5
- SNMPv3

Autres interfaces de gestion

- Web
- SSH CLI
- USB panneau frontal - Panneau opérateur virtuel via appareil mobile

Contrôle d'alimentation/de réinitialisation

- Mise sous tension
- Arrêt immédiat/graduel
- Contrôle d'alimentation planifié
- Réinitialisation du système
- Contrôle de l'ordre d'amorçage

Journaux des événements

- IPMI SEL
- Journal en caractères lisibles par l'utilisateur
- Journal d'audit
- Mini-journal

Surveillance environnementale

- Surveillance sans agent
- Surveillance de détecteur
- Contrôle de ventilateur
- Contrôle des voyants
- Erreurs de jeu de circuits (Caterr, IERR, etc.)
- Indication de l'état d'intégrité du système

- Surveillance des performances OOB pour adaptateurs d'E-S
- Affichage et exportation d'inventaire

RAS

- NMI virtuel
- Récupération du microprogramme automatique
- Promotion automatisée du microprogramme de sauvegarde
- Horloge de surveillance POST
- Horloge de surveillance du chargeur SE
- Programme de surveillance du système d'exploitation
- Capture d’écran bleu (défaillance du SE, dans FFDC)
- Outils de diagnostic intégrés
- Appel vers Lenovo

Configuration réseau

- IPv4
- IPv6
- Adresse IP, masque de sous-réseau, passerelle
- Modes d'affectation de l'adresse IP
- Nom d'hôte
- Adresse MAC programmable
- Sélection MAC double (si fonction prise en charge par le matériel serveur)
- Réaffectations de port réseau
- Marquage VLAN

Protocoles réseau

- DHCP
- DNS (Directory Name System)
- DDNS
- HTTP/HTTPS
- SNMPv3
- SSL
- SSH
- SMTP
- Client LDAP
- NTP (Network Time Protocol)
- SSDP
- LLDP

Alertes

- Interruptions PET
- Interruptions SNMP v1, v2c et v3

- E-mail
- Abonnements aux notifications Redfish

Présence à distance

- Disque distant sur carte (RDOC)

Redirection série

- SOL IPMI
- Configuration du port série, dont autorité et vitesse
- Tampon de console série (120)

Sécurité

- Processeur non hôte CRTM
- Mises à jour du microprogramme signées numériquement
- Role Based Access Control (RBAC)
- Comptes utilisateur locaux
- Comptes utilisateurs LDAP/AD
- Annulation sécurisée du microprogramme
- NIST SP 800-131a
- Détection d’intrusion de châssis (si prise en charge par le matériel du serveur)
- Protocoles sécurisés et chiffrés uniquement activés
- Journalisation des audits des modifications de configuration et des actions du serveur
- Authentification par clé publique
- Retrait/réaffectation de système (RTD/ERTD)
- Prise en charge de la technologie PFR
- FIPS 140-3
- Modes de sécurité et tableau de bord de sécurité
- Stockage sécurisé des mots de passe

Gestion de l'alimentation

- Compteur d'alimentation en temps réel

Features on Demand (FoD)

- Référentiel des clés d’activation

Déploiement et configuration

- Configuration à distance
- Relais du système d’exploitation
- Déploiement intégré, outils de configuration et modules de pilotes
- Sauvegarde et restauration de la configuration
- Taille RDOC étendue (avec carte MicroSD)
- Profils thermiques configurables

Mises à jour du microprogramme

- Mise à jour gratuite d'agent
- Mise à jour distante

Fonctionnalités de niveau Premier de XClarity Controller

Les fonctionnalités de niveau Premier de XClarity Controller sont les suivantes :

Toutes les « Fonctionnalités de niveau standard de XClarity Controller » **à la page 2****.**

Journaux des événements

- Journal de remplacement de composant

RAS

- Capture d'amorçage
- Capture de vidéo de panne

Alertes

- Syslog

Présence à distance

- KVM distant
- Montage de fichiers ISO/IMG de client local
- Contrôle qualité/bande passante
- Montage de supports virtuels de fichiers ISO/IMG distants HTTP, Samba et NFS

Redirection série

- Redirection série via SSH-CLI

Sécurité

- Authentification unique
- Security Key Lifecycle Manager (SKLM/KMIP)
- Blocage d'adresse IP
- Mode de sécurité Enterprise Strict (conforme à CNSA)
- Protection du système

Gestion de l'alimentation

- Plafonnement énergétique
- Surveillance des performances OOB - Mesures des performances du système
- Graphiques en temps réel
- Graphiques de température

Déploiement et configuration

- Déploiement du SE distant

Mises à jour du microprogramme

- Synchronisation avec le référentiel

- Mise à jour par lot du microprogramme du module système
- Restauration du microprogramme depuis le référentiel local dans une carte MicroSD

Mise à niveau de XClarity Controller

Si votre serveur a été fourni avec le niveau standard de la fonctionnalité de microprogramme XClarity Controller, vous pouvez peut-être mettre à niveau la fonctionnalité XClarity Controller sur votre serveur. Pour plus d'informations sur les mises à niveau disponibles et les modalités de commande, voir Chapitre 9 « Gestion des licences » à la page 89.

Exigences relatives au navigateur Web et au système d'exploitation

Les informations de cette rubrique vous indiquent comment afficher la liste des navigateurs, de suites de chiffrement et des systèmes d'exploitation pris en charge pour votre serveur.

L'interface Web de XClarity Controller requiert l'un des navigateurs Web suivants :

- Chrome 64.0 ou supérieur (64.0 ou supérieur pour console distante)
- Firefox ESR 78.0 ou supérieur
- Microsoft Edge 79.0 ou supérieur
- Safari 12.0 ou supérieur (iOS 7 ou supérieur et OS X)

Remarque : La prise en charge de la fonctionnalité de la console distante n'est pas disponible via le navigateur sur les systèmes d'exploitation d'appareil mobile.

Les navigateurs précédemment indiqués sont ceux qui sont actuellement pris en charge par le microprogramme XClarity Controller. Le microprogramme XClarity Controller peut faire l'objet d'améliorations régulières pour inclure la prise en charge d'autres navigateurs.

Selon la version du microprogramme dans XClarity Controller, la prise en charge du navigateur Web peut être différente de celle des navigateurs répertoriés dans cette section. Pour afficher la liste des navigateurs pris en charge pour le microprogramme actuellement dans XClarity Controller, cliquez sur la liste de menu **Navigateurs pris en charge** depuis la page de connexion XClarity Controller.

Pour une sécurité maximale, seuls les chiffrements puissants sont désormais pris en charge pour l'utilisation de HTTPS. Lors de l'utilisation de HTTPS, la combinaison de votre système d'exploitation client et de votre navigateur doit prendre en charge l'un des algorithmes de cryptographie suivants :

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_8_SHA256
- TLS_AES_128_CCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

Remarque : Le cache de votre navigateur Internet stocke les informations relatives aux pages Web que vous visitez afin qu'elles se chargent plus rapidement plus tard. Après une mise à jour flash du microprogramme XClarity Controller, il se peut que votre navigateur continue à utiliser les informations du cache au lieu de les extraire de XClarity Controller. Il est donc recommandé après une telle mise à jour de vider le cache afin de garantir un affichage correct des pages Web issues de XClarity Controller.

Support multilingue

Les informations de cette rubrique vous indiquent comment afficher la liste des langues prises en charge par XClarity Controller.

Par défaut, la langue choisie pour l'interface Web de XClarity Controller est l'anglais. L'interface peut être affichée dans plusieurs langues. Ces langues sont les suivantes :

- Français
- Allemand
- Italien
- Japonais
- Coréen
- Portugais (Brésil)
- Russe
- Chinois simplifié
- Espagnol (international)
- Chinois traditionnel

Pour définir votre langue de préférence, cliquez sur la flèche en regard de la langue sélectionnée. Un menu déroulant vous permet alors de choisir votre langue préférée.

Les chaînes de texte générées par le microprogramme XClarity Controller sont affichées dans la langue dictées par le navigateur. Si le navigateur indique une autre langue que l'une de celles ci-dessus, le texte s'affiche en anglais. En outre, toute chaîne de texte qui est affichée par le microprogramme XClarity Controller, mais qui n'est pas générée par XClarity Controller (par exemple les messages générés par UEFI, les adaptateurs PCIe, etc.)… sont affichés en anglais.

L'entrée de texte dans une autre langue que l'anglais, tel que le **message Trespass** n'est pas encore pris en charge. Seul le texte tapé en anglais est pris en charge.

Introduction aux MIB

Les informations de cette rubrique vous permettent d'accéder aux bases d'informations de gestion (MIB).

Les bases d'informations de gestion des SNMP peuvent être téléchargées à partir de https://support.lenovo.com/ (recherche par type de machine sur le portail). Les quatre MIB suivantes sont répertoriées.

- La **MIB SMI** décrit la structure des informations de gestion pour le groupe de centre de données Lenovo.
- La **MIB produit** décrit l'identificateur d'objet pour les produits Lenovo.
- La **MIB XCC** fournit les informations d'inventaire et de surveillance pour Lenovo XClarity Controller.
- La **MIB d'alerte XCC** définit des alertes pour les conditions d'alerte détectées par Lenovo XClarity Controller.

Remarque : L'ordre d'importation des quatre MIB est **MIB SMI** → **MIB produit** → **MIB XCC** → **MIB d'alerte XCC**.

Consignes utilisées dans ce document

Les informations de cette rubrique vous permettent de comprendre les notices qui sont utilisées dans ce document.

Les mentions suivantes sont utilisées dans la documentation :

- **Remarque :** Contient des instructions et conseils importants.
- **Important :** Fournit des informations ou des conseils pouvant vous aider à éviter des problèmes.
- **Avertissement :** Indique la présence d'un risque pouvant occasionner des dommages aux programmes, aux appareils ou aux données. Ce type de consigne est placé avant l'instruction ou la situation à laquelle elle se rapporte.

Chapitre 2. Ouverture et utilisation de l'interface Web de XClarity Controller

Cette rubrique décrit les procédures de connexion et les actions que vous pouvez effectuer à partir de l'interface Web de XClarity Controller.

XClarity Controller combine les fonctions de processeur de support, de contrôleur vidéo et une fonction de présence à distance dans une seule puce. Vous devez tout d'abord vous connecter à l'aide de l'interface Web XClarity Controller afin d'accéder à XClarity Controller à distance. Ce chapitre décrit les procédures de connexion et les actions que vous pouvez effectuer à partir de l'interface Web de XClarity Controller.

Accès à l'interface Web de XClarity Controller

Les informations de cette rubrique vous expliquent comment accéder à l'interface Web de XClarity Controller.

XClarity Controller prend en charge l'adressage IPv4 statique et DHCP (Dynamic Host Configuration Protocol). L'adresse IPv4 statique par défaut affectée à XClarity Controller est 192.168.70.125. XClarity Controller est configuré initialement pour tenter d'obtenir une adresse depuis un serveur DHCP, et s'il n'y parvient pas, il utilise alors l'adresse IPv4 statique.

XClarity Controller prend également en charge IPv6, mais il ne dispose pas d'une adresse IP IPv6 statique fixe par défaut. Pour un premier accès à XClarity Controller dans un environnement IPv6, vous pouvez utiliser l'adresse IP IPv4 ou l'adresse IPv6 de type lien local. XClarity Controller génère une adresse IPv6 unique de type lien local, en utilisant l'adresse MAC IEEE 802 par l'insertion de deux octets, avec les valeurs hexadécimales 0xFF et 0xFE au milieu de l'adresse MAC sur 48 bits, comme décrit dans RFC4291 et en inversant le 2e bit à la droite du premier octet de l'adresse MAC. Par exemple, si l'adresse MAC est 08-94-ef-2f-28-af, l'adresse de type lien local est :
`fe80::0a94:efff:fe2f:28af`

Lorsque vous accédez à XClarity Controller, les conditions IPv6 suivantes sont définies par défaut :

- La configuration d'adresse IPv6 automatique est activée.
- La configuration d'adresse IP statique IPv6 est désactivée.
- DHCPv6 est activé.
- L'autoconfiguration sans état est activée.

XClarity Controller permet de choisir entre l'utilisation d'une connexion réseau de gestion des systèmes **dédiée** (si applicable) ou **partagée** avec le serveur. La connexion par défaut pour les serveurs montés en armoire et au format tour utilise le connecteur réseau de gestion des systèmes **dédié**.

La connexion réseau dédiée à la gestion des systèmes sur la plupart des serveurs est fournie via un contrôleur distinct de l'interface réseau 1 Go. Cependant, sur certains systèmes, la connexion réseau de gestion des systèmes dédiée peut être fournie avec l'interface NCSI à l'un des ports réseau d'un contrôleur d'interface réseau à plusieurs ports. Dans ce cas, la connexion réseau de gestion des systèmes dédiée est limitée à la vitesse 10/100 de l'interface de bande latérale. Pour plus d'informations et plus de détails sur les limitations relatives à l'implémentation du port de gestion sur votre système, consultez la documentation de votre système.

Remarque : Il se peut qu'un port réseau **dédié** à la gestion des systèmes ne soit pas disponible sur votre serveur. Si votre matériel ne dispose pas d'un port réseau **dédié**, l'option **partagé** est la seule option XClarity Controller disponible.

Configuration de la configuration réseau de XClarity Controller via XClarity Provisioning Manager

Les informations de cette rubrique vous indiquent comment configurer une connexion XClarity Controller via XClarity Provisioning Manager.

Une fois le serveur démarré, vous pouvez utiliser XClarity Provisioning Manager pour configurer la connexion réseau de XClarity Controller. Le serveur hébergeant XClarity Controller doit être connecté à un serveur DHCP ou le réseau du serveur doit être configuré afin d'utiliser l'adresse IP statique de XClarity Controller. Pour configurer la connexion réseau de XClarity Controller à l'aide de Setup Utility, procédez comme suit :

Etape 1. Mettez le serveur sous tension. L'écran d'accueil de ThinkSystem s'affiche.

Remarque : 40 secondes peuvent être nécessaires après la connexion du serveur à une source d'alimentation en courant alternatif, pour que le bouton de mise sous tension devienne actif.

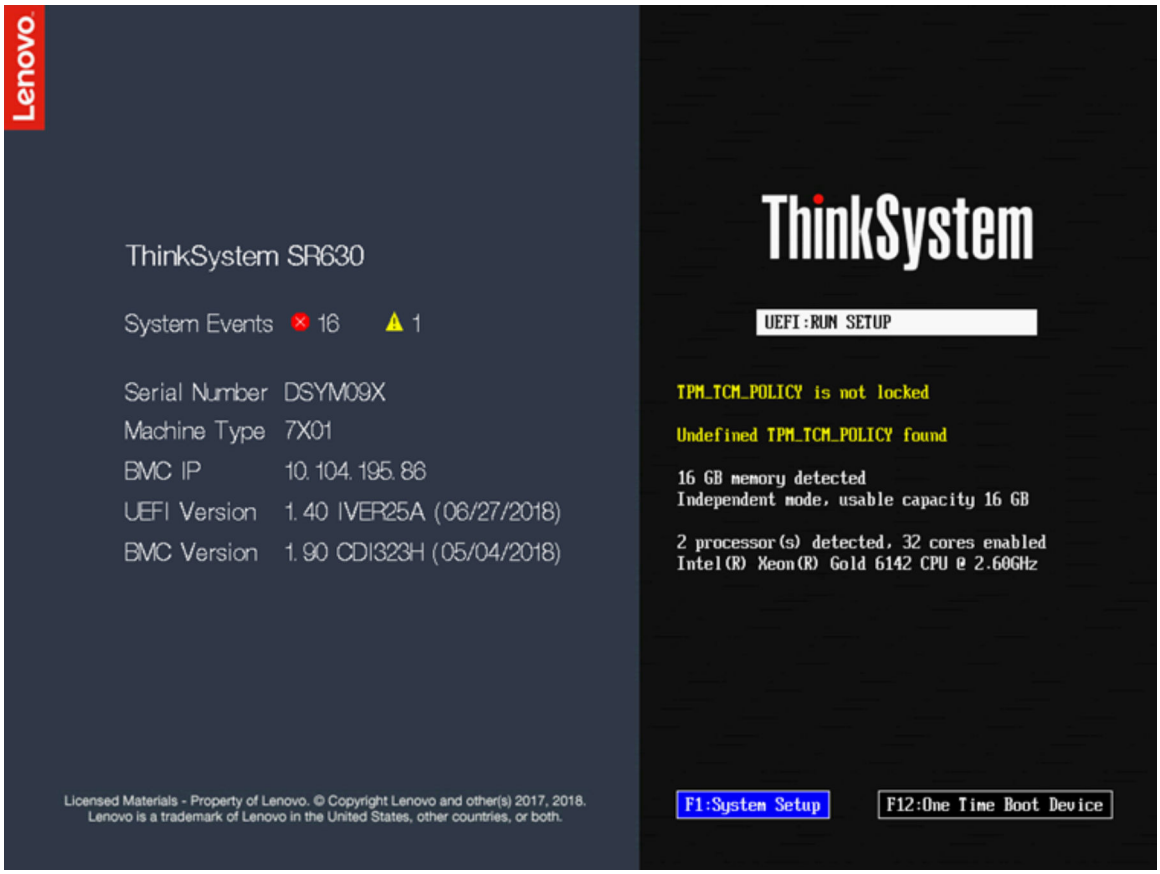


Figure 1. Écran d'accueil de ThinkSystem

Etape 2. Lorsque l'invite `<F1> System Setup` s'affiche, appuyez sur F1. Si vous avez défini un mot de passe à la mise sous tension et un mot de passe administrateur, vous devez entrer le mot de passe administrateur pour accéder à XClarity Provisioning Manager.

Etape 3. Depuis le menu principal de XClarity Provisioning Manager, sélectionnez **Configuration UEFI**.

Etape 4. À l'écran suivant, sélectionnez **Paramètres BMC**, puis cliquez sur **Paramètres réseau**.

Etape 5. Trois options de connexion réseau XClarity Controller sont présentées dans la zone **Contrôle DHCP** :

- Adresse IP statique
- DHCP activé
- DHCP avec rétromigration

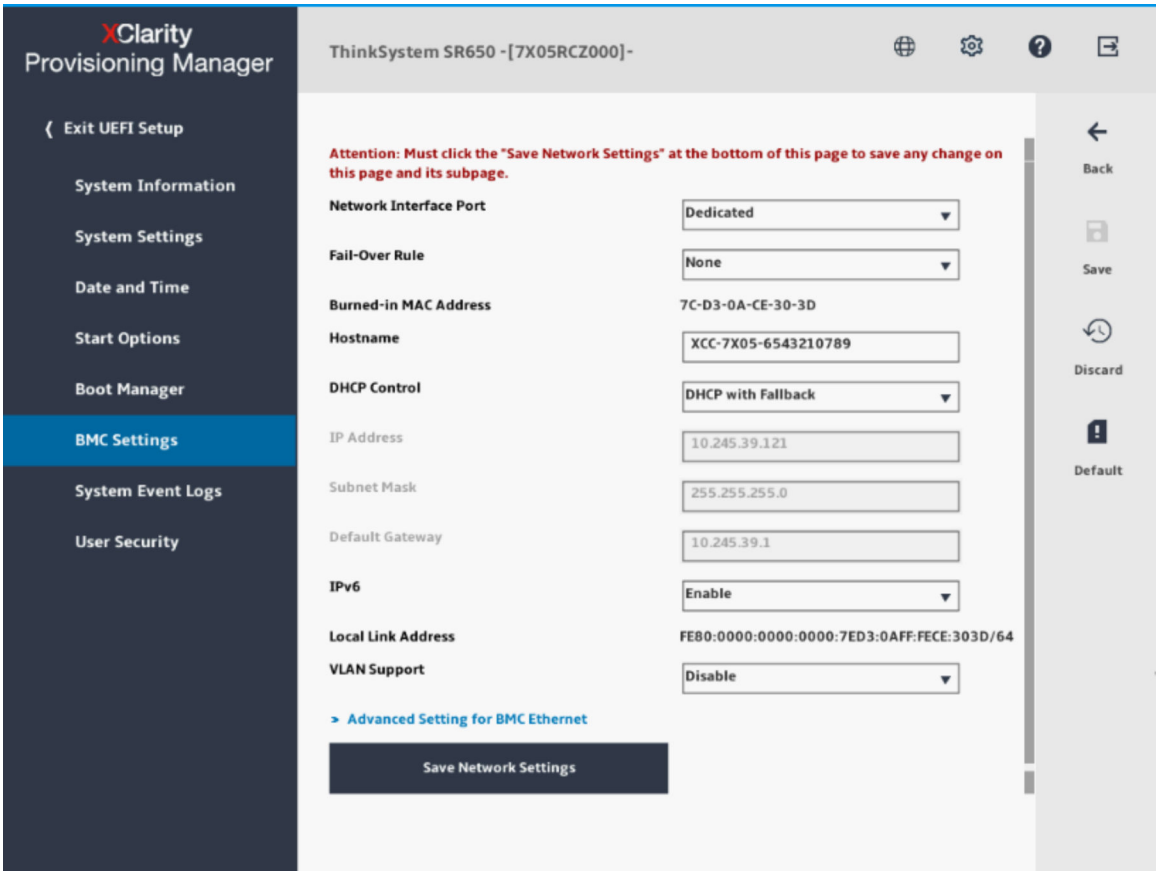


Figure 2. Paramètres de connexion réseau

Etape 6. Sélectionnez l'une des options de connexion réseau.

Etape 7. Si vous choisissez d'utiliser une adresse IP statique, vous devez spécifier l'adresse IP, le masque de sous-réseau, et la passerelle par défaut.

Etape 8. Vous pouvez également utiliser Lenovo XClarity Controller Manager pour sélectionner une connexion réseau dédiée (si votre serveur dispose d'un port réseau dédié) ou une connexion réseau XClarity Controller partagée.

Remarques :

- Il se peut qu'un port réseau dédié à la gestion des systèmes ne soit pas disponible sur votre serveur. Si votre matériel ne dispose pas d'un port réseau dédié, l'option **partagé** est la seule option XClarity Controller disponible. Depuis l'écran **Configuration réseau**, sélectionnez **Dédié**, le cas échéant, ou **Partagé** dans la zone **Port d'interface réseau**.
- Pour identifier l'emplacement des connecteurs Ethernet utilisés par XClarity Controller sur votre serveur, reportez-vous à la documentation accompagnant votre serveur.

Etape 9. Cliquez sur **Enregistrer**.

Etape 10. Quittez XClarity Provisioning Manager.

Remarques :

- Vous devez patienter environ 1 minute pour que les modifications prennent effet avant que le microprogramme du serveur ne soit à nouveau fonctionnel.
- Vous pouvez également configurer la connexion réseau XClarity Controller à travers l'interface Web ou l'interface de ligne de commande de XClarity Controller. Dans l'interface Web de XClarity Controller, des connexions réseau peuvent être configurées en cliquant sur **Configuration BMC** dans le volet de navigation gauche, puis en sélectionnant **Réseau**. Dans l'interface de ligne de commande de XClarity Controller, les connexions réseau sont configurées au moyen de plusieurs commandes qui dépendent de la configuration de votre installation.

Connexion à XClarity Controller

Les informations de cette rubrique vous indiquent comment accéder à XClarity Controller via l'interface Web de XClarity Controller.

Important : XClarity Controller est initialement défini avec le nom d'utilisateur `USERID` et le mot de passe `PASSWORD` (avec un zéro et non la lettre O). Cet utilisateur par défaut dispose d'un accès Superviseur. Pour une sécurité accrue, modifiez ce nom d'utilisateur et ce mot de passe lors de votre configuration initiale. Après avoir effectué la modification, vous ne pouvez pas définir à nouveau `PASSWORD`comme mot de passe.

Pour accéder à XClarity Controller via l'interface Web de XClarity Controller, procédez comme suit :

Etape 1. Ouvrez un navigateur Web. Dans le champ adresse ou URL, tapez `https://` suivi de l'adresse IP ou du nom d'hôte du XClarity Controller auquel vous souhaitez vous connecter.

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

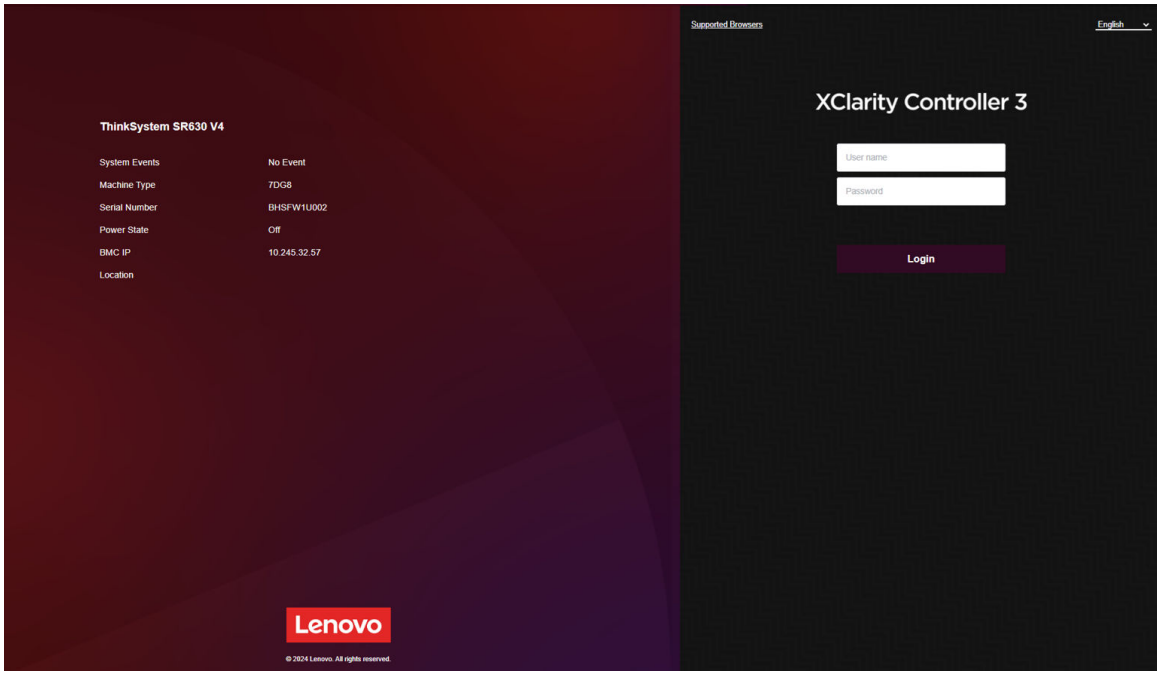


Figure 3. Page de connexion

Etape 3. Entrez ensuite votre nom d'utilisateur et votre mot de passe dans la fenêtre de connexion XClarity Controller. Si vous utilisez XClarity Controller pour la première fois, vous pouvez obtenir le nom d'utilisateur et le mot de passe auprès de votre administrateur système. Toutes les tentatives de connexion sont consignées dans le journal des événements. Selon la façon dont votre

administrateur système a configuré l'ID utilisateur, vous devrez éventuellement entrer un nouveau mot de passe après la connexion.

Etape 4. Cliquez sur **Se connecter** pour démarrer la session. Le navigateur ouvre la page d'accueil de XClarity Controller, comme représentée dans l'illustration suivante. La page d'accueil contient des informations sur le système géré par XClarity Controller, ainsi que des icônes indiquant le nombre d'erreurs critiques 1 et le nombre d'avertissements 1 actuellement présents sur le système.

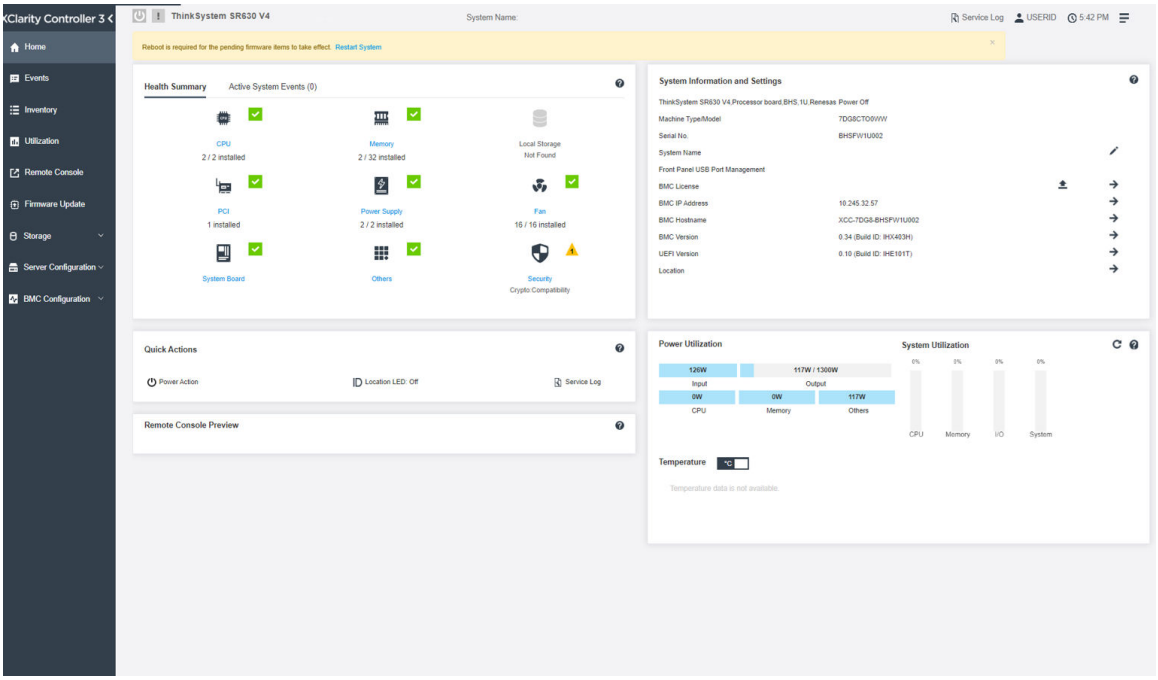


Figure 4. Page d'accueil

La page d'accueil est essentiellement divisée en deux sections. La première section est le panneau de navigation de gauche, qui est un ensemble des rubriques permettant d'effectuer les actions suivantes :

- Surveillance de l'état du serveur
- Configuration du serveur
- Configuration de XClarity Controller ou de BMC
- Mise à jour du microprogramme

La deuxième section concerne les informations graphiques fournies à droite du panneau de navigation. Le format modulaire offre un aperçu rapide de l'état du serveur et des actions rapides pouvant être exécutées.

Description des fonctions de XClarity Controller dans l'interface Web

Les informations de cette rubrique fournissent des explications sur les fonctions de XClarity Controller sur l'interface Web.

Le tableau suivant décrit les fonctions XClarity Controller du panneau de navigation de gauche.

Remarque : Lorsque vous naviguez dans l'interface Web, vous pouvez également cliquer sur l'icône de point d'interrogation pour afficher l'aide en ligne.

Tab	Sélection	Description
Accueil	Récapitulatif de l'intégrité/ Événements système actifs	Affiche l'état actuel des principaux composants matériels du système.
	Informations système et paramètres	Fournit un récapitulatif des informations système communes.
	Actions rapides	Fournit un lien rapide vers le contrôle de l'alimentation et le voyant de localisation, ainsi qu'un bouton pour télécharger les données de maintenance.
	Utilisation de l'alimentation	Fournit un aperçu rapide de l'utilisation actuelle de l'alimentation.
	Aperçu de la console distante	Permet de contrôler le serveur au niveau du système d'exploitation. Vous pouvez afficher et utiliser la console serveur à partir de votre ordinateur. La section de la console distante dans la page d'accueil de XClarity Controller affiche une image écran comportant un bouton Lancer.
Événements	Journal des événements	Fournit une liste historique de l'ensemble des événements de gestion et concernant le matériel.
	Journal d'audit	Fournit un historique des actions des utilisateurs.
	Historique de maintenance	Affiche l'historique relatif aux mises à jour de microprogramme, à la configuration et au remplacement du matériel.
	Destinataires d'alertes **Remarque :** Cette fonctionnalité sera prise en charge dans une future mise à jour.	Permet de gérer les destinataires des événements système. Elle vous permet de configurer chaque destinataire et de gérer les paramètres qui s'appliquent à tous les destinataires d'événement. Vous pouvez également générer un événement test afin de vérifier les paramètre de configuration de notification.
Inventaire		Affiche tous les composants du système, ainsi que leur état et les informations relatives aux clés. Vous pouvez cliquer sur un appareil pour afficher des informations supplémentaires. **Remarque :** Reportez-vous à l'interface Web SMM3 pour plus de détails sur l'état d'alimentation de la solution.
Utilisation		Affiche la température ambiante/des composants, l'utilisation de l'alimentation, les niveaux de tension et les informations relatives à la vitesse du ventilateur du serveur et ses composants, sous forme graphique ou tabulaire.
Console distante		Permet d'accéder à la fonctionnalité de console distante. Vous pouvez utiliser la fonction de support virtuel pour monter les fichiers ISO ou IMG qui se trouvent sur votre système ou dans un emplacement réseau qui est accessible au contrôleur BMC via CIFS, NFS, HTTPS ou SFTP. Le disque monté se présente sous la forme d'une unité de disque USB ou d'un DVD-ROM connecté au serveur.
Mise à jour du microprogramme		• Affiche les niveaux de microprogramme du système. • Permet de mettre à jour le microprogramme XClarity Controller et le microprogramme de serveur. • Permet de mettre à jour le microprogramme de XClarity Controller (XCC) à partir du Référentiel.
Stockage	Détails	Affiche la structure physique et la configuration de stockage des périphériques de stockage

Tab	Sélection	Description
	Configuration RAID	Permet d'afficher ou modifier la configuration RAID en cours, y compris les informations relatives aux disques virtuels et aux dispositifs de stockage physiques.
Configuration du serveur	Adaptateurs	Affiche les informations relatives aux adaptateurs réseau installés et les paramètres qui peuvent être configurés via XClarity Controller.
	Options de démarrage	• Permet de sélectionner le dispositif d'amorçage pour un amorçage unique au prochain redémarrage du serveur. • Permet de modifier le mode d'amorçage et les paramètres d'ordre d'amorçage.
	Règles d'alimentation	• Permet de configurer l'alimentation de secours au cours de l'événement d'une défaillance d'alimentation. • Permet de configurer une stratégie de plafonnement énergétique. • Permet de configurer la stratégie de restauration de l'alimentation. **Remarque :** Reportez-vous à l'interface Web SMM3 pour plus de détails sur l'état d'alimentation de la solution.
	Propriétés du serveur	• Permet de surveiller les propriétés, conditions d'état et paramètres de votre serveur. • Gérez les délais de mise hors tension du serveur. • Permet de créer le message Trespass. Le message Trespass est un message que vous pouvez créer à l'intention des utilisateurs qui se connectent au XClarity Controller.
	Châssis **Remarque :** Cet élément est uniquement disponible sur les nœuds compatibles du châssis D3 V2.	• Affiche les informations sur le châssis. • Redémarrer le nœud ou simulez la réinstallation d'un nœud physique. • Affiche les options de sélection du responsable du châssis. • Affiche l'historique de maintenance du châssis.
Configuration BMC	Sauvegarde et restauration	Permet de réinitialiser la configuration de XClarity Controller aux paramètres d'usine par défaut, sauvegarder la configuration actuelle ou restaurer la configuration à partir d'un fichier.
	Licence	Permet de les clés d'activation pour les fonctions XClarity Controller en option.
	Réseau	Permet de configurer les propriétés, l'état, et les paramètres de XClarity Controller.
	Sécurité	Permet de configurer les propriétés de sécurité, l'état, et les paramètres de XClarity Controller.

Tab	Sélection	Description
	Utilisateur/LDAP	• Permet de configurer les profils de connexion XClarity Controller et les paramètres de connexion globaux. • Permet d'afficher les comptes utilisateur actuellement connectés à XClarity Controller. • L'onglet LDAP permet de configurer l'authentification d'utilisateur qui sera utilisée avec un ou plusieurs serveurs LDAP. Il vous permet également d'activer ou de désactiver la sécurité LDAP et de gérer ses certificats.
	Appel vers Lenovo **Remarque :** Cette fonctionnalité sera prise en charge dans une future mise à jour.	Permet de configurer l'option appel vers Lenovo afin de collecter des informations sur le système et de les envoyer à Lenovo pour obtenir des services.

Chapitre 3. Configuration de XClarity Controller

Les informations de ce chapitre vous permettent de comprendre les options disponibles pour les configurations XClarity Controller.

Lors de la configuration de XClarity Controller, les principales options suivantes sont disponibles :

- Sauvegarde et restauration
- Licence
- Réseau
- Sécurité
- Utilisateur/LDAP

Configuration des comptes utilisateur/LDAP

Les informations de cette rubrique vous permettent de comprendre comment sont gérés les comptes utilisateur.

Cliquez sur **Utilisateur/LDAP** sous **Configuration BMC** pour créer, modifier et afficher les comptes utilisateur, et pour configurer les paramètres LDAP.

L'onglet **Utilisateur local** affiche les comptes utilisateurs qui sont dans XClarity Controller, et qui sont actuellement connectés à XClarity Controller.

L'onglet **LDAP** affiche la configuration LDAP pour l'accès aux comptes utilisateurs qui sont conservés sur un serveur LDAP.

Méthode d'authentification utilisateur

Les informations de cette rubrique vous permettent de comprendre les modes que peut utiliser XClarity Controller pour authentifier les tentatives de connexion.

Cliquez sur le menu déroulant à côté de **Autoriser les ouvertures de session à partir de** afin de sélectionner le mode d'authentification des tentatives de connexion de l'utilisateur. Vous pouvez sélectionner l'une des méthodes d'authentification suivantes :

- **Local uniquement :** Les utilisateurs sont authentifiés par une recherche du compte utilisateur local configuré dans XClarity Controller. Si l'ID et le mot de passe de l'utilisateur ne correspondent pas, l'accès est refusé.
- **LDAP uniquement :** XClarity Controller essaie d'authentifier l'utilisateur à l'aide des données d'identification conservées sur un serveur LDAP. Avec cette méthode d'authentification, la recherche **n'est pas** effectuée dans les comptes utilisateurs locaux se trouvant dans XClarity Controller.
- **Local d'abord, puis LDAP :** L'authentification locale est tentée en premier. Si l'authentification locale échoue, l'authentification LDAP est tentée.
- **LDAP d'abord, puis utilisateur local :** L'authentification LDAP est tentée en premier. Si l'authentification LDAP échoue, l'authentification locale est tentée.

Remarques :

- Seuls les comptes administrés au niveau local sont partagés avec les interfaces IPMI et SNMP. Ces interfaces ne prennent pas en charge l'authentification LDAP.

- Les utilisateurs IPMI et SNMP peuvent se connecter à l'aide des comptes administrés au niveau local lorsque la zone **Autoriser les connexions de** est définie sur **LDAP uniquement**.

Création d’un rôle

Les informations de cette rubrique vous indiquent comment créer un rôle.

Création de rôle

Cliquez sur l’onglet **Rôles**, puis cliquez sur **Créer** pour créer un rôle personnalisé.

Renseignez les champs suivants : **Nom du rôle** et **Niveau d’autorité**. Pour plus d'informations sur le niveau d'autorisation, voir la section suivante.

Le rôle créé est fourni à l’utilisateur dans le menu déroulant Rôle dans la section utilisateur.

Remarque : Le rôle utilisé dans Utilisateur et LDAP n’est pas autorisé à modifier et à supprimer le nom du rôle, mais il peut modifier le droit personnalisé correspondant.

Niveau d'autorisation

Un rôle personnalisé est autorisé à activer toutes les combinaisons des privilèges suivants :

Configuration - Réseau et sécurité BMC
L’utilisateur peut modifier les paramètres de configuration dans les pages Sécurité BMC et Réseau.

Gestion de compte utilisateur
L'utilisateur peut ajouter, modifier ou supprimer des utilisateurs, et modifier les paramètres de connexion globaux.

Accès console distante
L'utilisateur peut accéder à la console distante.

Accès console distante et disques distants
L'utilisateur peut accéder à la console distante et au dispositif de support virtuel.

Alimentation serveur à distance/Redémarrage
L'utilisateur peut exécuter les fonctions de mise sous tension et de redémarrage du serveur.

Configuration - De base
L'utilisateur peut modifier les paramètres de configuration dans les pages Propriétés du serveur et Événements.

Possibilité d'effacer les journaux d'événements
L'utilisateur peut effacer les journaux d'événements. Tout utilisateur peut consulter les journaux d'événements, mais ce niveau d'autorisation est obligatoire pour la suppression des journaux.

Configuration - Avancée (mise à jour du microprogramme, redémarrage BMC, restauration de configuration)
L'utilisateur n'est soumis à aucune restriction lorsqu'il configure XClarity Controller. De plus, il possède les droits d'accès administrateur à XClarity Controller. L'accès administrateur inclut les fonctions avancées suivantes : mises à jour de microprogramme, amorçage réseau PXE, restauration des valeurs usine par défaut de XClarity Controller, modification et restauration des paramètres XClarity Controller à partir d'un fichier de configuration, redémarrage et réinitialisation de XClarity Controller.

Configuration - Sécurité UEFI
Un utilisateur peut modifier les paramètres de sécurité UEFI.

Rôles prédéfinis

Les rôles suivants sont prédéfinis et ne peuvent pas être modifiés ou supprimés :

Administrateur
Le rôle Administrateur n’a aucune restriction et peut effectuer toutes les opérations.

Lecture seule
Le rôle Lecture seule peut afficher des informations du serveur, mais ne peut pas effectuer une opération qui affecte l’état du système, telles que enregistrer, modifier, effacer, réamorcer et mettre à jour le microprogramme.

Opérateur
L’utilisateur avec le rôle Opérateur dispose des privilèges suivants :

- Configuration - Réseau et sécurité BMC
- Alimentation serveur à distance/Redémarrage
- Configuration - De base
- Possibilité d'effacer les journaux d'événements
- Configuration - Avancée (mise à jour du microprogramme, redémarrage BMC, restauration de configuration)

Création d'un compte utilisateur

Les informations de cette rubrique vous indiquent comment créer un nouvel utilisateur local.

Création d'un utilisateur

Cliquez sur l’onglet **Utilisateurs locaux**, puis cliquez **Créer** afin de créer un compte utilisateur.

Renseignez les champs suivants : **Nom d’utilisateur**, **Mot de passe**, **Confirmer le mot de passe**, et sélectionnez un rôle dans le menu déroulant **Rôle**. Pour plus d’informations sur le **Rôle**, voir la section suivante.

Rôle

Les rôles suivants sont prédéfinis tandis que de nouveaux rôles personnalisés peuvent être créés en fonction des besoins de l’utilisateur :

Administrateur
Le rôle Administrateur n’a aucune restriction et peut effectuer toutes les opérations.

Lecture seule
Le rôle Lecture seule peut afficher des informations du serveur, mais ne peut pas effectuer une opération qui affecte l’état du système, telles que enregistrer, modifier, effacer, réamorcer et mettre à jour le microprogramme.

Opérateur
L’utilisateur avec le rôle Opérateur dispose des privilèges suivants :

- Configuration - Réseau et sécurité BMC
- Alimentation serveur à distance/Redémarrage
- Configuration - De base
- Possibilité d'effacer les journaux d'événements
- Configuration - Avancée (mise à jour du microprogramme, redémarrage BMC, restauration de configuration)

Paramètres SNMPv3

Pour activer l'accès SNMPv3 pour un utilisateur, cliquez sur le bouton **Modifier** à côté de l'utilisateur correspondant, puis cochez **SNMP** dans la liste déroulante de l'**interface accessible par l'utilisateur**. Les options d'accès utilisateur suivantes sont décrites :

Type d'accès
Seules les opérations **GET** sont prises en charge. XClarity Controller ne prend pas en charge les opérations **SET** SNMPv3. SNMP3 peut uniquement exécuter des opérations de requête.

Protocole d'authentication
Cet algorithme est utilisé par le modèle de sécurité SNMPv3 pour l'authentification. Les protocoles suivants sont pris en charge :

- Aucune
- HMAC-SHA (par défaut)
- HMAC-SHA224
- HMAC-SHA256
- HMAC-SHA384
- HMAC-SHA512

Protocole de confidentialité
Le transfert de données entre le client SNMP et l'agent peut être protégé à l'aide de leur chiffrement. Les méthodes suivantes sont prises en charge :

- Aucune
- CBC-DES
- AES (par défaut)
- AES192
- AES256
- AES192C
- AES256C

Remarques : Mêmes si les chaînes de mot de passe sont utilisées par un utilisateur SNMPv3, l'accès à XClarity Controller sera toujours possible. Deux exemples sont affichés pour référence.

- Si le mot de passe est défini par « **11111111** » (huit chiffres contenant huit 1), l'utilisateur peut tout de même accéder à XClarity Controller si le mot de passe est accidentellement entré avec plus de huit 1. Par exemple, si le mot de passe est entré avec « **1111111111** » (dix chiffres contenant dix 1), l'accès sera tout de même possible. La chaîne répétitive est considérée comme ayant la même clé.
- Si le mot de passe est défini sur « **bertbert** », l'utilisateur peut tout de même accéder à XClarity Controller si le mot de passe est accidentellement entré comme « **bertbertbert** ». Les deux mots de passe sont considérés comme ayant la même clé.

Pour en savoir plus, reportez-vous à **Considérations de sécurité** du document Internet Standard de RFC 3414 (https://tools.ietf.org/html/rfc3414).

Clé SSH

XClarity Controller prend en charge l'authentification par clé publique SSH (type de clé RSA). Pour ajouter une clé SSH au compte utilisateur local, cliquez sur le bouton **Modifier** à côté de l'utilisateur concerné, puis cochez **Clé SSH** sous la liste déroulante **Interface accessible par l'utilisateur**. Les deux options suivantes sont fournies :

Sélectionner un fichier de clé
Sélectionner le fichier de clé SSH à importer dans XClarity Controller depuis votre serveur.

Entrer une clé dans une zone de texte
Coller ou entrer les données de votre clé SSH dans la zone de texte.

Remarques :

- Lorsqu'ils sont exécutés sur le système d'exploitation du serveur, certains outils Lenovo peuvent créer un compte d'utilisateur temporaire pour accéder au XClarity Controller. Ce compte temporaire n'est pas visualisable et n'utilise aucun des 12 emplacements de compte utilisateur local. Le compte est créé avec un nom d'utilisateur (par exemple, « 20luN4SB ») et un mot de passe aléatoires. Le compte ne peut être utilisé que pour accéder à XClarity Controller sur l'interface interne Ethernet via USB, et uniquement pour les interfaces Redfish et SFTP. La création et la suppression de ce compte temporaire sont consignées dans le journal d'audit comme toute autre action effectuée par l'outil à l'aide de ces données d'identification.
- Pour l'ID du moteur SNMPv3, XClarity Controller utilise un chaîne HEXADÉCIMALE pour indiquer l'ID. Cette chaîne HEXADÉCIMALE est convertie à partir du nom d'hôte XClarity Controller par défaut. Reportez-vous à l'exemple ci-dessous :

  Le nom d'hôte « XCC-7X06-S4AHJ300 » est tout d'abord converti au format ASCII : 88 67 67 45 55 88 48 54 45 83 52 65 72 74 51 48 48

  La chaîne HEXADÉCIMALE est générée en utilisant le format ASCII imprimables (ignorer les espaces entre les caractères) : 58 43 43 36 de 30 2d 37 58 48 41 de 34 2d 53 4a 33 30 30

Suppression d'un compte utilisateur

Les informations de cette rubrique vous indiquent comment supprimer un compte utilisateur local.

Pour supprimer un compte utilisateur local, cliquez sur l'icône de corbeille sur la ligne du compte que vous souhaitez supprimer. Si vous êtes autorisé(e) à le faire, vous pouvez supprimer votre propre compte ou celui d'autres utilisateurs, tant qu'il ne s'agit pas du dernier compte restant doté de privilèges de **gestion de compte utilisateur**.

Utilisation de mots de passe cryptés pour l'authentification

Utilisez les informations dans cette rubrique pour comprendre comment utiliser les mots de passe cryptés pour l'authentification.

Outre l'utilisation des mots de passe et des comptes utilisateur LDAP/AD, le XClarity Controller prend également en charge les mots de passe cryptés de tiers pour l'authentification. Le mot de passe spécial utilise un format de cryptage à sens unique (SHA256) et est pris en charge également par XClarity Controller Web et les interfaces OneCLI et CLI. Toutefois, veuillez noter que l'authentification de XCC SNMP et des interfaces IPMI et CIM ne prennent pas en charge les mots de passe cryptés de tiers. Uniquement l'outil OneCLI et l'interface CLI de XCC peuvent créer un nouveau compte avec un mot de passe crypté ou effectuer une mise à jour du mot de passe crypté. Le XClarity Controller permet également à l'outil OneCLI et l'interface XClarity Controller CLI de récupérer le mot de passe crypté si la fonction de lecture de mot de passe crypté est activée.

Définir un mot de passe crypté via XClarity Controller Web

Cliquez sur **Sécurité** sous **Configuration BMC**, faites défiler jusqu'à la section **Gestionnaire de mots de passe de sécurité** pour activer ou désactiver la fonction **Mot de passer tiers**. Si activé, un mot de passe crypté de tiers est utilisé pour l'authentification de la connexion. La récupération du mot de passe crypté de tiers depuis le XClarity Controller peut également être activée ou désactivée.

Remarque : Par défaut, les fonctions **Mot de passe tier** et **Autoriser la récupération de mots de passe tiers** sont désactivées.

Pour vérifier si le mot de passe est **natif** ou un **mot de passe de tiers**, cliquez sur **User/LDAP** sous **Configuration BMC** pour plus d'informations. Les informations se trouveront dans la colonne **attribut avancé**.

Remarques :

- Les utilisateurs ne seront pas en mesure de modifier un mot de passe s'il s'agit d'un mot de passe de tiers et les zones **Mot de passe** et **Confirmer mot de passe** seront grisées.
- Si le mot de passe de tiers a expiré, un message d'avertissement s'affichera lors du processus de connexion de l'utilisateur.

Définir le mot de passe crypté via la fonction OneCLI

- Activation de la fonctionnalité

  ```
  $ sudo OneCli config set IMM.ThirdPartyPassword Enabled
  ```

- Création d'un mot de passe crypté (sans Salt). L'exemple suivant montre un example d'une connexion à XClarity Controller à l'aide du mot de passe **password123**.

  ```
  $ pwhash = `echo -n password123 | openssl dgst -sha256 | awk '{print $NF}'`

  $ echo $pwhash 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

  $ sudo OneCli config set IMM.Loginid.2 admin

  $ sudo OneCli config set IMM.SHA256Password.2 $pwhash

  $ sudo OneCli config set IMM.SHA256PasswordSalt.2 ""
  ```

- Création d'un utilisateur avec un mot de passe crypté (avec Salt). L'exemple suivant montre un example d'une connexion à XClarity Controller à l'aide du mot de passe **password123**. Salt=abc.

  ```
  $ pwhash = `echo -n password123abc | openssl dgst -sha256 | awk '{print $NF}'`

  $ echo $pwhash 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee

  $ sudo OneCli config set IMM.Loginid.3 Admin

  $ sudo OneCli config set IMM.SHA256Password.3 $pwhash

  $ sudo OneCli config set IMM.SHA256PasswordSalt.3 'abc'
  ```

- Récupération du mot de passe crypté et salt.

  ```
  $ sudo OneCli config set IMM.ThirdPartyPasswordReadable Enabled

  $ sudo OneCli config show IMM.SHA256Password.3

  $ sudo OneCli config show IMM.SHA256PasswordSalt.3
  ```

- Suppression du mot de passe crypté et salt.

  ```
  $ sudo OneCli config set IMM.SHA256Password.3 ""

  $ sudo OneCli config set IMM.SHA256PasswordSalt.3 ""
  ```

- Attribution du mot de passe crypté à un compte existant.

  ```
  $ sudo OneCli config set IMM.Loginid.2 admin

  $ sudo OneCli config set IMM.Password.2 Passw0rd123abc

  $ sudo OneCli config set IMM.SHA256Password.2 $pwhash
  ```

```
$ sudo OneCli config set IMM.SHA256PasswordSalt.2 ""
```

Remarque : Lorsque le mot de passe crypté est défini, ce mot de passe prend effet immédiatement. Le mot de passe standard d'origine ne fonctionnera plus. Dans cet exemple, le mot de passe d'origine standard **Passw0rd123abc** ne peut plus être utilisé jusqu'à ce que le mot de passe crypté est supprimé.

Définir le mot de passe crypté via la fonction CLI

- Activation de la fonctionnalité

  ```
  > hashpw -sw enabled
  ```

- Création d'un mot de passe crypté (sans Salt). L'exemple suivant montre un example d'une connexion à XClarity Controller à l'aide du mot de passe **password123**.

  ```
  $ pwhash = `echo -n password123 | openssl dgst -sha256 | awk '{print $NF}'`

  5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

  > users -2 -n admin -shp 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a
  super
  ```

- Création d'un utilisateur avec un mot de passe crypté (avec Salt). L'exemple suivant montre un example d'une connexion à XClarity Controller à l'aide du mot de passe **password123**. Salt=abc.

  ```
  $ pwhash = `echo -n password123abc | openssl dgst -sha256 | awk '{print $NF}'`

  $ echo $pwhash 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee

  > users -3 -n Admin -shp 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
  -ssalt 'abc' -a super
  ```

- Récupération du mot de passe crypté et salt.

  ```
  > hashpw -re enabled

  > users -3 -ghp -gsalt
  ```

- Suppression du mot de passe crypté et salt.

  ```
  > users -3 -shp "" -ssalt ""
  ```

- Attribution du mot de passe crypté à un compte existant.

  ```
  > users -2 -n admin -p Passw0rd123abc -shp
  5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a super
  ```

  Remarque : Lorsque le mot de passe crypté est défini, ce mot de passe prend effet immédiatement. Le mot de passe standard d'origine ne fonctionnera plus. Dans cet exemple, le mot de passe d'origine standard **Passw0rd123abc** ne peut plus être utilisé jusqu'à ce que le mot de passe crypté est supprimé.

Une fois la configuration du mot de passe crypté terminée, rappelez-vous de pas utiliser ce dernier pour vous connecter à XClarity Controller. Lors de la connexion, vous devez utiliser le mot de passe en texte clair. Dans l'exemple ci-dessous, le mots de passe en texte clair est « password123 ».

```
$ pwhash = 'echo –n password123 | openssl dgst –sha256 | awk '{print $NF}''

5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

> users -2 -n admin -shp 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a super
```

Configuration des paramètres de connexion globale

Les informations de cette rubrique vous permettent de configurer les paramètres de stratégie de connexion et mots de passe qui s'appliquent à tous les utilisateurs.

Délai d'attente d'inactivité de session Web

Les informations de cette rubrique vous permettent de définir l'option de délai d'attente d'inactivité de session Web.

Dans la zone **Délai d'attente d'inactivité de session Web**, vous pouvez spécifier combien de temps, en minutes, XClarity Controller doit attendre avant de déconnecter une session Web inactive. Le délai d'attente maximum est de 1 440 minutes. Si elle est associée à la valeur 0, la session Web n'expire jamais.

Le microprogramme XClarity Controller prend en charge jusqu'à six sessions Web simultanées. Pour libérer une session au profit d'un autre utilisateur, il est recommandé de se déconnecter de la session Web dès vous avez fini, au lieu d'attendre que le délai d'attente d'inactivité ferme votre session.

Remarque : Si vous laissez votre navigateur ouvert sur une page Web de XClarity Controller qui s'actualise automatiquement, votre session Web ne se fermera pas automatiquement pour cause d'inactivité.

Paramètres de stratégie de sécurité de compte

Ces informations vous indiquent comment définir la stratégie de sécurité de compte pour votre serveur.

Les informations suivantes offrent une description des zones de configuration des paramètres de sécurité.

Forcer la modification du mot de passe lors du premier accès

Après avoir défini un nouvel utilisateur avec un mot de passe par défaut, la sélection de cette case forcera l'utilisateur à modifier son mot de passe lors de sa première connexion. La valeur par défaut de cette zone est de faire activer la case à cocher.

Mot de passe complexe requis

La case d'option est cochée par défaut et le mot de passe complexe doit respecter les règles suivantes :

- Ne contenir que les caractères suivants (les espaces ou caractères espace blancs ne sont pas autorisés) : A-Z, a-z, 0-9, ~`!@#$%^&*()-+={}[]|:;"'<>,?/._
- Doit contenir au moins une lettre
- Doit contenir au moins un nombre
- Doit contenir au moins deux des combinaisons suivantes :
  - Au moins une lettre en majuscule.
  - Au moins une lettre en minuscule.
  - Au moins un caractère spécial.
- Aucun autre caractère (en particulier les espaces ou caractères blancs) n'est autorisé
- Les mots de passe ne peuvent pas avoir plus de deux caractères identiques consécutifs (par exemple, « aaa »).
- Le mot de passe ne peut pas être identique au nom d'utilisateur, en répétant simplement le nom d'utilisateur une ou plusieurs fois ou en suivant un ordre de caractères inversés du nom d'utilisateur.
- Les mots de passe doivent avoir un minimum de 8 et un maximum de 255 caractères.

Si la case d'option n'est pas cochée, le nombre indiqué par la longueur de mot de passe minimum peut être défini sur une valeur allant de 0 à 255 caractères. Le mot de passe du compte peut être vide si la longueur de mot de passe minimum est définie sur 0.

Période d'expiration du mot de passe (jours)
Cette zone contient l'âge maximal autorisé du mot de passe, avant lequel il devra être modifié.

Période d'avertissement d'expiration du mot de passe (jours)
Cette zone contient le nombre de jours pendant lesquels un utilisateur est averti avant que le mot de passe expire.

Longueur minimale du mot de passe (caractères)
Cette zone contient la longueur minimale du mot de passe.

Cycle de réutilisation du mot de passe minimum (fois)
Cette zone contient le nombre de mots de passe antérieurs ne pouvant pas être réutilisés.

Intervalle de modification du mot de passe minimum (heures)
Cette zone contient la durée nécessaire à attendre pour que l'utilisateur puisse à nouveau changer son mot de passe.

Nombre maximum d'échecs de connexion (fois)
Cette zone contient le nombre d'échecs de tentatives de connexion autorisé avant que ne l'utilisateur soit verrouillé pendant une période définie.

Période de verrouillage après le nombre maximum d'échecs de connexion (minutes)
Cette zone indique la durée (en minutes) pendant laquelle XClarity Controller va désactiver les tentatives de connexion à distance une fois le nombre maximum d'échecs de connexion atteint.

Configuration LDAP

Les informations de cette rubrique vous indiquent comment afficher ou modifier les paramètres LDAP de XClarity Controller.

La prise en charge LDAP contient :

- Prise en charge pour la version de protocole LDAP 3 (RFC-2251)
- Prise en charge pour le client LDAP standard API (RFC-1823)
- Prise en charge pour la syntaxe de filtre recherche LDAP standard (RFC-2254)
- Prise en charge pour l'extension de Lightweight Directory Access Protocol (v3) pour le Transport Layer Security (RFC-2830)

L’implémentation LDAP prend en charge les serveurs LDAP suivants :

- Microsoft Active Directory (Windows 2003, Windows 2008, Windows 2012, Windows 2016, Windows 2019)
- Microsoft Active Directory Application Mode (Windows 2003, Windows 2008)
- Microsoft Lightweight Directory Service (Windows 2008, Windows 2012, Windows 2016, Windows 2019)
- Serveur Novell eDirectory, version 8.7 et 8.8
- OpenLDAP Server 2.1, 2.2, 2.3, 2.4, 2.5 et 2.6

Cliquez sur l'onglet **LDAP** pour afficher ou modifier les paramètres LDAP de XClarity Controller.

XClarity Controller peut authentifier à distance l'accès d'un utilisateur via un serveur LDAP central, ou en plus des comptes utilisateur locaux qui sont stockés dans XClarity Controller lui-même. Des privilèges peuvent être désignés pour chaque compte d’utilisateur à l’aide de l’indicateur « Attribut d’autorisation de connexion ». Vous pouvez aussi utiliser le serveur LDAP pour affecter des utilisateurs à des groupes et effectuer une authentification de groupe, en plus de l'authentification utilisateur (vérification de mot de passe)

normale. Par exemple, XClarity Controller peut être associé à un ou plusieurs groupes, l'utilisateur réussit l'authentification de groupe uniquement s'il appartient à au moins un groupe qui est associé à XClarity Controller.

Pour configurer un serveur LDAP, procédez comme suit :

1. Sous **Informations du serveur LDAP**, les options suivantes sont disponibles dans la liste d'éléments :
   - **Utiliser le serveur LDAP pour l'authentification uniquement (avec autorisation)** : Cette sélection permet d'indiquer à XClarity Controller d'utiliser les données d'identification uniquement pour s'authentifier auprès du serveur LDAP et pour extraire les informations d'appartenance de membre au groupe. Les noms et les rôles des groupes peuvent être configurés dans la section **Groupes pour l'autorisation locale**.
   - **Utiliser le serveur LDAP pour l'authentification et l'autorisation** : Cette section permet d'indiquer à XClarity Controller d'utiliser les données d'identification à la fois pour s'authentifier auprès du serveur LDAP et pour identifier les autorisations de l'utilisateur.

   Remarque : Les serveurs LDAP à utiliser pour l'authentification peuvent être configurés manuellement ou détectés de manière dynamique via des enregistrements SRV DNS.

   - **Utiliser des serveurs préconfigurés** : Vous pouvez configurer jusqu'à trois serveurs LDAP en saisissant l'adresse IP ou le nom d'hôte de chaque serveur si le DNS est activé. Le numéro de port de chaque serveur est facultatif. Si cette zone est laissée vide, la valeur par défaut 389 est utilisée pour les connexions LDAP non sécurisées. Pour les connexions sécurisées, la valeur de port par défaut est 636. Vous devez configurer au moins un serveur LDAP.
   - **Utiliser DNS pour rechercher des serveurs** : Vous pouvez choisir de détecter le ou les serveurs LDAP de manière dynamique. Les mécanismes décrits dans RFC2782 (A DNS RR pour l'indication de l'emplacement des services) permettent de localiser le ou les serveurs LDAP. Il s'agit du SRV DNS. Vous devez spécifier un nom FQDN à utiliser comme nom de domaine dans la demande SRV DNS.
     - **Forêt AD** : Dans un environnement avec des groupes universels communs à plusieurs domaines, le nom de la forêt (ensemble de domaines) doit être configuré pour reconnaître les catalogues globaux (GC) requis. Dans un environnement où l'appartenance à un groupe commun à plusieurs domaines ne s'applique pas, cette zone peut rester vide.
     - **Domaine AD** : Vous devez spécifier un nom de domaine qualifié complet (FQDN) à utiliser comme nom de domaine dans la demande SRV DNS.

   Si vous souhaitez activer LDAP sécurisé, cochez la case **Activer le LDAP sécurisé**. Pour permettre la prise en charge de LDAP sécurisé, il est nécessaire de mettre en place un certificat SSL valide et au moins un certificat sécurisé client SSL doit être importé dans XClarity Controller. Votre serveur LDAP doit prendre en charge Transport Layer Security (TLS) version 1.2 pour être compatible avec le client LDAP sécurisé de XClarity Controller. Pour plus d'information sur le traitement des certificats, voir « Traitement des certificats SSL » à la page 43.
2. Renseignez les information sous **Paramètres supplémentaires**. Les paramètres sont décrits ci-dessous.

   Type de LDAP

   Sélectionnez le type de serveur LDAP pour l'authentification basée sur LDAP. Les types de serveur suivants sont disponibles :

   - **OpenLDAP**

     OpenLDAP
   - **Active Directory**

     Répertoire : Windows Active Directory
   - **Autre**

Répertoire : Apache Directory, eDirectory, etc.

Méthode de liaison

Avant d'effectuer une recherche ou d'interroger le serveur LDAP, vous devez envoyer une demande de liaison. Cette zone contrôle la façon dont cette liaison initiale au serveur LDAP est réalisée. Les méthodes de liaison suivantes sont disponibles :

- **Utiliser les données d'identification configurées**

  Utilisez cette méthode pour effectuer une liaison avec le DN et le mot de passe du client configuré.

- **Utiliser les données d'identification de connexion**

  Utilisez cette méthode pour effectuer une liaison avec les données d'identification fournies au cours du processus de connexion. L'ID utilisateur peut être fourni via un nom distinctif (DN), un DN partiel, un nom de domaine qualifié complet ou via un ID utilisateur qui correspond à l'attribut de recherche UID qui est configuré dans XClarity Controller. Si les données d'identification présentées ressemblent à un nom distinctif partiel (par exemple, cn=joe), celui-ci sera apposé en préfixe au nom distinctif racine configuré afin de tenter de créer un nom distinctif correspondant à l'enregistrement de l'utilisateur. Si la tentative de liaison échoue, une tentative finale sera effectuée en ajoutant le préfixe cn= aux données d'identification de connexion, puis en ajoutant la chaîne résultante au nom distinctif racine configuré.

Si la liaison initiale est réussie, une recherche est lancée pour trouver une entrée sur le serveur LDAP correspondant à l'utilisateur se connectant. Si nécessaire, une seconde tentative de liaison est effectuée, cette fois-ci avec le DN extrait de l'enregistrement LDAP de l'utilisateur et le mot de passe entré lors du processus de connexion. Si la seconde tentative de liaison échoue, la demande d'accès de l'utilisateur est refusée. La seconde liaison est effectuée uniquement lorsque les méthodes de liaison **Utiliser des données d'identification configurées** sont utilisées.

Nom distinctif du client

Nom distinctif du client (DN) à utiliser pour la liaison initiale. En outre, il est limité à un maximum de 300 caractères.

Mot de passe du client

Le mot de passe de ce client distinctif.

Nom distinctif (DN) racine

Il s'agit du nom distinctif (DN) de l'entrée racine de l'arborescence de répertoires sur le serveur LDAP (par exemple, dn=mycompany,dc=com). Ce nom distinctif est utilisé comme objet de base pour toutes les demandes de recherche.

Attribut de recherche du nom de connexion de l'utilisateur

Lorsque la méthode de liaison est définie sur **Utiliser des données d'identification configurées**, la liaison initiale vers le serveur LDAP est suivie d'une demande de recherche qui extrait des informations spécifiques sur l'utilisateur, y compris son nom distinctif, ses droits de connexion et son appartenance à un groupe. Cette demande de recherche doit spécifier le nom d'attribut représentant les ID d'utilisateur sur ce serveur. Ce nom d'attribut est configuré dans cette zone. Sur les serveurs Active Directory, le nom de l'attribut est généralement **CN** ou **sAMAccountName**. Sur les serveurs Novell eDirectory et OpenLDAP, le nom d'attribut est uid. Si ce champ est laissé vide, la valeur par défaut est **sAMAccountName**.

Filtre de groupe

La zone **Filtre de groupe** est utilisée pour l'authentification des groupes. L'authentification de groupe est tentée une fois que la vérification des données d'identification de l'utilisateur a été réalisée avec succès. Si l'authentification de groupe échoue, la tentative de connexion de

l'utilisateur est refusée. Lorsque le filtre de groupe est configuré, il est utilisé pour spécifier à quels groupes XClarity Controller appartient. Cela signifie que l'utilisateur doit appartenir au moins à l'un des groupes configurés pour que l'authentification de groupe réussisse. Si la zone **Filtre de groupe** est laissée vide, l'authentification de groupe réussit automatiquement. Si le filtre de groupe est configuré, le système vérifie si au moins un groupe de la liste correspond à l'un des groupes auxquels l'utilisateur appartient. S'il n'y a pas de groupe concordant, l'authentification de l'utilisateur échoue et l'accès est refusé. Si au moins une concordance est trouvée, l'authentification de groupe réussit.
Les comparaisons sont sensibles à la casse. Le filtre est limité à 511 caractères et peut comprendre un ou plusieurs noms de groupe. Le signe deux-points (:) doit être utilisé pour délimiter plusieurs noms de groupes. Les espaces de début et de fin sont ignorés. Tous les autres espaces sont traités comme faisant partie du nom du groupe.

Remarque : Le caractère générique (*) n'est plus traité comme un caractère générique. Le concept de caractère générique n'est plus utilisé en raison des risques qui peuvent affecter la sécurité. Un nom de groupe peut être spécifié en utilisant un nom distinctif complet ou seulement la portion **cn**. Par exemple, un groupe dont le nom distinctif est cn=adminGroup, dc=mycompany, dc=com peut être spécifié en utilisant ce nom distinctif ou adminGroup.

Attribut de recherche d'appartenance à un groupe
Le champ **Attribut de recherche de groupe** indique le nom de l'attribut utilisé pour identifier les groupes auxquels appartient un utilisateur. Sur les serveurs Active Directory, le nom de l'attribut est généralement **memberOf**. Sur les serveurs Novell eDirectory, le nom de l'attribut est **groupMembership**. Sur les serveurs OpenLDAP, les utilisateurs sont généralement affectés à des groupes dont objectClass est égal à PosixGroup. Dans ce contexte, cette zone spécifie le nom d'attribut utilisé pour identifier les membres d'un groupe PosixGroup particulier. Ce nom d'attribut est **memberUid**. Si cette zone est laissée vide, le nom d'attribut du filtre correspond par défaut à **memberOf**.

Attribut d'autorisation de connexion
Lorsqu'un utilisateur s'authentifie avec succès à travers un serveur LDAP, les droits de connexion de l'utilisateur doivent être récupérés. Pour récupérer les droits de connexion, le filtre de recherche envoyé au serveur doit indiquer le nom d'attribut associé aux droits de connexion. Le champ **Attribut d'autorisation de connexion** indique le nom d'attribut. Si vous utilisez le serveur LDAP pour l'authentification et l'autorisation, mais que ce champ est laissé vide, l'utilisateur se voit refuser l'accès.
La valeur d'attribut renvoyée par les recherches du serveur LDAP doit être une chaîne de bits saisie sous la forme de 13 « 0 » ou « 1 » consécutifs, ou une chaîne de bits sous la forme de 13 « 0 » ou « 1 » consécutifs au total. Chaque bit représente un ensemble de fonctions. Les bits sont numérotés selon leur position. Le bit le plus à gauche est la position de bit 0 et le bit le plus à droite est la position de bit 12. Une valeur de 1 à la position d'un bit active la fonction associée à cette position de bit. Si une position de bit a la valeur 0, la fonction associée à cette position de bit est désactivée. La chaîne 0100000000000 est un exemple valide, qui est utilisé pour permettre de le placer dans n'importe quel champ. L'attribut utilisé permet une chaîne au format libre. Lorsque l'attribut est récupéré avec succès, la valeur renvoyée par le serveur LDAP est interprétée conformément à l'information du tableau suivant.

Tableau 1. Bits d'autorisation

Tableau à trois colonnes contenant des explications sur les positions de bit.

Tableau 1. Bits d'autorisation (suite)

Position de bit	Fonction	Explication
0	Refus permanent	L'authentification de l'utilisateur échoue toujours. Cette fonction peut être utilisée pour bloquer un ou plusieurs utilisateurs associés à un groupe spécifique.
1	Accès superviseur	L'utilisateur obtient les privilèges d'administrateur. L'utilisateur dispose d'un accès en lecture et écriture à chaque fonction. Si vous définissez ce bit, vous n'avez pas à définir individuellement les autres.
2	Accès en lecture seule	L'utilisateur dispose d'un accès en lecture seule et ne peut pas exécuter de procédures de maintenance (par exemple, un redémarrage, des actions à distance ou des mises à jour de microprogramme) ni effectuer de modifications (par exemple, les fonctions de sauvegarde, suppression ou restauration). La position de bit 2 et tous les autres bits s'excluent mutuellement, la position de bit 2 étant celle avec la plus faible priorité. Si un autre bit est défini, ce bit sera ignoré.
3	Configuration - Réseau et sécurité BMC	L'utilisateur peut modifier la configuration des pages Sécurité, Protocoles réseau, Interface réseau, Affectations des ports et Port série.
4	Gestion de compte utilisateur	L'utilisateur peut ajouter, modifier ou supprimer des utilisateurs et modifier les paramètres de connexion globaux (Paramètres de connexion globaux) dans la fenêtre Profils de connexion.
5	Accès console distante	L'utilisateur peut accéder à la console du serveur distant.
6	Accès console distante et disques distants	L'utilisateur peut accéder à la console du serveur distant et aux fonctions de disque distant du serveur distant.
7	Démarrage serveur distant/Accès redémarrage	L'utilisateur peut accéder aux fonctions de mise sous tension et de redémarrage du serveur distant.
8	Configuration - De base	L'utilisateur peut modifier les paramètres de configuration dans les fenêtres Paramètres système et Alertes.
9	Possibilité d'effacer les journaux d'événements	L'utilisateur peut effacer les journaux d'événements. **Remarque :** Tous les utilisateurs peuvent afficher les journaux des événements mais ce niveau d'autorisation est requis pour pouvoir effacer leur contenu.
10	Configuration - Avancée (mise à jour du microprogramme, redémarrage BMC, restauration de configuration)	L'utilisateur n'est soumis à aucune restriction lorsqu'il configure XClarity Controller. De plus, il possède les droits d'accès administrateur à XClarity Controller. L'utilisateur peut exécuter les fonctions avancées suivantes : mises à jour de microprogramme, amorçage réseau PXE, restauration des paramètres usine par défaut de l'adaptateur, modification et restauration de la configuration de l'adaptateur depuis un fichier de configuration et redémarrage/ réinitialisation de l'adaptateur.
11	Configuration - Sécurité UEFI	Un utilisateur peut configurer les paramètres liés à la sécurité UEFI, qui peuvent également être configurés à partir de la page de configuration de la sécurité UEFI F1.
12	Réservé	Réservé pour une utilisation ultérieure et actuellement ignoré.

Si aucun des bits n'est défini, l'accès sera refusé à l'utilisateur

Remarque : Veuillez noter que le système donne la priorité aux droits de connexion récupérés directement de l'enregistrement utilisateur. Si l'utilisateur ne dispose pas de la permission de connexion dans son enregistrement, le système tente d'extraire les autorisations du(des) groupe(s) au(x)quel(s) appartient l'utilisateur et, si configuré, qui corresponde(nt) au filtre de groupe. Dans ce cas, l'utilisateur recevra l'opérateur inclusif OR de tous les bits pour tous ceux des groupes. De même, le bit **Accès en lecture seule** sera défini uniquement si tous les autres bits correspondent à 0. Notez également que si le bit **Refus permanent** est défini pour l'un des groupes, l'accès sera refusé à l'utilisateur. Le bit **Refus permanent** a toujours priorité sur les autres bits.

Important : Si l'autorisation de modifier les paramètres de configuration de base, de réseau et/ou de sécurité de l'adaptateur est accordée à l'utilisateur, vous devriez envisager d'autoriser ce même utilisateur à redémarrer XClarity Controller (bit de position 10). Sans cette autorisation, l'utilisateur pourra modifier des paramètres (par exemple, l'adresse IP de l'adaptateur), mais sans qu'ils ne prennent effet.

3. Si le mode **Utiliser le serveur LDAP pour l'authentification uniquement (avec autorisation locale)** est utilisé, configurez l'option **Groupes pour l'autorisation locale**. Le nom du groupe, le domaine du groupe et le rôle sont configurés pour fournir une autorisation locale aux groupes d'utilisateurs. Chaque groupe peut se voir attribuer un rôle (autorisations) identique à celui configuré dans les rôles dans Utilisateur local. Les comptes d'utilisateurs sont affectés à différents groupes sur le serveur LDAP. Un compte utilisateur se verra attribuer le rôle (autorisations) du groupe auquel ce compte d'utilisateur appartient après la connexion au module BMC. Le domaine du groupe doit être au même format que le nom distinctif, par exemple : dc=mycompany,dc=com, sera utilisé comme objet de base pour les recherches de groupe. Si le champ est laissé vide, il utilisera la même valeur que le champ « Root DN ». Des groupes supplémentaires peuvent être ajoutés en cliquant sur l'icône « + » ou supprimés en cliquant sur l'icône « x ».
4. Sélectionnez l'attribut utilisé pour afficher le nom d'utilisateur dans le menu déroulant **Spécifier l'attribut utilisé pour afficher le nom d'utilisateur**.

Configuration des protocoles réseau

Les informations de cette rubrique vous permettent d'afficher ou de définir les paramètres réseau de XClarity Controller.

Configuration des paramètres Ethernet

Les informations de cette rubrique vous indiquent comment afficher ou modifier la manière dont XClarity Controller communique via une connexion Ethernet.

Remarque : Les serveurs AMD ne prennent pas en charge la fonction de basculement Ethernet.

XClarity Controller utilise deux contrôleurs de réseau. Un contrôleur de réseau est connecté au port de gestion dédié et l'autre, au port partagé. Chacun des contrôleurs de réseau se voit attribuer sa propre adresse MAC gravée. Si DHCP est utilisé pour affecter une adresse IP au XClarity Controller, lorsqu'un utilisateur passe d'un port réseau à un autre ou en cas de bascule du port réseau dédié vers le port réseau partagé, une adresse IP différente peut être affectée au XClarity Controller par le serveur DHCP. En utilisant le protocole DHCP, il est recommandé que les utilisateurs utilisent le nom d'hôte pour accéder au XClarity Controller plutôt que de compter sur une adresse IP. Même si les ports de réseau XClarity Controller ne sont pas modifiés, le serveur DHCP peut affecter une adresse IP différente au XClarity Controller à l'expiration du bail DHCP, ou au redémarrage du XClarity Controller. Si un utilisateur doit accéder au XClarity Controller à l'aide d'une adresse IP qui ne change pas, le XClarity Controller doit être configuré en vue d'une adresse IP statique plutôt que du protocole DHCP.

Cliquez sur **Réseau** sous **Configuration BMC** pour modifier les paramètres Ethernet de XClarity Controller.

Configuration du nom d'hôte de XClarity Controller

Le nom d'hôte par défaut de XClarity Controller est généré en utilisant une combinaison de la chaîne « XCC - », suivie par le type de machine du serveur et le numéro de série du serveur (par exemple, « XCC-7X03-1234567890 »). Vous pouvez modifier le nom d'hôte de XClarity Controller en entrant jusqu'à 63 caractères dans cette zone. Le nom d'hôte ne doit pas contenir un point (.) et il peut contenir uniquement des caractères alphanumériques, le trait d'union et des caractères de soulignement.

Ports Ethernet

Ce paramètre contrôle l'activation des ports Ethernet utilisés par le contrôleur de gestion, y compris les ports partagés et dédiés.

Une fois **désactivés**, certains ports Ethernet ne reçoivent pas d'adresses IPv4 ou IPv6, empêchant toute modification supplémentaire des configurations Ethernet.

Remarque : Ce paramètre n'affecte pas l'interface LAN USB ni le port de gestion USB situé à l'avant du serveur. Ces interfaces disposent de leurs propres paramètres d'activation dédiés.

Configuration des paramètres réseau IPv4

Pour utiliser une connexion Ethernet IPv4, procédez comme suit :

1. Activez l'option **IPv4**.

   Remarque : La désactivation de l'interface Ethernet empêche l'accès à XClarity Controller depuis le réseau externe.
2. Dans la zone **Méthode**, sélectionnez l'une des options suivantes :
   - **Obtenir IP depuis DHCP** : XClarity Controller obtient son adresse IPv4 d'un serveur DHCP.
   - **Utiliser une adresse IP statique** : XClarity Controller utilise la valeur spécifiée par l'utilisateur pour son adresse IPv4.
   - **DHCP d'abord, puis adresse IP statique** : XClarity Controller essaie d'obtenir son adresse IPv4 d'un serveur DHCP, mais sa tentative échoue, il utilise alors la valeur spécifiée par l'utilisateur pour son adresse IPv4.
3. Dans la zone **Adresse statique IPv4**, saisissez l'adresse IP que vous voulez affecter à XClarity Controller.

   Remarque : L'adresse IP doit contenir quatre nombres entiers compris entre 0 et 255, sans espace et séparés par des points. Cette zone ne sera pas configurable si la méthode est définie sur **Obtenir IP depuis DHCP**.
4. Dans la zone **Masque de réseau**, entrez le masque de sous-réseau utilisé par XClarity Controller.

   Remarque : Le masque de sous-réseau doit contenir quatre nombres entiers compris entre 0 et 255, sans espace ni points consécutifs et séparés par des points. La valeur par défaut est 255.255.255.0. Cette zone ne sera pas configurable si la méthode est définie sur **Obtenir IP depuis DHCP**.
5. Dans la zone **Passerelle par défaut**, entrez le routeur de votre passerelle réseau.

   Remarque : L'adresse de passerelle doit contenir quatre nombre entiers compris entre 0 et 255, sans espace ni points consécutifs et séparés par des points. Cette zone ne sera pas configurable si la méthode est définie sur **Obtenir IP depuis DHCP**.

Configuration des paramètres Ethernet avancés

Cliquez sur l'onglet **Ethernet avancé** pour définir des paramètres Ethernet supplémentaires.

Pour activer le marquage VLAN (LAN virtuel), cochez la case **Activer VLAN**. Lorsque le réseau local virtuel (VLAN) est activé et qu'un ID VLAN est configuré, XClarity Controller accepte uniquement les paquets avec les ID VLAN spécifiés. Ces ID VLAN peuvent être configurés avec des valeurs numériques comprises entre 1 et 4094.

Dans la liste **Adresse MAC**, choisissez l'une des sélections suivantes :

- **Utiliser l'adresse MAC gravée**

  L'option Adresse MAC gravée est une adresse physique unique attribuée à XClarity Controller par le fabricant. L'adresse constitue une zone en lecture seule.

- **Utiliser une adresse MAC personnalisée**

  Si une valeur est spécifiée, l'adresse administrée localement remplace l'adresse MAC gravée. L'adresse administrée localement doit être une valeur hexadécimale comprise entre `00000000000` et `FFFFFFFFFFFF`. Cette valeur doit être indiquée au format **xx:xx:xx:xx:xx:xx** où **x** est un nombre hexadecimal de 0 à 9 ou de « a » à « f ». XClarity Controller ne prend pas en charge l'utilisation d'une adresse de multidiffusion. Le premier octet d'une adresse de multidiffusion est un nombre impair (le bit le moins significatif est défini sur 1), par conséquent, le premier octet doit être un nombre pair.

Dans la zone **Vitesse de transfert et duplex**, sélectionnez **négociation automatique** ou **sur mesure** pour préciser la vitesse de transfert et le duplex.

Dans la zone **MTU (unité de transmission maximale)**, spécifiez l'unité de transmission maximale d'un paquet (en octets) pour votre interface réseau. La portée maximale de l'unité de transmission est de 1 000 à 1 500. La valeur par défaut de ce champ est 1 500.

Configuration des paramètres réseau IPv6

1. Activez l'option **IPv6**.
2. Affectez une adresse IPv6 à l'interface à l'aide de l'une des méthodes d'affectation suivantes :
   - Utiliser la configuration automatique d'adresse sans état
   - Utiliser la configuration d'adresse dynamique (DHCPv6)
   - Utiliser l'adresse IP affectée de façon statique

     Remarques : Si l'option **Utiliser l'adresse IP affectée de manière statique** est sélectionnée, vous êtes invité(e) à entrer les informations suivantes :

     – Adresse IPv6
     – Longueur du préfixe
     – Passerelle

Configuration DNS

Les informations de cette rubrique vous indiquent comment afficher ou modifier les paramètres DNS de XClarity Controller.

Cliquez sur **Réseau** sous **Configuration BMC** pour afficher ou modifier les paramètres DNS de XClarity Controller.

Si vous cochez la case **Utiliser des serveurs d'adresse DNS supplémentaires**, spécifiez les adresses IP de jusqu'à trois serveurs DNS sur votre réseau. Chaque adresse IP doit contenir quatre entiers (compris entre 0 et 255) séparés par des points, sans espace. Ces adresses de serveur DNS sont ajoutées en tête de la liste de recherche, de sorte que la recherche de nom d'hôte est effectuée sur ces serveurs avant d'être effectuée sur un serveur DNS affecté automatiquement par un serveur DHCP.

Si vous cochez la case **Utiliser DNS pour détecter Lenovo XClarity Administrator**, XClarity Manager doit être sélectionné.

Configuration DDNS

Les informations de cette rubrique vous indiquent comment activer ou désactiver le protocole Dynamic Domain Name System (DDNS) dans XClarity Controller.

Cliquez sur **Réseau** sous **Configuration BMC** pour afficher ou modifier les paramètres DDNS de XClarity Controller.

Cochez la case **Activer DDNS** pour activer le DDNS. Lorsque le DDNS est activé, XClarity Controller indique à un DNS de modifier, en temps réel, la configuration DNS active des noms d'hôte, adresses ou autres informations configurées, stockées dans le DNS.

Sélectionnez une option dans la liste des éléments pour décider la façon dont vous souhaitez que le nom de domaine de XClarity Controller soit sélectionné.

- **Utiliser le nom de domaine personnalisé** : Vous pouvez spécifier le nom de domaine auquel le XClarity Controller appartient.
- **Nom de domaine d'utilisation obtenu du serveur DHCP** : Le nom de domaine auquel le XClarity Controller appartient est spécifié par le serveur DHCP.

Configuration d'Ethernet sur USB

Les informations de cette rubrique vous indiquent comment contrôler l'interface Ethernet sur USB utilisée pour la communication par voie interne entre le serveur et XClarity Controller.

Cliquez sur **Réseau** sous **Configuration BMC** pour afficher ou modifier les paramètres XClarity Controller sur USB.

Ethernet sur USB est utilisé pour les communications intrabande avec XClarity Controller. Cochez la case pour activer ou désactiver l'interface Ethernet sur USB.

Important :

- Si vous désactivez **Ethernet sur USB**, vous ne pouvez plus effectuer une mise à jour intrabande du microprogramme XClarity Controller ou du microprogramme du serveur à l'aide des utilitaires de mise à jour intrabande XClarity Essentials. Utilisez l'option de mise à jour du microprogramme sur l'interface Web XClarity Controller ou l'utilitaire de mise à jour hors bande XClarity Essentials pour mettre à jour le microprogramme.
- Il est important de désactiver les délais d'attente du programme de surveillance pour éviter que le serveur ne redémarre de manière inattendue lorsque l'interface USB intrabande est désactivée.
- Pour utiliser cette interface, les pilotes du système d'exploitation qui prennent en charge cette fonction (RNDIS pour Windows, cdc_ether et usbnet pour Linux) doivent être installés. XClarity Controller fournit un fichier INF pour Windows qui permet à Windows de reconnaître le périphérique USB XClarity Controller en tant que périphérique RNDIS.

Sélectionnez la méthode utilisée par XClarity Controller pour affecter à des adresses aux nœuds finaux Ethernet sur USB.

- **Utiliser l'adresse de type lien local IPv6 pour Ethernet via USB** : Cette méthode utilise les adresses IPv6 basées sur l'adresse MAC qui sont affectés aux nœuds finaux Ethernet sur USB. Normalement, l'adresse IPv6 locale de liaison est générée à l'aide de l'adresse MAC (RFC 4862) mais Windows 2008 et les systèmes d'exploitation 2016 les plus récents ne prennent pas en charge une adresse IPv6 de type lien local statique sur l'hôte de l'interface. Au lieu de cela, le comportement Windows par défaut consiste

à regénérer des adresses de type lien local aléatoires lors de son exécution. Si l'interface XClarity Controller sur USB est configurée pour utiliser le mode d'adresse de type lien local IPv6, les différentes fonctions qui utilisent cette interface ne fonctionneront pas car XClarity Controller ne connaît pas l'adresse que Windows a affecté à l'interface. Si le serveur exécute Windows, utilisez l'une des autres méthodes de configuration d'adresse Ethernet sur USB ou désactivez le comportement Windows par défaut à l'aide de la commande :
`netsh interface ipv6 set global randomizeidentifiers=disabled`

- **Configurer le paramètre IPv4 pour Ethernet via USB** : Cette méthode indique les adresses IP et le masque réseau qui sont affectés à XClarity Controller et côté serveur de l'interface Ethernet sur USB.

  Remarques :

  – Vous devez configurer manuellement l'adresse IP de l'interface Ethernet sur USB dans le système d'exploitation local après avoir configuré l'adresse IP XClarity Controller, l'adresse IP du système d'exploitation et le masque de réseau.

  – Le paramètre d'adresse IP du système d'exploitation est utilisé pour que XClarity Controller détecte l'extrémité opposée du réseau Ethernet sur USB (système d'exploitation) à des fins de communication, telles que l'état du programme de surveillance ou la mise à jour du microprogramme intrabande.

Le mappage de numéros de port Ethernet externes à des numéros de port Ethernet via USB s'effectue en cliquant sur la case à cocher **Activer le réacheminement de port Ethernet externe à Ethernet via USB** et en complétant les données de mappage pour les ports que vous souhaitez réacheminer de l'interface de gestion réseau vers le serveur.

Configuration SNMP

Les informations de cette rubrique vous permettent de configurer des agents SNMP.

Procédez comme suit pour configurer les paramètres d'alerte SNMP de XClarity Controller.

1. Cliquez sur **Réseau** sous **Configuration du contrôleur BMC**.
2. Sélectionnez la case à cocher correspondante pour activer **Agent SNMPv3**, **Interruption SNMPv1**, **Interruption SNMPv2** et/ou **Interruption SNMPv3**.

   Remarques :

   - Pour activer l'agent **SNMPv3**, un contact et un emplacement BMC doivent être spécifiés.
   - Une fois l'agent **SNMPv3** activé, vous pouvez configurer SNMPv3 pour chaque compte utilisateur XClarity Controller.
   - Pour recevoir des interruptions, les interruptions SNMP et l'agent SNMPv3 doivent être activés
3. Si vous activez **Interruption SNMPv1** ou**Interruption SNMPv2**, renseignez les champs suivants :
   a. Dans le champ **Nom de la communauté**, entrez le nom de la communauté ; le nom ne peut pas être vide.
   b. Dans le champ **Hôte**, entrez l'adresse de l'hôte.
4. Si l'option **Interruption SNMPv3** est activée, renseignez les champs suivants :
   a. Dans le champ **ID moteur**, entrez l'ID de moteur. L'ID de moteur ne peut pas être vide.
   b. Dans le champ **Port récepteur d'interruption**, entrez le numéro de port. Le numéro de port par défaut est 162.
5. Si vous activez les interruptions SNMP, sélectionnez les types d'événement suivants pour lesquels vous souhaitez être alerté :
   - **Critique**
   - **Attention**

- **Système**

Remarque : Cliquez sur chaque catégorie principale pour sélectionner plus avant les types d'événement de sous-catégorie pour lesquels vous souhaitez être alerté.

6. Si l'**agent SNMPv3** est activé, renseignez les éléments suivants :
   a. Cliquez sur **Utilisateur/LDAP** dans la **Configuration BMC**.
   b. Cliquez sur le bouton **Modifier** à côté de l'utilisateur correspondant, puis cochez **SNMP** dans la liste déroulante de l'**interface accessible par l'utilisateur**.

Remarque : Cliquez sur le bouton **Envoyer** à côté de **Envoyer une interruption test** pour vérifier les paramètres SNMP.

Activation de l'accès réseau IPMI

Les informations de cette rubrique vous indiquent comment contrôler l'accès réseau IPMI à XClarity Controller.

Procédez comme suit pour activer l'accès IPMI sur LAN.

1. Cliquez sur **Réseau** sous **Configuration BMC** pour afficher ou modifier les paramètres IPMI de XClarity Controller.
2. Cliquez sur le commutateur **IPMI sur LAN** sous **Activation de service et affectation de port** afin d'activer l'accès réseau IPMI à XClarity Controller.
3. Cliquez sur **Utilisateur/LDAP** dans la **Configuration BMC**.
4. Cliquez sur le bouton **Modifier** à côté de l'utilisateur correspondant, puis cochez **IPMI sur LAN** dans la liste déroulante de l'**interface accessible par l'utilisateur**.

Important :

- Si vous n'utilisez pas d'outils ou d'application ayant accès à XClarity Controller via le réseau utilisant le protocole IPMI, il est fortement recommandé de désactiver l'accès réseau IPMI pour une sécurité accrue.
- L'accès IPMI sur LAN au module XClarity Controller est désactivé par défaut.

Configuration des paramètres réseau à l'aide de commandes IPMI

Les informations de cette rubrique vous permettent de configurer les paramètres réseau à l'aide de commandes IPMI.

Étant donné que chaque paramètre réseau du module BMC est configuré à l'aide de demandes IPMI distinctes et dans aucun ordre particulier, le module BMC n'a pas une vision complète de tous les paramètres réseau tant qu'il n'est pas redémarré pour appliquer les modifications du réseau en attente. La demande de modification d'un paramètre réseau peut réussir au moment où la demande est faite, mais être ensuite déclarée non valide lorsque des changements supplémentaires sont demandés. Si les paramètres réseau en attente sont incompatibles au redémarrage du module BMC, les nouveaux paramètres ne seront pas appliqués. Après avoir redémarré le module BMC, essayez d'y accéder à l'aide des nouveaux paramètres afin de vérifier qu'ils ont été appliqués comme prévu.

Activation du service et affectation de port

Les informations de cette rubrique vous indiquent comme afficher ou modifier les numéros de port utilisés par certains services dans XClarity Controller.

Cliquez sur **Réseau** sous **Configuration BMC** pour afficher ou modifier les affectations de port XClarity Controller. Renseignez les zones suivantes pour afficher ou modifier les affectations de ports :

HTTPS (Web/Redfish)
Cet élément est toujours activé. Dans cette zone, spécifiez le numéro de port pour Web via HTTPS. La valeur par défaut est 443.

Présence à distance
Cet élément est toujours activé. Le numéro de port est 443.

Réseau local (IPMI) sur LAN
Le numéro de port est 623. Cette zone n'est pas configurable par l'utilisateur.

Remarque : Assurez-vous que **IPMI sur LAN** est sélectionné et appliqué dans le champ **Interface accessible par l'utilisateur** pour l'utilisateur correspondant à la page Utilisateur/LDAP.

SSDP
Le numéro de port est 1900. Cette zone n'est pas configurable par l'utilisateur.

SSH
Dans cette zone, spécifiez le numéro de port configuré pour l'accès à l'interface de ligne de commande à l'aide du protocole SSH. La valeur par défaut est 22.

Agent SNMP
Dans cette zone, spécifiez le numéro de port pour l'agent SNMP s'exécutant dans XClarity Controller. La valeur par défaut est 161. Les valeurs de numéro de port valides sont comprises entre 1 et 65535.

Remarque : Assurez-vous que **SNMP** est sélectionné et appliqué dans le champ **Interface accessible par l'utilisateur** pour l'utilisateur correspondant à la page Utilisateur/LDAP.

Configuration de la restriction d'accès

Les informations de cette rubrique vous indiquent comment afficher ou modifier les paramètres qui bloquent l'accès des adresses IP ou des adresses MAC à XClarity Controller.

Cliquez sur **Réseau** sous **Configuration BMC** pour afficher ou modifier les paramètres de contrôle d'accès de XClarity Controller.

Liste de blocage et restriction de temps

Ces options vous permettent de bloquer des adresses IP/MAC spécifiques pour un laps de temps spécifique.

- **Liste des adresses IP bloquées**
  - Vous pouvez entrer jusqu'à trois adresses IPv4 ou plages et trois adresses IPv6 ou plages séparées par des virgules, qui ne sont pas admises pour accéder à XClarity Controller. Reportez-vous aux exemples IPv4 ci-dessous :
  - Exemple d'adresse IPv4 unique : 192.168.1.1
  - Exemple d'adresse IPv4 supernet : 192.168.1.0/24
  - Exemple de plage IPv4 : 192.168.1.1 à 192.168.1.5
- **Listes des adresses MAC bloquées**
  - Vous pouvez entrer jusqu'à trois adresses MAC séparées par des virgules, qui ne sont pas admises pour accéder à XClarity Controller. Par exemple : 11:22:33:44:55:66.
- **Accès restreint (unique)**
  - Vous pouvez planifier un intervalle unique pendant lequel XClarity Controller est inaccessible. Pour l'intervalle que vous indiquez :

  - Les date et heure de début ne doivent pas être postérieures à l'heure XCC en cours.
  - Les date et heure de fin ne doivent pas être postérieures aux date et heure de début.
- **Accès restreint (quotidien)**
  - Vous pouvez planifier un ou plusieurs intervalles quotidiens pendant lesquels XClarity Controller est inaccessible. Pour chaque intervalle que vous indiquez :
  - Les date et heure de fin ne doivent pas être postérieures aux date et heure de début.

Liste de blocage déclenché de manière externe

Ces options vous permettent de configurer le blocage automatique d'adresses IP spécifiques (IPv4 et IPv6) à partir desquelles le client a tenté de se connecter successivement à XClarity Controller avec un nom d'utilisateur ou un mot de passe incorrect.

Le blocage automatique détermine de façon dynamique lorsqu'un trop grand nombre d'échecs de journalisation se produit à partir d'une adresse IP spécifique et empêche cette adresse d'accéder à XClarity Controller pour une durée déterminée.

- **Nombre maximum d'échecs de connexion à partir d'une adresse IP spécifique**
  - Le nombre maximal de fois fait référence au nombre d'échecs de journalisation autorisés pour un utilisateur avec un mot de passe incorrect à partir d'une adresse IP spécifique, avant qu'elle ne soit verrouillée.
  - Si la valeur est 0, l'adresse IP n'est jamais verrouillée en raison d'échecs de journalisation.
  - Le compteur d'échecs de connexion pour l'adresse IP spécifique est remis à zéro après chaque connexion réussie à partir de cette adresse IP.
- **Période de verrouillage pour le blocage d'une adresse IP**
  - La durée minimale (en minutes) qui doit s'écouler avant qu'un utilisateur puisse de nouveau tenter de se connecter à partir d'une adresse IP verrouillée.
  - Si la valeur est 0, l'accès à partir de l'adresse IP verrouillée reste bloqué jusqu'à ce que l'administrateur le déverrouille explicitement.
- **Liste de blocage**
  - Le tableau Liste de blocage affiche toutes les adresses IP verrouillées. Vous pouvez déverrouiller une ou l'ensemble des adresses IP de la liste de blocage.

Configuration du port USB du panneau frontal pour la gestion

Les informations de cette rubrique vous indiquent comment configurer le port USB du panneau frontal de XClarity Controller.

La connexion à XClarity Controller est destinée principalement à une utilisation avec un appareil mobile exécutant l'application mobile Lenovo XClarity. Lorsqu'un câble USB est connecté entre l'appareil mobile et le panneau frontal du serveur, une connexion Ethernet sur USB est établie entre l'application mobile s'exécutant sur l'appareil et XClarity Controller.

Sur certains serveurs, le port USB du panneau frontal peut être commuté pour être relié au serveur ou à XClarity Controller.

Remarque : Cette fonctionnalité sera prise en charge dans une future mise à jour.

Configuration des paramètres de sécurité

Les informations de cette rubrique vous permettent de configurer les protocoles de sécurité.

Remarque : Le paramètre de version TLS minimum par défaut est TLS 1.2, mais vous pouvez configurer XClarity Controller pour utiliser d'autres versions TLS nécessaires à vos applications de navigateur ou de gestion. Pour plus d'informations, voir « Commande tls » à la page 138.

Cliquez sur **Sécurité** sous **Configuration du contrôleur BMC** pour accéder et configurer les propriétés de sécurité, l'état, et les paramètres de XClarity Controller.

Tableau de bord de sécurité

Cette rubrique fournit une présentation du tableau de bord de sécurité.

Le tableau de bord de sécurité livre une évaluation globale relative à la sécurité et à l'état du système.

- Les **événements de sécurité BMC** signalent des événements déclarés par des problèmes de sécurité, par exemple, une intrusion dans le châssis, une corruption détectée par PFR, une incohérence matérielle détectée par la protection du système, l'ouverture d'un cavalier de sécurité sur une carte, etc.
- Le **mode de sécurité BMC** présente un état général de la conformité au mode de sécurité.
- Les **services et ports BMC** énumèrent tous les ports/services non sécurisés qui sont actuellement activés, mais non conformes au mode de sécurité actuel.
- Les **certificats BMC** présentent tous les certificats non conformes utilisés par XCC.
- Les **comptes utilisateur BMC** fournissent des suggestions d'ordre général pour rendre la gestion du compte et des mots de passe plus sécurisée.

Remarque : Le tableau de bord affiche une icône d'avertissement en cas de risque dans ces zones de sécurité contrôlées par XCC. Le lien **Détails** de chaque catégorie permet également à l'utilisateur de résoudre les problèmes depuis la page de configuration.

Mode de sécurité

Cette rubrique fournit une présentation du mode de sécurité.

La licence XCC standard permet aux utilisateurs de configurer leurs serveurs selon l'un des deux modes de sécurité : le mode standard et le mode compatibilité. Ces derniers sont disponibles pour tous les serveurs V4.

La licence de mise à niveau Premier Lenovo XClarity Controller 3 est livrée avec un troisième mode de sécurité : le mode Enterprise Strict. Ce mode convient plus particulièrement aux exigences de sécurité de haut niveau.

Remarque : Par défaut, XCC utilise un certificat ECDSA autosigné et seuls des algorithmes basés sur ECDSA sont disponibles. Pour utiliser un certificat basé sur RSA, générez une demande de signature de certificat et faites la signer par une autorité de certification interne ou externe, puis importez le certificat signé dans XCC.

Mode de sécurité Enterprise Strict

- Le mode de sécurité Enterprise Strict est le mode le plus sécurisé.
- Tous les algorithmes de chiffrement utilisés par BMC sont compatibles avec CNSA 1.0.
- BMC fonctionne en mode validé FIPS 140-3.
- Nécessite des certificats de niveau Enterprise Strict.
- Seuls les services qui prennent en charge le chiffrement CNSA 1.0 peuvent être activés.
- Nécessite la fonction Feature on Demand pour être activé.

Mode de sécurité standard

- Le mode standard est le mode de sécurité par défaut.
- Tous les algorithmes de cryptographie utilisés par BMC sont compatibles avec FIPS 140-3.
- BMC fonctionne en mode validé FIPS 140-3 lorsque tous les services activés utilisent un chiffrement conforme à la norme FIPS 140-3.
- Nécessite des certificats de niveau standard.
- Les services nécessitant un chiffrement qui ne prend pas en charge le chiffrement conforme à la norme FIPS 140-3 sont désactivés par défaut.

Mode compatibilité.

- Le mode compatibilité est le mode à utiliser lorsque les services et les clients nécessitent un chiffrement non compatible avec Enterprise Strict/standard.
- Une plus grande gamme d'algorithmes de chiffrement est prise en charge.
- Lorsque ce mode est activé, BMC **NE FONCTIONNE PAS** en mode standard validé.
- Permet d'activer tous les services.

Algorithmes de cryptographie TLS pris en charge

Le paramètre cryptographique TLS sert à limiter les algorithmes de cryptographie TLS pris en charge par les services BMC.

Algorithmes de cryptographie TLS	Mode de sécurité	Version TLS
TLS_AES_256_GCM_SHA384	• Enterprise Strict • Standard* • Compatibilité*	TLS 1.3
TLS_CHACHA20_POLY1305_SHA256	• Compatibilité	TLS 1.3
TLS_AES_128_GCM_SHA256	• Normal • Compatibilité	TLS 1.3
TLS_AES_128_CCM_SHA256	• Normal • Compatibilité	TLS 1.3
TLS_AES_128_CCM_8_SHA256	• Normal • Compatibilité	TLS 1.3
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	• Enterprise Strict • Standard* • Compatibilité*	TLS 1.2
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	• Enterprise Strict • Compatibilité*	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	• Enterprise Strict	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	• Normal • Compatibilité	TLS 1.2

Algorithmes de cryptographie TLS	Mode de sécurité	Version TLS
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	• Normal • Compatibilité	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ SHA256	• Normal • Compatibilité	TLS 1.2
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305	• Compatibilité	TLS 1.2
TLS_ECDHE_ECDSA_WITH_CHACHA20_ POLY1305	• Compatibilité	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	• Normal • Compatibilité	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	• Normal • Compatibilité	TLS 1.2
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	• Normal • Compatibilité	TLS 1.2
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	• Normal • Compatibilité	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_ SHA384	• Normal • Compatibilité	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_ SHA256	• Normal • Compatibilité	TLS 1.2
TLS_RSA_WITH_AES_256_GCM_SHA384	• Normal • Compatibilité	TLS 1.2
TLS_RSA_WITH_AES_128_GCM_SHA256	• Normal • Compatibilité	TLS 1.2
TLS_DHE_RSA_LATH_AES_256_GCM_SHA384	• Normal	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA3U	• Normal	TLS 1.2
TLS_RSA_WITH_AES_256_CBC_SHA256	• Normal	TLS 1.2
TLS_RSA_WITH_AES_128_CBC_SHA256	• Normal	TLS 1.2

Remarque : Les modes de sécurité avec un astérisque (*) répertoriés dans le tableau nécessitent une licence de mise à niveau Premier Lenovo XClarity Controller 3.

Matrice de service dans les trois modes de sécurité

Fonctionnalité/service	Utilise le chiffrement	État par défaut	Pris en charge en mode strict	Pris en charge en mode standard	Pris en charge en mode compatibilité
IPMI sur KCS	Non	Activé	Oui	Oui	Oui
IPMI sur LAN	Oui	Désactivé	Non	Oui	Oui
Interruptions SNMPv1	Non	Non configurées	Non	Oui	Oui
Interruptions SNMPv3	Oui	Non configurées	Non	Oui Si activées, elles permettent d'avertir l'utilisation d'un chiffrement non-FIPS	Oui
Agent SNMPv3	Oui	Non configurées	Non	Oui Si activées, elles permettent d'avertir l'utilisation d'un chiffrement non-FIPS	Oui
Alertes e-mail	Oui	Non configurées	Oui Ne peuvent PAS être activées avec l'authentification CRAM-MD5	Oui Si CRAM-MD5 est requis, elles permettent d'avertir l'utilisation d'un chiffrement non-FIPS.	Oui
Alertes Syslog	Non	Non configurées	Non	Oui	Oui
TLS 1.2	Oui	Activé	Oui	Oui	Oui
TLS 1.3	Oui	Activé	Oui	Oui	Oui
Web via HTTPS	Oui	Activé	Oui	Oui	Oui
Redfish sur HTTPS	Oui	Activé	Oui	Oui	Oui
SSDP	Non	Activé	Oui	Oui	Oui
SSH-CLI	Oui	Activé	Oui	Oui	Oui
SFTP	Oui	Désactivé	Oui	Oui	Oui
LDAP	Non	Non configuré	Non	Oui	Oui
LDAP sécurisé	Oui	Non configuré	Oui	Oui	Oui
Gestion de la clé de sécurité	Oui	Non configuré	Oui	Oui	Oui
Console distante	Oui	Activé	Oui	Oui	Oui
Support virtuel - CIFS	Oui	Non configuré	Non	Oui	Oui

Fonctionnalité/service	Utilise le chiffrement	État par défaut	Pris en charge en mode strict	Pris en charge en mode standard	Pris en charge en mode compatibilité
Support virtuel - NFS	Non	Non configuré	Non	Oui	Oui
Support virtuel - HTTPFS	Oui	Non configuré	Oui	Oui	Oui
RDOC - Local	Oui	Non configuré	Oui	Oui	Oui
RDOC - CIFS	Oui	Non configuré	Non	Oui	Oui
RDOC - HTTP	Non	Non configuré	Non	Oui	Oui
RDOC - HTTPS	Oui	Non configuré	Oui	Oui	Oui
RDOC - FTP	Non	Non configuré	Non	Oui	Oui
RDOC - SFTP	Oui	Non configuré	Oui	Oui	Oui
Chargement FFDC (SFTP)	Oui	Activé	Oui	Oui	Oui
Chargement FFDC (TFTP)	Non	Activé	Non	Oui	Oui
Mise à jour à partir du référentiel - CIFS	Oui	Non configuré	Non	Oui	Oui
Mise à jour à partir du référentiel - NFS	Non	Non configuré	Non	Oui	Oui
Mise à jour à partir du référentiel - HTTP	Non	Non configuré	Non	Oui	Oui
Mise à jour à partir du référentiel - HTTPS	Oui	Non configuré	Oui	Oui	Oui
Appel vers Lenovo	Oui	Désactivé	Oui	Oui	Oui
Mot de passe tiers	Oui	Non configuré	Non	Oui	Oui
Réacheminement de port	N/A	Désactivé	Oui	Oui	Oui

Passage au mode de sécurité

Les informations de cette rubrique vous permettent de passer à un autre mode de sécurité et de le valider.

Le mode standard est le mode de sécurité par défaut.

De manière générale, si XCC détecte un paramètre non conforme au mode standard, XCC affiche une notification, mais ne demande toutefois pas à l'utilisateur de modifier le mode. Dans ce cas, XCC passe en mode de sécurité standard avec remplacement (non conforme).

L'utilisateur peut alors accéder au menu déroulant afin de sélectionner un mode différent, puis utiliser la fonction **Valider** afin de déterminer le nombre d'éléments non conformes détectés par XCC.

XCC valide les éléments conformes lorsque l'utilisateur clique sur **Appliquer**.

Présentation de SSL

Cette rubrique fournit une présentation du protocole de sécurité SSL.

SSL est un protocole de sécurité qui assure la confidentialité des communications. SSL permet aux applications client/serveur de communiquer en empêchant les écoutes, la contrefaçon et la falsification des messages. Vous pouvez configurer XClarity Controller afin qu'il utilise la prise en charge SSL pour différents types de connexions, comme le serveur Web sécurisé (HTTPS), la connexion LDAP sécurisée, la connexion CIM via HTTPS et le serveur SSH, et pour gérer les certificats qui sont nécessaires pour SSL.

Traitement des certificats SSL

Cette rubrique fournit des informations sur l'administration des certificats qui peuvent être utilisés avec le protocole de sécurité SSL.

Les clients WEB, Redfish et LDAP utilisent la même configuration de certificat. La connexion SSL doit être rétablie à chaque fois que vous souhaitez modifier la configuration du certificat SSL. SSL peut être utilisé soit avec un certificat autosigné, soit avec un certificat signé par une autorité de certification tierce. L'utilisation d'un certificat autosigné est la méthode la plus simple pour utiliser SSL, mais au prix d'un faible risque de sécurité. Le risque provient du fait que le client SSL n'a aucun moyen de valider l'identité du serveur SSL pour la première tentative de connexion entre le client et le serveur. Il est possible qu'un tiers malveillant se fasse passer pour le serveur et intercepte les données circulant entre XClarity Controller et le navigateur. Si le certificat autosigné est importé dans le magasin de certificats du navigateur lors de la première connexion entre le navigateur et XClarity Controller, toutes les communications futures avec le navigateur seront sécurisées (sous réserve que la première connexion n'a pas été compromise par une attaque). Après avoir utilisé la page Gestion des certificats SSL pour générer une paire de clés et un certificat autosigné, SSL peut être activé.

Pour une sécurité plus complète, utilisez un certificat signé par une autorité de certification (CA). Pour obtenir un certificat signé :

- Sélectionnez **Générer une demande de signature de certificat (CSR)** depuis l'icône **Générer** sous **Gestion de certificat SSL**.
- Remplissez les champs obligatoires et sélectionnez **Générer**.
- Une fois qu'un certificat autosigné est généré, il est affiché dans **Gestion de certificat SSL**.
- Sélectionnez **Télécharger la demande de signature de certificat (CSR)** à partir de l'icône **Télécharger** pour télécharger le certificat signé.
- Lorsque le certificat signé est téléchargé, sélectionnez l'icône **Importer un certificat signé** sous **Gestion de certificat de l'autorité de certification** pour l'importer dans XClarity Controller.

La fonction de l'autorité de certification est de vérifier l'identité de XClarity Controller. Un certificat contient des signatures numériques pour l'autorité de certification et le BMC. Si une autorité de certification fiable émet le certificat ou si le certificat de l'autorité de certification a déjà été importé dans le navigateur Web, le navigateur sera en mesure de valider le certificat et d'identifier avec certitude le serveur Web BMC.

Veuillez noter que SSL compare le nom d'hôte XClarity Controller (ou nom commun) dans le certificat avec le nom d'hôte tel qu'il apparaît dans votre navigateur Web.

Gestion des certificats SSL

Cette rubrique fournit des informations sur les actions qui peuvent être sélectionnées pour la gestion des certificats à l'aide du protocole de sécurité SSL.

Cliquez sur **Sécurité** sous **Configuration BMC** pour configurer la gestion des certificats SSL.

Lors de la gestion des certificats de XClarity Controller, vous disposez des actions suivantes :

Télécharger le certificat signé
Utilisez ce lien pour télécharger une copie du certificat actuellement installé. Le certificat peut être téléchargé au format PEM ou DER. Le contenu du certificat peut être consulté à l'aide d'un outil tiers tel que OpenSSL (http://www.openssl.org). Voici un exemple de la ligne de commande pour l'affichage du contenu du certificat à l'aide de OpenSSL :
```
openssl x509 -in cert.der -inform DER -text
```

Télécharger la demande de signature de certificat (CSR)
Utilisez ce lien pour télécharger une copie de la demande de signature de certificat. La demande de signature de certificat peut être téléchargée au format PEM ou DER.

Générer un certificat signé
Générer un certificat auto-signé. Une fois l'opération terminée, SSL peut être activé à l'aide du nouveau certificat.

Remarque : Lors de l'exécution de l'action **Générer un certificat signé**, une fenêtre Générer un certificat auto-signé pour HTTPS s'affiche. Vous êtes invité(e) à compléter les zones obligatoires et facultatives. Les zones obligatoires **doivent impérativement** être renseignées. Une fois que vous avez entré les informations, cliquez sur **Générer** pour terminer la tâche.

Générer la demande de signature de certificat (CSR).
Générer une demande de signature de certificat (CSR). Une fois l'opération terminée, le fichier de demande de signature de certificat peut être téléchargé et envoyé à une autorité de certification (CA) pour la signature.

Remarque : Lors de l'exécution de l'action **Générer une demande de signature de certificat**, une fenêtre Générer une demande de signature de certificat pour HTTPS s'affiche. Vous êtes invité(e) à compléter les zones obligatoires et facultatives. Les zones obligatoires **doivent impérativement** être renseignées. Une fois que vous avez entré les informations, cliquez sur **Générer** pour terminer la tâche.

Importer un certificat signé
Cette option permet d'importer un certificat signé. Pour obtenir un certificat signé, il est nécessaire de générer au préalable une demande de signature de certificat et de l'envoyer à une autorité de certification.

Configuration du serveur Secure Shell

Les informations de cette rubrique vous indiquent comment activer le protocole de sécurité SSH.

Cliquez sur **Réseau** sous **Configuration BMC** pour configurer le serveur SSH.

Pour utiliser le protocole SSH, il est nécessaire de générer au préalable une clé pour activer le serveur SSH.

Remarques :

- Aucune gestion de certificat n'est requis pour utiliser cette option.
- Le module XClarity Controller crée initialement une clé de serveur SSH. Si vous souhaitez générer une nouvelle clé de serveur SSH, cliquez sur **Réseau** sous **Configuration BMC** ; puis cliquez sur **Générer une clé** sous **Serveur SSH**.
- Une fois l'action terminée, redémarrez XClarity Controller pour que vos modifications prennent effet.

Accès IMPI sur Keyboard Controller Style (KCS)

Les informations de cette rubrique vous indiquent comment contrôler l'accès IPMI sur Keyboard Controller Style (KCS) à XClarity Controller.

XClarity Controller fournit une interface IPMI via le canal KCS qui ne nécessite pas d'authentification.

Cliquez sur **Sécurité** sous **Configuration BMC** pour activer ou désactiver **Accès IPMI sur KCS**.

Remarques :

- Une fois les paramètres modifiés, vous devez redémarrer XClarity Controller pour que vos modifications prennent effet.
- **Désactivé (activer à la demande)** permet de désactiver le canal KCS la plupart du temps. Toutefois, cela permet également à certains outils Lenovo d'échanger des informations avec XClarity Controller pendant la fenêtre de mise à jour du microprogramme du système. Lorsque cela se produit, le canal KCS est activé brièvement pendant quelques minutes, puis désactivé à la fin ou lors du dépassement du délai d'attente.

Important : Si vous n'utilisez pas d'outils ou d'application sur le serveur ayant accès à XClarity Controller via le réseau utilisant le protocole IPMI, il est fortement recommandé de désactiver l'accès IPMI sur KCS pour améliorer la sécurité. XClarity Essentials utilise l'interface IPMI sur KCS avec XClarity Controller. Si vous avez désactivé l'interface IPMI sur KCS, réactivez-la avant d'exécuter XClarity Essentials sur le serveur. Ensuite, désactivez l'interface lorsque vous avez terminé.

Comment éviter de revenir au niveau antérieur du microprogramme du système -

Les informations de cette rubrique vous indiquent comment éviter que le microprogramme du système ne passe à des niveaux de microprogramme plus anciens.

Cette fonction vous permet d'autoriser ou non le microprogramme du système à revenir à un niveau de microprogramme plus ancien.

Cliquez sur **Réseau** sous **Configuration BMC** pour activer ou désactiver **Empêcher de revenir au niveau antérieur du microprogramme du système**.

Toutes les modifications apportées prennent effet immédiatement sans qu'il soit nécessaire de redémarrer XClarity Controller.

Configuration du serveur de gestion de clé de sécurité (SKM)

Les informations de cette rubrique vous permettent de créer et gérer des clés de sécurité.

Cette fonction utilise un serveur de gestion de clé centralisé pour fournir des clés qui déverrouillent le matériel de stockage, afin d'accéder à des données stockées sur des SED sur un serveur ThinkSystem. Le serveur de gestion de clé inclut le serveur de gestion de clé SKLM - IBM SED, et les serveurs de gestion de clé KMIP - Thales.Gemalto SED (KeySecure et CipherTrust).

Remarque : Cette fonctionnalité sera prise en charge dans une future mise à jour.

Gestionnaire des mots de passe de sécurité

Les informations de cette rubrique vous permettent d'autoriser les mots de passe tiers.

Cette fonctionnalité permet à l'utilisateur d'autoriser ou non l'utilisation de mots de passe tiers.

- **Mots de passe tiers** : si leur utilisation est activée, BMC est alors en mesure d'utiliser un hachage de mot de passe fourni par un utilisateur en vue de l'authentification.
- **Autoriser la récupération de mots de passe tiers** : L'utilisateur peut en outre activer ou désactiver la récupération du hachage de mot de passe tiers depuis BMC.

Journal d'audit étendu

Les informations de cette rubrique vous permettent de contrôler le journal d'audit étendu.

Cette fonction vous permet de décider si vous souhaitez inclure ou non les entrées de journal de la commande set d'IPMI (données brutes) depuis les canaux LAN et KCS dans le journal d'audit.

Cliquez sur **Sécurité** sous **Configuration BMC** dans l'interface Web de XCC pour activer/désactiver le journal d'audit étendu.

Remarque : Si la commande set d'IPMI provient du canal LAN, le nom d'utilisateur et l'adresse IP source sont inclus dans le message de journal. Toutes les commandes IPMI avec des informations de sécurité sensibles (par exemple, le mot de passe) sont exclues.

Limite de connexions simultanées par compte utilisateur

Les informations de cette rubrique vous indiquent comment limiter les sessions simultanées par compte utilisateur.

Cette fonctionnalité permet à un utilisateur de décider combien de sessions simultanées sont autorisées par compte utilisateur.

- **Nombre de sessions Web simultanées** : Cette option peut être définie sur 1 à 10 sessions.
- **Nombre de sessions de ligne de commande simultanées** : Cette option peut être définie sur 1 ou 2 sessions.
- **Nombre de sessions Redfish simultanées** : Cette option peut être définie sur 1 à 16 sessions.

Remarque : Si le nombre total de sessions dépasse la valeur définie, l'utilisateur ne peut plus créer de nouvelle session.

Protection du système

La présente rubrique décrit la protection du système.

Les fonctionnalités System Guard réalisent un instantané de l'inventaire des composants matériels pour s'en servir en tant que référence fiable. Ensuite, elles surveillent tout écart par rapport à cet instantané. En cas

d'écart, elles sont est en mesure de signaler un événement à l'utilisateur. En option, elles peuvent également prévenir l'amorçage du serveur dans le SE et avertir l'utilisateur afin qu'il réagisse.

L'utilisateur peut réaliser un instantané à tout moment, même lorsque la fonctionnalité est désactivée. La génération d'un instantané prend environ une minute. L'utilisateur peut sélectionner un sous-ensemble de composants matériels à appliquer et sélectionner une mesure correspondante à prendre en cas de détection d'écart.

Remarque : La détection de l'écart se produit au moment de l'alimentation du serveur (POST), ou du redémarrage du système. Par exemple, lorsque le SE est en cours d'exécution, si un disque est retiré, puis inséré à nouveau, la protection du système ne va pas enregistrer d'événement, ou lancer d'action. Si le disque retiré demeure absent jusqu'au prochain redémarrage, alors la protection du système va agir.

Remarques : Lors de la restauration de l'alimentation en courant alternatif suivie de la première mise sous tension, XCC peut ne pas avertir l'UEFI d'empêcher l'amorçage du SE si les conditions suivantes sont remplies :

- Protection du système activé avec :
  - Matériel **UC** ou **DIMM** sélectionné
  - Option **Empêcher l'amorçage du système d'exploitation** activée
- Une modification de la configuration matérielle qui ne correspond pas à un instantané fiable.

Le XCC signale une non-concordance de configuration après POST et cette limitation ne persiste pas au prochain redémarrage du système d'exploitation.

Activation de la protection du système

Les informations de cette rubrique vous permettent d'activer la protection du système.

Par défaut, les fonctionnalités System Guard sont désactivées. Toutefois, elles sont activées avant la livraison si l'utilisateur final l'exige.

L'option de réinitialisation des valeurs par défaut de XCC désactive la protection du système et efface les paramètres, sauf l'historique des instantanés.

Lors de l'activation de System Guard, l'utilisateur doit confirmer les paramètres, utiliser un instantané existant et fiable, ou capturer l'inventaire afin de créer un nouvel instantané fiable avant d'activer System Guard. Une fois cette fonctionnalité activée :

- Si l'alimentation système est désactivée, la protection du système commence immédiatement à collecter l'inventaire matériel.
- Si l'alimentation système est activée, alors la fonctionnalité de protection du système compare les données d'inventaire du composant avec l'instantané fiable.

Si le résultat de la comparaison indique un écart par rapport à l'instantané fiable, XCC affiche un avertissement de **non-conformité relatif à une non-concordance de la configuration matérielle**. Les détails de la non-concordance énumèrent chaque composant manquant/modifié/les nouveaux composants, ainsi que leurs attributs d'emplacement/d'identification/leurs descriptions, en les comparant avec l'instantané fiable.

L'utilisateur peut configurer la portée et l'action de la protection du système. Il peut en outre décider les mesures à prendre lorsque le système devient non conforme par le biais du panneau Portée et action.

Prise en charge de la version TLS

Les informations de cette rubrique vous permettent de comprendre les différents versions TLS prises en charge.

Les versions TLS suivantes sont prises en charge :

- TLS 1.2 et ultérieure
- TLS 1.3

Pour obtenir la liste complète des suites de chiffrement TLS prises en charge, voir « Algorithmes de cryptographie TLS pris en charge » à la page 39

Sauvegarde et restauration de la configuration BMC

Les informations de cette rubrique vous expliquent comment restaurer ou modifier la configuration BMC.

Sélectionnez **Sauvegarde et restauration** sous **BMC Configuration** pour effectuer les actions suivantes :

- Afficher un récapitulatif de configuration du contrôleur de gestion
- Sauvegarder et restaurer la configuration de contrôleur de gestion
- Afficher l'état de sauvegarde et de restauration
- Réinitialiser la configuration du contrôleur de gestion à ses paramètres d'usine par défaut.
- Accéder à l'assistant de configuration initiale du contrôleur de gestion

Sauvegarde de la configuration BMC

Les informations de cette rubrique vous expliquent comment sauvegarder votre configuration BMC.

Sélectionnez **Sauvegarde et restauration** sous **Configuration BMC**. Dans la partie supérieure figure la section **Configuration BMC de sauvegarde**.

Si une sauvegarde a été précédemment effectuée, vous voyez les détails dans la zone **Dernière sauvegarde**.

Pour sauvegarder la configuration BMC en cours, suivez les étapes indiquées ci-dessous :

1. Spécifiez le mot de passe pour le fichier de sauvegarde BMC.
2. Indiquez si vous voulez chiffrer l'intégralité du fichier ou uniquement les données sensibles.
3. Démarrez le processus de sauvegarde en cliquant sur **Démarrer la sauvegarde**. Au cours du processus, vous n'êtes pas autorisé à exécuter des actions de restauration/réinitialisation.
4. Lorsque la procédure est terminée, un bouton s'affiche pour vous permettre de télécharger et de sauvegarder le fichier.

Remarque : Lorsque l'utilisateur définit un nouvel utilisateur/mot de passe XClarity Controller et effectue une sauvegarde de la configuration, le compte/mot de passe par défaut (`USERID/PASSWORD`) est également inclus. Supprimer par la suite le compte/mot de passe par défaut à partir de la sauvegarde fera apparaître un message dans le système indiquant à l'utilisateur qu'il y a une défaillance de la restauration du compte/mot de passe XClarity Controller. Les utilisateurs peuvent ignorer ce message.

Restauration de la configuration BMC

Les informations de cette rubrique vous expliquent comment restaurer la configuration BMC.

Sélectionnez **Sauvegarde et restauration** sous **Configuration BMC**. Au-dessous de **Sauvegarder la configuration BMC** figure la section **Restauration de BMC à partir d'un fichier de configuration**.

Pour restaurer BMC à partir d'une configuration précédemment enregistrée, suivez les étapes indiquées ci-dessous :

1. Sélectionnez le fichier de sauvegarde et saisissez le mot de passe lorsque vous y êtes invité(e), puis cliquez sur **Suivant >**.
2. Vérifiez le fichier en cliquant sur **Afficher les détails**.
3. Après avoir vérifié le contenu, cliquez sur **Démarrer la restauration**.

Réinitialisation de BMC aux paramètres d'usine par défaut

Les informations de cette rubrique vous expliquent comment réinitialiser les paramètres d'usine par défaut de BMC.

Sélectionnez **Sauvegarde et restauration** sous **Configuration BMC**. Au-dessous de **Restaurer BMC à partir d'un fichier de configuration** figure la section **Réinitialisation avec les paramètres d'usine BMC par défaut**.

Pour réinitialiser BMC avec les paramètres d'usine par défaut, suivez les étapes indiquées ci-dessous :

1. Cliquez sur **Démarrer la réinitialisation des paramètres d'usine BMC**.

   Remarques :

   - Seuls les utilisateurs disposant du niveau d'autorisation Superviseur peuvent exécuter cette action.
   - La connexion Ethernet est temporairement désactivée. Vous devez de nouveau vous connecter à l'interface Web de XClarity Controller une fois l'opération de réinitialisation terminée.
   - Dès que vous cliquez sur **Démarrer la réinitialisation des paramètres d'usine BMC**, une fenêtre contextuelle de confirmation s'affiche. Vous pouvez alors cocher les cases afin de sélectionner les paramètres ci-après :
     - **Conserver les paramètres de l'utilisateur local** : L'utilisateur/le rôle/le paramètre global actuel sera sauvegardé. Ceci permet de restaurer la commande CLI de contenu « users »/« roles »/ « accesscfg ». Par exemple : Nom d'utilisateur/nom du rôle/avertissement d'expiration du mot de passe/règles de complexité du mot de passe activées, etc.
     - **Conserver les paramètres réseau** : Les paramètres réseau actuels seront sauvegardés. Ceci permet de restaurer la sortie réseau de la commande CLI « ifconfig ». Par exemple : Nom d'hôte/ adresse ipv4/adresse ipv6/passerelle, etc.
   - Dès que vous cliquez sur **OK**, toutes les modifications de configuration précédentes sont effacées, sauf celles que vous décidez de conserver.
   - Si vous souhaitez activer LDAP lors de la restauration de la configuration BMC, vous devez d'abord préalablement importer un certificat de confiance.
   - Si vous travaillez depuis le système local BMC, votre connexion TCP/IP sera, par conséquent, perdue. Vous devrez configurer à nouveau l'interface réseau BMC afin de restaurer la connectivité.
   - Une fois le processus terminé, XClarity Controller redémarre.
   - La réinitialisation du module BMC aux paramètres d'usine par défaut n'affectera pas les paramètres UEFI et le mode d'accès (mono/multi-utilisateur) de la console distante (ces paramètres sont enregistrés dans les cookies du navigateur).

Redémarrage de XClarity Controller

Les informations de cette rubrique vous expliquent comment redémarrer XClarity Controller.

Pour plus d’informations sur le redémarrage de XClarity Controller, voir « Actions d'alimentation » à la page 63.

Chapitre 4. Surveillance de l'état du serveur

Les informations de ce chapitre vous expliquent comment afficher et surveiller les informations sur le serveur auquel vous accédez.

Une fois que vous êtes connecté(e) à XClarity Controller, une page d'état du système s'affiche. Dans cette page, vous pouvez afficher l'état du matériel serveur, les journaux d'événements et d'audit, l'état du système, l'historique de maintenance et les destinataires d'alerte.

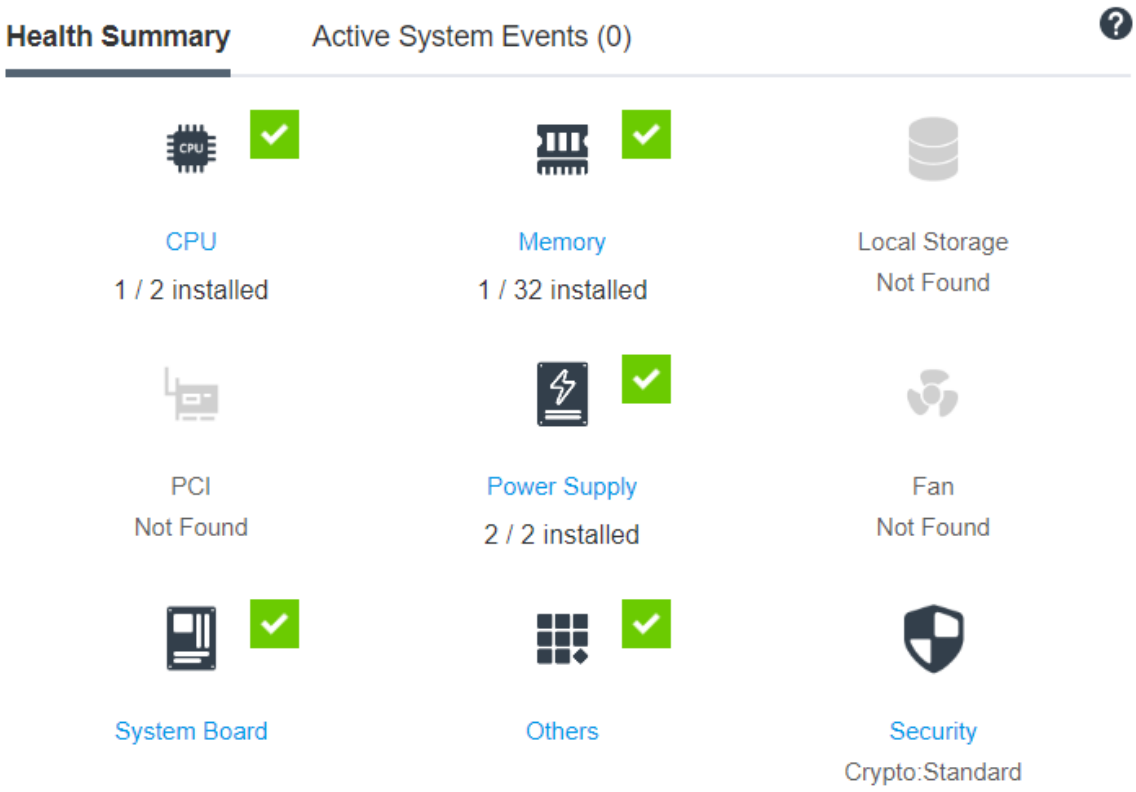
Affichage de l'état d'intégrité/des événements système actifs

Les informations de cette rubrique vous permettent de comprendre comment afficher le récapitulatif d’intégrité/Événements système actifs.

Lorsque vous accédez à la page d’accueil de XClarity Controller, la page **Récapitulatif d'intégrité** est affichée par défaut. Une représentation graphique est fournie, qui indique le nombre de composants matériels qui ont été installés et leur état d'intégrité respectif. Les composants matériels surveillés sont les suivants :

- UC (processeur)
- Mémoire
- Stockage local
- Adaptateurs PCI
- Bloc d'alimentation
- Ventilateur
- Carte mère
- Autres
- Sécurité

Remarque : Stockage local peut afficher l’icône d’état **non disponible** sur les systèmes avec une configuration de fond de panier à remplacement standard.



Si l'un des composants matériels ne fonctionne pas normalement, il est associé à une icône indiquant un état critique ou un avertissement. Une condition critique est indiquée par une icône représentant un cercle rouge, tandis qu'une condition d'avertissement est indiquée par une icône représentant un triangle jaune. Si vous survolez avec l'icône de la souris sur le signe Critique ou Avertissement, jusqu'à trois événements actuellement actifs du composant s'affichent.

Pour afficher les autres événements, cliquez sur l'onglet **Événements système actifs**. Une fenêtre affiche alors les événements qui sont actuellement actifs sur le système. Cliquez sur **Afficher tous les journaux des événements** pour afficher tout l'historique des événements.

Si le composant matériel est signalé par une coche verte, il fonctionne normalement et il n'y a aucun événement actif.

Le texte figurant sous le composant matériel indique le nombre de composants installés. Si vous cliquez sur ce texte (lien), vous êtes redirigé(e) à la page **Inventaire**.

Remarque : Dans les nœuds compatibles avec le châssis D3 V2, le lien **bloc d'alimentation** est uniquement disponible sur le nœud responsable.

Affichage des informations système

Cette rubrique explique comment obtenir un récapitulatif des informations de serveur communes.

Le panneau **Informations système et paramètres** situé à droite de la page d'accueil fournit un récapitulatif des informations de serveur communes, qui comprennent les éléments suivants :

- Nom de machine, état d'alimentation et de système d'exploitation
- Type/modèle de machine
- Numéro de série
- Nom du système
- Port USB du panneau frontal pour la gestion

  Remarque : Cette fonctionnalité sera prise en charge dans une future mise à jour.
- Licence BMC
- Adresse IP BMC
- Nom d'hôte BMC
- Responsable du châssis actif

  Remarque : Cet élément est uniquement disponible sur les nœuds compatibles du châssis D3 V2.
- Version BMC
- Version UEFI
- Emplacement

Le serveur peut se trouver dans l'un des états de système listés dans le tableau suivant.

Tableau 2. Descriptions des états de système

Tableau à deux colonnes avec en-têtes indiquant les états système du serveur.

État	Description
Système hors tension/État inconnu	Le serveur est hors tension.
System sous tension/démarrage UEFI	Le serveur est sous tension mais UEFI n'est pas en cours d'exécution.
Système fonctionnant dans UEFI	Le serveur est sous tension et UEFI est en cours d'exécution.
Système d'exploitation en cours d'amorçage ou dans un système d'exploitation non pris en charge (le système peut être dans cet état si le système d'exploitation ne répond pas aux pings)	Le serveur peut se trouver dans cet état pour l'une des raisons suivantes : • Le chargeur du système d'exploitation a démarré mais le système d'exploitation n'est pas en cours d'exécution. • L'interface Ethernet via USB du module BMC est désactivée. • Le système d'exploitation n'a pas chargé les pilotes prenant en charge l'interface Ethernet via USB.
Système d'exploitation amorcé	Le système d'exploitation du serveur est en cours d'exécution.
Système exécuté en test mémoire	Le serveur est sous tension et exécute des outils de diagnostic de la mémoire.

Tableau 2. Descriptions des états de système (suite)

État	Description
Système exécuté en mode configuration	Le serveur est sous tension et a démarré dans le menu de configuration F1 UEFI ou le menu LXPM.
Système fonctionnant en mode de maintenance LXPM	Le serveur est sous tension et le système a démarré en mode maintenance LXPM qui empêche les utilisateurs de naviguer dans le menu LXPM.

Si vous souhaitez modifier le nom de système, cliquez sur l'icône représentant un crayon. Saisissez le nom de système que vous souhaitez utiliser, puis cliquez sur la coche verte.

Si votre serveur dispose d'une licence autre que la licence de niveau Premier XClarity Controller, vous pouvez peut-être acheter une mise à niveau de licence pour activer les fonctionnalités améliorées. Pour installer la licence de mise à niveau que vous avez obtenue, cliquez sur l'icône représentant une flèche pointant vers le haut.

Pour ajouter, supprimer ou exporter une licence, cliquez sur l'icône représentant une flèche pointant vers la droite.

Pour modifier les paramètres pertinents relatifs à l'adresse IP BMC, le nom d'hôte BMC, la version UEFI, la version BMC et les éléments d'emplacement, cliquez sur la flèche pointant vers la droite.

- Pour l'adresse IP et le nom d'hôte, vous êtes redirigé(e) à la section **Configuration Ethernet** sous **Réseau**.
- Pour les éléments de version UEFI et BMC, vous êtes redirigé(e) à la page **Mise à jour du microprogramme**.
- Pour l'élément d'emplacement, vous êtes redirigé(e) à la section **Propriétés du serveur** sur la page **Configuration du serveur**.

Affichage de l'utilisation du système

Lorsque vous cliquez sur **Utilisation** dans le panneau de gauche, un récapitulatif des informations communes d'utilisation du serveur s'affiche.

L'utilisation du système est une mesure composite basée sur l'utilisation en temps réel du processeur, de la mémoire et des sous-systèmes d'E-S. Les données d'utilisation peuvent être consultées dans la vue Graphique ou la vue Tableau, qui comprend les éléments suivants :

- **Température**
  - Permet d'afficher la température ambiante en temps réel et des températures des composants clés.

  - Survoler le curseur de la souris au-dessus d'un module de mémoire permet d'afficher sa température actuelle.
- **Utilisation de l'alimentation**
  - Permet d'afficher le graphique circulaire de la consommation d'énergie actuelle.
  - Survoler le curseur de la souris sur le graphique circulaire permet également d'afficher la consommation d'énergie actuelle.
  - Le graphique circulaire sur la consommation d'énergie actuelle comprend quatre catégories : UC, mémoire, autre et de secours. « Autre » fait référence à la consommation d'énergie totale du système, hors la consommation d'énergie de l'UC et de la mémoire. « De secours » fait référence à l'alimentation totale allouée et disponible, hors la consommation d'énergie totale du système.
  - L'onglet Tension permet d'afficher les valeurs et les états de tension actuels concernant tous les capteurs de tension pris en charge par le matériel.
- **Utilisation du système**
  - Permet d'afficher une représentation d'un instantané d'utilisation actuelle du système, ainsi que des sous-système du processeur, de la mémoire et d'E-S.

    Remarque : Cette fonctionnalité sera prise en charge dans une future mise à jour.
- **Vitesse du ventilateur (tr/min)**
  - La section relative à la vitesse du ventilateur indique, sous la forme d'un pourcentage de la vitesse maximale, la vitesse du ventilateur.
  - L'utilisateur peut cliquer sur l'icône engrenage afin d'accéder aux options **Augmentation de la vitesse du ventilateur**.
    - Ce paramètre permet d'apporter un refroidissement supplémentaire au serveur, et ce, en fonction de la température ambiante. Il permet d'augmenter la vitesse du ventilateur au-delà de la vitesse normale en contrôlant l'algorithme thermique. Il n'y aura aucun changement si les ventilateurs fonctionnent déjà à plein régime.

Affichage des journaux des événements

Le **journal des événements** fournit une liste historique de l'ensemble des événements de gestion et concernant le matériel.

Sélectionnez **Journal des événements** dans **Événements** pour afficher la page **Journal des événements**. Tous les événements recensés dans le journal sont accompagnés d'un horodatage qui utilise les paramètres de date et d'heure de XClarity Controller. Certains événements génèrent également des alertes s'ils sont configurés en conséquence sur la page **Destinataires de l'alerte**. Vous pouvez trier et filtrer les événements dans le journal des événements.

Voici une description des actions qui peuvent être exécutées dans la page **Journal des événements**.

- **Personnaliser la table** : Sélectionnez cette action pour sélectionner le type d'informations que vous souhaitez à l'écran dans la table. Un numéro de séquence peut être affiché pour déterminer l'ordre des événements lorsque plusieurs événement ont le même horodatage.

  Remarque : Certains numéros de séquence sont utilisés par les processus internes BMC, il est donc normal que des espaces soient présents dans les numéros de séquence lorsque les événements sont triés par numéro de séquence.
- **Effacer les journaux** : Sélectionnez cette action pour supprimer les journaux des événements.
- **Actualiser** : Sélectionnez cette action pour mettre à jour l'affichage de entrées du journal des événements qui ont pu se produire depuis le dernier affichage de la page.

- **Type** : Sélectionnez les types d'événements à afficher. Les types d'événement sont les suivants :
  -  Affiche les entrées d’erreur du journal
  -  Affiche les entrées d’avertissement du journal
  -  Affiche les entrées d’information du journal

  Cliquez sur chaque icône pour activer ou désactiver les types d'erreur à afficher. Cliquez sur l'icône successivement pour alterner entre l'affichage ou non des événements. Un encadré noir entourant l’icône indique que le type d’événement sera affiché.
- **Type de filtre de source** : Sélectionnez un élément dans le menu déroulant pour afficher uniquement le type d'entrées du journal des événements à afficher.
- **Filtre de temps** : Sélectionnez cette action pour indiquer l'intervalle des événements que vous voulez afficher.
- **Rechercher** : Pour rechercher des types d'événement ou de clés spécifiques, cliquez l'icône de loupe, et entrez un mot à rechercher dans la zone **Rechercher**. Notez que l'entrée est sensible à la casse.

Remarque : Le nombre maximal d'enregistrements de journal des événements est de 1024. Une fois les journaux des événements saturés, la nouvelle entrée de journal remplace automatiquement la plus ancienne.

Affichage des journaux d'audit

Le **Journal d'audit** fournit une archive de l'historique des actions utilisateur, comme la connexion à XClarity Controller, la création d'un utilisateur ou la modification d'un mot de passe utilisateur.

Vous pouvez utiliser le journal d'audit pour suivre et consigner l'authentification, les modifications et les actions système.

Le journal des événements et le journal d'audit prennent tous deux en charge des actions de maintenance et d'affichage similaires. Pour afficher la description des actions d’affichage et de filtrage pouvant être exécutées sur la page du journal d’audit, voir « Affichage des journaux des événements » à la page 55.

Remarques :

- Après avoir exécuté les outils Lenovo sur votre système d'exploitation du serveur, le Journal d'audit peut contenir des enregistrements d'actions effectuées par un nom d'utilisateur (« 20luN4SB » par exemple) que vous pouvez ne pas reconnaître. Lorsqu'ils sont exécutés sur le système d'exploitation du serveur, certains outils peuvent créer un compte d'utilisateur temporaire pour accéder au XClarity Controller. Le compte est créé avec un nom d'utilisateur et un mot de passe aléatoires et ne sert qu'à accéder au XClarity Controller sur l'interface Ethernet sur USB interne. Le compte ne peut être utilisé que pour accéder aux interfaces Redfish et SFTP du XClarity Controller. La création et la suppression de ce compte temporaire sont consignées dans le journal d'audit comme toute autre action effectuée par l'outil à l'aide de ces données d'identification.
- Le nombre maximal d'enregistrements de journal d'audit est de 1024. Une fois les journaux d'audit saturés, la nouvelle entrée de journal remplace automatiquement la plus ancienne.

Affichage de l'historique de maintenance

La page **Historique de maintenance** contient des informations sur l'historique des mises à jour de microprogramme, de configuration et de remplacement du matériel.

Le contenu de l'historique de maintenance peut être filtré pour afficher certains types d'événements ou certains intervalles de temps.

Remarque : Le nombre maximal d'enregistrements d'historique de maintenance est de 250. Une fois les journaux d'historique de maintenance saturés, la nouvelle entrée de journal remplace automatiquement la plus ancienne.

Configuration des destinataires de l'alerte

Utilisez les informations de la présente rubrique pour ajouter et modifier les destinataires de notifications par e-mail et syslog ou d’interruptions SNMP.

Remarque : Cette fonctionnalité sera prise en charge dans une future mise à jour.

Chapitre 5. Configuration du serveur

Les informations de ce chapitre vous permettent de comprendre les options disponibles pour les configurations de serveur.

Lors de la configuration du serveur, les options suivantes sont disponibles :

- Adaptateurs
- Options d'amorçage
- Règles d'alimentation
- Propriétés du serveur
- Châssis

  Remarque : Cet élément est uniquement disponible sur les nœuds compatibles du châssis D3 V2.

Affichage des informations et des paramètres de configuration de l'adaptateur

Les informations de cette rubrique vous permettent d'afficher des informations sur les adaptateurs installés sur le serveur.

Cliquez sur l'option **Adaptateurs** sous l'onglet **Configuration de serveur** pour afficher des informations sur les adaptateurs PCIe installés sur le serveur.

Remarque : Si l'adaptateur ne prend pas en charge la surveillance de l'état, il ne sera pas visible pour la surveillance ou la configuration. Pour les informations relatives à l'inventaire de tous les adaptateurs PCI installés, consultez la page **Inventaire**.

Configuration du mode d'amorçage système et de l'ordre d'amorçage

Pour configurer le mode et l'ordre d'amorçage du système, utilisez les informations de cette rubrique.

Lorsque vous sélectionnez **Options d’amorçage** sous **Configuration du serveur**, vous pouvez configurer l’ordre d’amorçage du système.

Remarque : Aucune méthode interne non authentifiée n'est autorisée à modifier les paramètres système liés à la sécurité. Par exemple, l'amorçage sécurisé ne doit PAS être en mesure de configurer via des API internes non authentifiées depuis le système d'exploitation ou l'interpréteur de commandes UEFI. Cela inclut l'exécution en interne de OneCLI et l'obtention de données d'identification temporaires à l'aide d'IPMI ou de tout outil et API pour configurer les paramètres liés à l'amorçage sécurisé, TPM et le mot de passe de l'installation UEFI. Tous les paramètres liés à la sécurité doivent nécessiter une authentification appropriée disposant de privilèges suffisants.

Pour configurer l'ordre d'amorçage du système, sélectionnez une unité dans la liste **Unités disponibles** et cliquez sur la flèche droite pour ajouter l'unité dans l'ordre d'amorçage. Pour supprimer une unité de l'ordre d'amorçage, sélectionnez une unité dans la liste d'ordre d'amorçage et cliquez sur la flèche gauche pour replacer l'unité dans la liste des unités disponibles. Pour modifier l'ordre d'amorçage, sélectionnez une unité et cliquez sur la flèche vers le haut ou vers le bas pour positionner l'unité dans l'ordre de priorité.

Lorsque vous modifiez l'ordre d'amorçage, vous devez sélectionner une option de redémarrage avant d'appliquer la modification. Les options suivantes sont disponibles :

- **Redémarrer le serveur immédiatement** : Les modifications de l'ordre de amorçage sont enregistrées et le serveur est redémarré immédiatement sans arrêter le système d'exploitation.
- **Redémarrer le serveur normalement** : Les modifications de l'ordre de amorçage sont enregistrées et le système d'exploitation est arrêté avant le redémarrage du serveur.
- **Redémarrer manuellement plus tard** : Les modifications de l'ordre de amorçage seront enregistrées, mais n'entreront pas en vigueur avant le prochain redémarrage du serveur.

Configuration d'amorçage unique

Pour ignorer temporairement l'amorçage configuré et amorcer exceptionnellement sur une unité spécifiée unique, utilisez les informations de cette rubrique.

Cliquez sur **Options d'amorçage** sous **Configuration du serveur** et sélectionnez une unité dans le menu déroulant pour configurer l'unité sur laquelle le système démarrera exceptionnelle au prochain redémarrage du serveur. Vous avez plusieurs possibilités :

Réseau PXE
Configure votre serveur de sorte de tenter un amorçage réseau PXE (Preboot Execution Environment).

Support amovible primaire
Le serveur est démarré de l'unité USB par défaut.

CD/DVD par défaut
Le serveur est démarré à partir de l'unité CD/DVD par défaut.

Configuration du système F1
Le serveur est démarré dans le Lenovo XClarity Provisioning Manager.

Diagnostic de partition
Le serveur est démarré dans la section Diagnostics du Lenovo XClarity Provisioning Manager.

Disque dur par défaut
Le serveur est démarré à partir de l'unité de disque par défaut.

Support éloigné primaire
Le serveur est initialisé à partir du support virtuel monté.

Monté
L'ordre d'amorçage configuré est utilisé. Il n'y a pas d'autre amorçage que l'ordre d'amorçage configuré.

Démarrage non unique
L'ordre d'amorçage configuré est utilisé. Il n'y a pas d'autre amorçage que l'ordre d'amorçage configuré.

Lorsque vous sélectionnez de modifier exceptionnellement l'ordre d'amorçage, vous devez sélectionner une option de redémarrage avant d'appliquer la modification.

- **Redémarrer le serveur immédiatement** : La modification apportée à l'ordre de amorçage est enregistrée et le serveur est redémarré immédiatement sans arrêter le système d'exploitation.
- **Redémarrer le serveur normalement** : La modification apportée à l'ordre de amorçage est enregistrée et le système d'exploitation est arrêté avant le redémarrage du serveur.
- **Redémarrer manuellement plus tard** : La modification apportée à l'ordre de amorçage est enregistrée, mais n'entrera pas en vigueur avant le prochain redémarrage du serveur.

Gestion de l'alimentation du serveur

Pour afficher les informations de gestion de l'alimentation et exécuter des fonctions de gestion de l'alimentation, utilisez les informations de cette rubrique.

Sélectionnez l'option **Règles d'alimentation** sous l'onglet **Configuration du serveur** pour afficher des informations relatives à la gestion de l'alimentation et utiliser les fonctions de gestion correspondantes.

Remarque : Dans un boîtier contenant des nœuds de serveur haute densité, le refroidissement et l'alimentation du châssis sont contrôlés par le module SMM et non par XClarity Controller. Reportez-vous à l'interface Web SMM3 pour plus de détails sur l'état d'alimentation de la solution.

Configuration de la redondance d'alimentation

Les informations de cette rubrique vous permettent de configurer la redondance d'alimentation.

Remarques :

- Les serveurs AMD ne prennent pas en charge la configuration de la fonction de politique d'alimentation.
- Lorsque 2 unités d'alimentation électrique sont installées, le mode de redondance est définie sur Redondance (N+N). Avec cette configuration de 2 unités d'alimentation, si l'un des unités d'alimentation est défaillante, si l'alimentation en courant alternatif a été coupée ou a été retirée, elle signale un événement de perte de redondance dans le journal des événements XCC.
- Si une seule unité d'alimentation est installée après l'expédition, le mode de redondance est automatiquement défini sur Non redondant.

Les champs disponibles dans la section de redondance d'alimentation sont les suivants :

- **Redondance (N+N)** : Au moins deux sources d'alimentation indépendantes sont en mesure d'alimenter le système de manière simultanée. Cela signifie qu'en cas de panne d'une ou de plusieurs sources d'alimentation, les autres sources peuvent continuer à alimenter le système, et ce, sans interruption. La redondance N+N offre un haut niveau de tolérance aux pannes. Elle garantit en outre l'état opérationnel du système, même dans l'éventualité de plusieurs défaillances.
  - **Mode zéro sortie** : Une fois le mode Redondant activé, certaines blocs alimentation entrent automatiquement en mode veille en cas de charge peu importante. Ainsi, le bloc d'alimentation restant fournit l'ensemble de la charge d'alimentation pour augmenter l'efficacité.
- **Mode non redondant** : Dans ce mode, le serveur n'est pas assuré de rester opérationnel en cas de perte d'un bloc d'alimentation. Le serveur se régule en cas de panne d'un bloc d'alimentation pour tenter de rester opérationnel.

Cliquez sur **Appliquer** après avoir modifié la configuration.

Configuration de la stratégie de plafonnement énergétique

Les informations de cette rubrique vous permettent de configurer la stratégie de plafonnement énergétique.

Remarques :

- Les serveurs AMD ne prennent pas en charge la configuration de la fonction de politique de plafonnement énergétique.
- Dans un boîtier contenant des nœuds de serveur haute densité, le refroidissement et l'alimentation du châssis sont contrôlés par le module SMM et non par XClarity Controller. Reportez-vous à l'interface Web SMM3 pour plus de détails sur l'état d'alimentation de la solution.

Vous pouvez choisir d'activer ou de désactiver la fonction de plafonnement énergétique. Si le plafonnement énergétique est activé, une sélection peut être effectuée pour limiter la quantité d'énergie utilisée par le serveur. Si le plafonnement énergétique est désactivé, la quantité d'énergie maximale utilisée par le serveur est déterminée par la règle de redondance d'alimentation. Pour modifier le paramètre, cliquez d'abord sur **Réinitialiser**. Sélectionnez vos paramètres favoris ; puis cliquez sur **Appliquer**.

La capacité d'alimentation totale est calculée en fonction du mode de redondance de l'alimentation et du nombre de blocs d'alimentation installés dans le système. Le réglage manuel de la limite d'alimentation maximale peut dépasser la capacité d'alimentation réelle.

Lorsque le plafonnement énergétique est activé, le système peut être limité afin de maintenir la limite en matière d'alimentation.

Remarque : Même lorsque le plafonnement énergétique est désactivé, le système peut être limité si certaines conditions de défaillance surviennent, telles qu'une panne d'alimentation, un problème de refroidissement, etc.

Le plafonnement énergétique peut être activé à l'aide des paramètres **Entrée** ou **Sortie**. Dans le menu déroulant, sélectionnez le type de mesures qui sera utilisé pour déterminer la limite de plafonnement énergétique. Lorsque vous passez d'une mesure à l'autre, le nombre sur le curseur change en conséquence.

Il existe deux méthodes pour modifier la valeur de plafonnement énergétique :

- **Méthode 1** : Déplacez le curseur sur la puissance souhaitée pour définir la limite d'alimentation globale du serveur.
- **Méthode 2** : Entrez la valeur dans la zone d'entrée. Le curseur se déplacera automatiquement à la position correspondante.

Cliquez sur **Appliquer** après avoir modifié la configuration. Les modifications entreront en vigueur immédiatement.

Configuration de la stratégie de restauration de l'alimentation

Pour configurer la manière avec laquelle le serveur réagit lors du rétablissement du courant suite à une coupure d'alimentation, utilisez les informations de cette rubrique.

Pour configurer la stratégie de restauration de l'alimentation, les trois options suivantes sont disponibles :

Toujours désactivé
Le serveur reste hors tension même lorsque le courant est rétabli.

Restaurer
Le serveur est automatiquement mis sous tension lorsque l'alimentation est restaurée si le serveur était sous tension lors de la coupure d'alimentation. Autrement, l'alimentation du serveur reste hors tension même lorsque le courant est rétabli.

Remarque : Cochez la case ci-dessous afin de définir un délai aléatoire compris entre 1 et 15 secondes pour la mise sous tension si le serveur était sous tension avant la panne d'alimentation.

Toujours activé
Le serveur se met automatiquement sous tension une fois l'alimentation restaurée.

Cliquez sur **Appliquer** après avoir modifié la configuration.

Actions d'alimentation

Consultez les informations de cette rubrique pour découvrir les actions d'alimentation qui peuvent être affectées au serveur.

Cliquez sur **Action d'alimentation** dans la section **Action rapide** de la page d'accueil de XClarity Controller.

Le tableau suivant contient une description des actions d'alimentation et de redémarrage pouvant être réalisées sur le serveur.

Tableau 3. Actions d'alimentation et descriptions

Tableau à deux colonnes contenant les descriptions des actions d'alimentation et de redémarrage du serveur.

Action d'alimentation	Description
Mettre le serveur sous tension	Sélectionnez cette action pour mettre le serveur sous tension et démarrer le système d'exploitation.
Mettre le serveur hors tension normalement	Sélectionnez cette action pour arrêter le système d'exploitation et mettre le serveur hors tension.
Mettre le serveur hors tension immédiatement	Sélectionnez cette action pour mettre le serveur hors tension sans arrêter d'abord le système d'exploitation.
Redémarrer le serveur normalement	Sélectionnez cette action pour arrêter le système d'exploitation et effectuer un cycle d'alimentation du serveur.
Redémarrer le serveur immédiatement	Sélectionnez cette action pour éteindre et rallumer le serveur immédiatement, sans arrêter d'abord le système d'exploitation.
Démarrer le serveur pour configurer le système	Sélectionnez cet élément pour mettre sous tension le serveur ou le redémarrer en affichant automatiquement la configuration du système sans avoir besoin d'appuyer sur F1.
Déclencher une interruption non masquable (NMI)	Sélectionnez cette action pour forcer une interruption non masquable (NMI) sur un système « bloqué ». La sélection de cette action permet au système d'exploitation de la plateforme d'effectuer un vidage de mémoire pouvant être utilisé pour déboguer l'état de blocage du système. Le paramètre de redémarrage automatique en cas d'interruption non masquable (NMI) dans le menu de configuration système F1 détermine si XClarity Controller redémarre le serveur après l'interruption non masquable.
Planifier les actions d'alimentation	Sélectionnez cette action pour programmer des actions d'alimentation et de redémarrage quotidiennes et hebdomadaires pour le serveur.
Redémarrer le contrôleur de gestion	Sélectionnez cette action pour redémarrer XClarity Controller.

Tableau 3. Actions d'alimentation et descriptions (suite)

Action d'alimentation	Description
Cycle d'alimentation en courant alternatif du serveur	Sélectionnez cette action pour effectuer un cycle d'alimentation sur le serveur.

Remarques :

- Si le système d'exploitation se trouve en mode écran de veille ou en mode de verrouillage lorsque l'arrêt du système d'exploitation est tenté, XClarity Controller peut ne pas pouvoir déclencher un arrêt normal. XClarity Controller exécutera une réinitialisation ou un arrêt immédiat à l'expiration du délai de mise hors tension, même si le système d'exploitation est toujours en opération.
- Si le voyant d'alimentation du panneau frontal clignote rapidement, il se peut que le XClarity Controller ne puisse pas lancer une séquence de mise sous tension normale. Le XClarity Controller peut mettre le système sous tension une fois que le voyant d'alimentation se met à clignoter lentement.

Gestion et surveillance de la consommation électrique à l'aide de commandes IPMI

Les informations de cette rubrique vous permettent de gérer et de surveiller la consommation électrique à l'aide de commandes IPMI.

Cette rubrique décrit comment la technologie Intel Intelligent Power Node Manager et l'interface DCMI (Data Center Manageability Interface) peuvent être utilisées pour assurer la surveillance électrique et thermique ainsi que la gestion de l'alimentation basée sur une stratégie pour un serveur à l'aide des commandes IPMI (Intelligent Platform Management Interface) de gestion de l'alimentation.

Pour les serveurs qui utilisent le gestionnaire de nœud Intel SPS 3.0, les utilisateurs de XClarity Controller peuvent utiliser les commandes de gestion d'alimentation IPMI fournies par le moteur de gestion d'Intel pour contrôler les fonctions du gestionnaire de nœud et surveiller la consommation d'énergie du serveur. La gestion de l'alimentation du serveur peut également être effectuée à l'aide des commandes de gestion de l'alimentation DCMI. Des exemples de commandes de gestion de l'alimentation DCMI et du gestionnaire de nœud sont fournis dans cette rubrique.

Gestion de l'alimentation du serveur à l'aide des commandes du gestionnaire de nœud

Les informations de cette rubrique vous permettent de gérer l'alimentation du serveur à l'aide du gestionnaire de nœud.

Le microprogramme du gestionnaire de nœud Intel n'a pas d'interface externe. Par conséquent, les commandes du gestionnaire de nœud doivent d'abord être reçues par XClarity Controller avant d'être envoyées au gestionnaire de nœud Intel. XClarity Controller sert de relais et d'unité de transport pour les commandes IPMI à l'aide de la passerelle IPMI standard.

Remarque : Changer les règles du gestionnaire de nœud à l'aide des commandes IPMI du gestionnaire de nœud peut créer des conflits avec la fonction de gestion de l'alimentation de XClarity Controller. Par défaut, la passerelle des commandes du gestionnaire de nœud est désactivée pour empêcher tout conflit.

Pour les utilisateurs qui souhaitent gérer l'alimentation du serveur à l'aide du gestionnaire de nœud au lieu du XClarity Controller, une commande IMPI OEM composée de (fonction de réseau : **0x3A**) et (commande : **0xC7**) est disponible pour utilisation.

Pour activer les commandes IPMI natives du gestionnaire de nœud, tapez : `ipmitool -H` **<$XClarity_ Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x3a 0xc7 0x01**

Pour désactiver les commandes IPMI natives du gestionnaire de nœud, tapez : `ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x3a 0xc7 0x00**

Les informations suivantes sont des exemples de commandes de gestion d'alimentation du gestionnaire de nœud.

Remarques :

- En spécifiant IMPI **canal 0** et l'adresse cible **0x2c**, vous pouvez utiliser l'outil IPMITOOL pour envoyer des commandes au gestionnaire de nœud Intel pour traitement. Un message de demande est utilisé pour lancer une action et un message de réponse est renvoyé au demandeur.
- Les commandes sont affichées dans le format suivant en raison du manque d'espace.

Surveillance de l'alimentation à l'aide de la commande d'obtention des statistiques d'alimentation système globales (code 0xC8) : Demande :`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `-b` **0x00** `-t` **0x2c** `raw` **0x2E 0xC8 0x57 0x01 0x00 0x01 0x00 0x00** Réponse :57 01 00 38 00 04 00 41 00 39 00 ec 56 f7 53 5a 86 00 00 50

Plafonnement énergétique à l'aide de la commande de définition de stratégie du gestionnaire de nœud Intel (code 0xC1) : Demande :`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `-b` **0x00** `-t` **0x2c** `raw` **0x2e 0xC1 0x57 0x01 0x00 0x10 0x01 0xA0 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00 0x00 0x1e 0x00**Réponse :57 01 00

Économies d'énergie à l'aide de la commande de définition de stratégie du gestionnaire de nœud Intel (code 0xC1) : Demande :`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `-b` **0x00** `-t` **0x2c** `raw` **0x2e 0xC1 0x57 0x01 0x00 0x10 0x01 0x00 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00 0x00 0x1e 0x00**

Fonction d'obtention d'ID d'unité à l'aide de la commande d'obtention d'ID de moteur de gestion Intel : Demande :`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `-b` **0x00** `-t` **0x2c** `raw` **0x06 0x01**Réponse :50 01 03 05 02 21 57 01 00 05 0b 03 40 20 01

Pour des commandes supplémentaires du gestionnaire de nœud Intel, voir la dernière édition de **Intel Intelligent Power Node Manager External Interface Specification Using IPMI** sur https://businessportal.intel.com.

Gestion de l'alimentation du serveur à l'aide de commandes DCMI

Les informations de cette rubrique vous permettent de gérer l'alimentation du serveur à l'aide de commandes DCMI.

Le DCMI fournit des fonctions de surveillance et de contrôle qui peuvent être affichées dans des interfaces de logiciel de gestion standard. Les fonctions de gestion de l'alimentation du serveur peut également être exécutées à l'aide des commandes DCMI.

Les informations suivantes sont des exemples de fonctions et de commandes de gestion d'alimentation DCMI couramment utilisées. Un message de demande est utilisé pour lancer une action et un message de réponse est renvoyé au demandeur.

Remarque : Les commandes sont affichées dans les formats suivants en raison du manque d'espace.

Affichage de l'alimentation : Demande :`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x2c 0x02 0xdc 0x01 0x00 0x00** Réponse :`dc 39 00 38 00 3b 00 39 00 e3 6f 0a 39 e8 03 00 00 40`

Définir la limite d'énergie : Demande :`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **PASSW0RD** `raw` **0x2c 0x04 0xdc 0x00 0x00 0x00 0x00 0xA0 0x00 0xe8 0x03 0x00 0x00 0x00 0x00 0xe8 0x03** Réponse :`dc`

Affichage de capacité énergétique : Demande :`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x2c 0x03 0xdc 0x00 0x00** Réponse :`dc 00 00 00 a0 00 e8 03 00 00 00 00 01 00`

Activer la limite d'énergie : Demande :`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x2c 0x05 0xdc 0x01 0x00 0x00** Réponse :`dc`

Désactiver la limite d'énergie : Demande :`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x2c 0x05 0xdc 0x00 0x00 0x00** Réponse :`dc`

Remarque : Sur certains serveurs, les actions d'exception de la commande **Définir la limite d'énergie** peuvent ne pas être prises en charge. Par exemple, le paramètre **Effectuer une mise hors tension matérielle du système et consigner les événements dans le SEL** peut ne pas être pris en charge.

Pour la liste complète des commandes qui sont prises en charge par la spécification DCMI, voir la dernière édition de la **Data Center Manageability Interface Specification** sur https://www.intel.com/content/dam/www/public/us/en/documents/technical-specifications/dcmi-v1-5-rev-spec.pdf.

Téléchargement du journal des données de maintenance

Les informations de cette rubrique permettent de collecter des informations de maintenance sur le serveur. Ce processus n'est normalement effectué qu'à la demande du personnel de maintenance pour contribuer à la résolution d'un problème serveur.

À la page d'accueil de XClarity Controller, cliquez sur l'option **Journal de service** dans la section **Action rapide**, puis sélectionnez **Journal des données de maintenance**.

Par défaut, le journal de maintenance contient les données suivantes : informations système, inventaire du système, utilisation du système, tableau SMBIOS, lecture des capteurs, journal des événements, clé FOD, clé SLP, configuration UEFI et configuration de XClarity Controller 3.

Déplacez la souris sur l'option Informations de base et cliquez sur la fenêtre flottante pour voir certaines des données réelles qui seront exportées.

Bien que les informations de base soient obligatoires, les informations suivantes peuvent également être exportées :

- Informations réseau (IP, nom d'hôte)
- Télémesure (données sur 24 heures)
- Journal d'audit (contient le nom d'utilisateur)
- Dernier écran de défaillance en date

Cliquez sur **Exporter** pour télécharger le journal des données de maintenance.

La réalisation du processus de collecte des données de maintenance et de support nécessite quelques minutes. Le fichier est enregistré dans votre dossier de téléchargement par défaut. La convention de dénomination pour le fichier de données de maintenance suit cette convention :`<machine type and model>_<serial number>_xcc3_ServiceData_<date>-<time>.zip`

Par exemple : 7X2106Z01A_2345678_xcc3_ServiceData_240517-112857.zip.

En plus des données de maintenance au format .zip, le journal de débogage peut également être téléchargé au format de fichier .tar.zst via **Parcourir l'historique...**. La convention de dénomination pour le fichier lodf de débogage suit la convention ci-après : `<machine type and model>_<serial number>_xcc3_DebugLog_<date>-<time>.tar.zst`

Par exemple : 7X2106Z01A_2345678_xcc3_DebugLog_240517-112857.zip.

Remarques :

- **Parcourir l'historique...** permet également de conserver les journaux de service récemment exportés.
- Le format de fichier .tar.zst utilise un algorithme de compression différent et peut être extrait avec le module « zstd ». Par exemple :
  `tar --use-compress-program=unzstd -xvf <machine type and model>_<serial number>_xcc3_DebugLog_<date>-<time>.tar.zst`

Propriétés du serveur

Les informations de cette rubrique vous permettent de modifier ou d'afficher les propriétés du serveur pertinentes.

Définition de l'emplacement et des personnes à contacter

Les informations de cette rubrique vous permettent de définir différents paramètres pour identifier les opérations système et le personnel de support.

Sélectionnez **Propriétés du serveur** sous **Configuration du serveur**, pour configurer les informations **Emplacement et contact**.

Contact
Vous permet de spécifier le nom et le numéro de téléphone de la personne à contacter en cas de problème du système.

Remarque : Ce champ est identique au champ Contact de la configuration SNMPv3 et est obligatoire pour activer le protocole SNMPv3.

Nom de l'armoire
Permet de localiser le serveur plus facilement en indiquant l'armoire dans laquelle il se trouve.

Numéro salle
Permet de localiser le serveur plus facilement en indiquant la salle dans laquelle il se trouve.

Création
Permet de localiser le serveur plus facilement en indiquant l'immeuble dans laquelle il se trouve.

Le U le plus bas
Permet de localiser le serveur plus facilement en indiquant sa position dans l'armoire.

Adresse
Vous permet de spécifier l'adresse postale complète où se trouve le serveur.

Remarque : Lorsque des informations pertinentes ont été entrées, elles apparaissent sous forme d'une ligne unique dans le champ **Emplacement** de la section SNMPv3 et de la page d'accueil du XClarity Controller.

Configuration des délais d'attente du serveur

Les informations de cette rubrique permettent de définir les délais d'attente du serveur.

Ces délais d'attente sont utilisés pour restaurer le fonctionnement d'un serveur qui s'est bloqué.

Sélectionnez **Propriétés du serveur** sous **Configuration du serveur**, pour configurer les délais d'attente du serveur. Les sélections de délai d'attente suivantes du serveur sont affichées :

Activer le délai de mise hors tension

Utilisez cette zone pour spécifier le nombre de minutes pendant lesquelles le sous-système BMC attendra que le système d'exploitation s'arrête avant de mettre le système hors tension.

Pour définir la valeur du délai d'attente de mise hors tension, sélectionnez l'intervalle de temps dans le menu déroulant et cliquez sur **Appliquer**. Pour empêcher la mise hors tension par XClarity Controller, sélectionnez **Aucun** dans le menu déroulant.

Message Trespass

Les informations de cette section vous permettent de créer un message qui est affiché lorsqu'un utilisateur se connecte à XClarity Controller.

Sélectionnez **Propriétés serveur** sous **Configuration du serveur**. Utilisez l'option **Message Trespass** pour configurer un message que vous souhaitez afficher pour l'utilisateur. Lorsque vous avez terminé, cliquez sur **Appliquer**.

Le texte du message s'affichera dans la zone Message de la page de connexion du XClarity Controller à chaque connexion d'utilisateur.

Service de résolution

Les informations de la présente rubrique vous permettent d'activer ou de désactiver le service de solution.

Remarque : Cette fonctionnalité sera prise en charge dans une future mise à jour.

Définition des date et heure XClarity Controller

Les informations de cette rubrique vous permettent de comprendre les paramètres de date et heure XClarity Controller. Les instructions sont fournies pour configurer la date et l'heure du XClarity Controller. La date et l'heure du XClarity Controller sont utilisées pour horodater tous les événements consignés dans le journal des événements et les alertes qui sont envoyées.

Dans la page d'accueil de XClarity Controller, cliquez sur l'icône d'horloge dans l'angle supérieur droit pour afficher ou modifier la date et l'heure du XClarity Controller. Le XClarity Controller n'a pas sa propre horloge en temps réel. Vous pouvez configurer le XClarity Controller de sorte de synchroniser sa date et son heure avec un serveur NTP ou avec l'horloge matérielle en temps réel du serveur.

Synchronisation avec NTP

Pour synchroniser l'horloge du XClarity Controller avec le serveur NTP, procédez comme suit :

- Sélectionnez **Synchronisation de l'horloge avec NTP** et spécifiez l'adresse du serveur NTP.
- Vous pouvez spécifier des serveurs NTP supplémentaires en cliquant sur l'icône « + ».
- Indiquez la fréquence à laquelle vous voulez que XClarity Controller se synchronise avec le serveur NTP.
- L'heure obtenue du serveur NTP est au format UTC (Coordinated Universal Time).
  - Si vous souhaitez que le XClarity Controller règle sa date et son heure sur votre région, sélectionnez le décalage de fuseau horaire correspondant à votre localisation dans le menu déroulant.

  - Si le lieu où vous vous trouvez observe le heure d'été, cochez la case à cocher **Régler automatiquement le passage à l'heure d'été**.
- Lorsque vos modifications de configuration sont terminées, cliquez sur **Appliquer**.

Synchronisation avec l'hôte

L'heure conservée dans l'horloge matérielle en temps réel du serveur peut être au format UTC (Coordinated Universal Time) ou peut avoir déjà été réglée et stockée au format de l'heure locale. Certains systèmes d'exploitation stockent l'horloge en temps réel au format UTC tandis que d'autres stockent l'heure comme l'heure locale. L'horloge en temps réel du serveur n'indique pas le format de l'heure. Par conséquent lorsque le XClarity Controller est configuré de sorte de se synchroniser avec l'horloge en temps réel de l'hôte, l'utilisateur peut choisir la manière avec laquelle le XClarity Controller utilise la date et l'heure provenant de l'horloge en temps réel.

- Local (exemple : Windows) : Dans ce mode, le XClarity Controller traite la date et heure qui proviennent de l'horloge en temps réel comme l'heure locale avec tous les décalages de fuseau horaire et de passage à l'heure d'été (DST) déjà appliqués. Si le lieu où vous vous trouvez observe l'heure d'été, vous pouvez également cocher la case **Régler automatiquement le passage à l'heure d'été**.
- UTC (exemple : Linux) : Dans ce mode, le XClarity Controller traite la date et heure qui proviennent de l'horloge en temps réel comme l'heure UTC (Coordinated Universal Time), sans décalage de fuseau horaire ou de passage à l'heure d'été (DST) déjà appliqué. Dans ce mode, vous pouvez choisir de régler l'heure et la date sur votre région en sélectionnant le décalage de fuseau horaire correspondant à votre localisation dans le menu déroulant. Si le lieu où vous vous trouvez observe l'heure d'été, vous pouvez également cocher la case **Régler automatiquement le passage à l'heure d'été**.
- Lorsque vos modifications de configuration sont terminées, cliquez sur **Appliquer**.

Remarque : Lorsque le passage à l'heure d'été se produit, toute action planifiée pour être exécutée par le XClarity Controller pendant l'intervalle omise par le saut en avant dans le temps de l'horloge ne sera pas effectuée. Par exemple, si l'heure d'été américaine démarre à 02h00 le 12 mars, et qu'une action d'alimentation est programmée à 02h10 le même jour, cette action n'aura pas lieu. Lorsque l'heure atteint 02h00, le XClarity Controller lit 03h00 du matin à la place.

Configuration du châssis D3 V2

Les informations de la présente rubrique vous permettent de comprendre les paramètres du châssis D3 V2.

Cliquez sur **Châssis** sous **Configuration du serveur** pour afficher les informations concernant le châssis D3 V2.

Informations sur le châssis

Cette section affiche les informations sur le châssis, notamment l'UUID, le numéro de série, le type de machine et la version du microprogramme. Elle affiche également les informations sur les nœuds, dont le facteur de forme, l'état de l'alimentation et l'adresse IP.

Remarques :

- Cliquez sur le bouton **Réinitialiser/Réinstaller** à côté du nœud correspondant pour redémarrer le nœud ou simuler la réinstallation d'un nœud physique.
- Seul le nœud responsable ne peut réinitialiser ou réinstaller d'autres nœuds.

Rôle de responsable sur le châssis

Cette section affiche les options de sélection du responsable du châssis.

Remarques :

- Sélectionnez **Participer au rôle de responsable du châssis** afin de permettre à un nœud de participer au processus de sélection du responsable. S'il existe un autre nœud désigné comme responsable permanent, aucun processus de sélection n'aura lieu, sauf si ce nœud est absent.
- Sélectionnez **Désigner ce nœud comme responsable permanent du châssis** si vous voulez qu'un seul nœud soit le responsable. Dans ce cas, il n'y a pas de haute disponibilité pour le rôle de responsable. Si le nœud responsable permanent est absent du châssis, le processus de sélection du responsable se produit pour sélectionner le prochain responsable adéquat.

Historique de maintenance du châssis

L'historique de maintenance du châssis conserve un enregistrement des nœuds ajoutés ou retirés du châssis, ainsi que le changement de rôle de responsable d'un nœud à un autre.

Chapitre 6. Fonctionnalité de console distante

Les informations de cette rubrique vous permettent de comprendre comment afficher et interagir à distance avec la console du serveur.

Vous pouvez utiliser la fonction de console distante dans l'interface Web de XClarity Controller, pour afficher et interagir avec la console du serveur. Vous pouvez affecter une image disque (fichier ISO ou IMG) comme unité virtuelle sur le serveur. La fonctionnalité de console distante est disponible avec les fonctionnalités de niveau Premier de XClarity Controller et n'est disponible que via l'interface Web. Pour utiliser les fonctions de console distante, vous devez vous connecter à XClarity Controller avec un ID disposant d'un accès Superviseur ou de privilèges d'accès à la console distante. Pour plus d'informations sur la mise à jour du niveau standard de XClarity Controller vers le niveau Premier de XClarity Controller, reportez-vous à « Mise à niveau de XClarity Controller » à la page 6.

Utilisez les fonctionnalités de console distante pour effectuer les actions suivantes :

- Visualiser des vidéos à distance avec une résolution graphique allant jusqu'à 1 920 x 1 200 32 bpp/60 Hz, quel que soit l'état du serveur.
- Accéder au serveur à distance à l'aide du clavier et de la souris depuis un client distant.
- Monter les fichiers ISO et IMG qui se trouvent sur votre système local ou sur un système distant en tant qu'unités virtuelles accessibles au serveur.
- Télécharger une image IMG ou ISO vers la mémoire XClarity Controller et montez-la sur le serveur comme unité virtuelle. Jusqu'à deux fichiers d'une capacité totale maximale de 100 Mo peuvent être téléchargés en mémoire XClarity Controller.

Remarques :

- Lorsque la fonction de console distante est démarrée en mode multi-utilisateur, (lorsque les fonctionnalités de niveau Premier sont activées, XClarity Controller prend en charge jusqu'à six sessions simultanées), la fonction de disque distant ne peut être exercée que par une seule session à la fois.
- La console distante est capable d'afficher uniquement la vidéo générée par le contrôleur vidéo de la carte mère. Si un adaptateur de contrôleur vidéo distinct est installé et utilisé à la place de celui du système, la console distante XClarity Controller ne peut pas afficher le contenu de la vidéo depuis l'adaptateur ajouté.
- Si votre réseau contient des pare-feu, un port réseau doit être ouvert pour prendre en charge la fonction de console distante. Pour afficher ou modifier le numéro de port réseau utilisé par la fonction de console distante, voir « Activation du service et affectation de port » à la page 35.
- La fonction de console distante utilise HTML5 pour afficher la vidéo du serveur sur les pages Web. Pour utiliser cette fonction, votre navigateur doit prendre en charge l'affichage de contenu vidéo à l'aide des éléments HTML5.
- Si vous utilisez des certificats auto-signés et une adresse IPv6 pour accéder au contrôleur BMC à l'aide du navigateur Internet Explorer, la session de console distante peut ne pas réussir à démarrer en raison d'une erreur de certificat. Pour éviter ce problème, le certificat auto-signé peut être ajouté aux Autorités de certification racines de confiance d'Internet Explorer :
  - Sélectionnez **Sécurité** sous **Configuration BMC** et téléchargez le certificat auto-signé.
  - Modifiez l'extension du fichier du certificat en *.crt et double-cliquez sur le fichier de certificat Web.
  - Effacez le cache du navigateur IE11.
  - Cliquez sur **Installer le certificat** pour installer le certificat dans le Magasin de certificats en suivant les étapes de l'assistant d'importation de certificat.

Activation de la fonctionnalité de la console distante

Cette rubrique fournit des informations sur la fonctionnalité de console distante.

La fonctionnalité de console distante XClarity Controller n'est disponible que dans les fonctionnalités de niveau Premier de XClarity Controller. Si vous ne disposez pas des droits d'utilisation de la console distante, vous verrez une icône de verrouillage.

Après avoir acheté et récupéré la clé d'activation pour la mise à niveau Premier de XClarity Controller, installez-la en suivant les instructions sous « Installation d'une clé d'activation » à la page 89.

Pour utiliser la fonctionnalité de console distante, cliquez sur l'image avec une flèche blanche pointant en diagonale dans la section **Aperçu de la console distante** de la page d'accueil de XClarity Controller ou à la page Web **Console distante**.

Contrôle à distance de l'alimentation

Cette rubrique explique comment envoyer des commandes d'alimentation et de redémarrage du serveur depuis la fenêtre de la console distante.

Vous pouvez envoyer des commandes de contrôle de l'alimentation et de redémarrage du serveur depuis la fenêtre de la console distante sans qu'il soit nécessaire de revenir à la page Web principale. Pour contrôler l'alimentation du serveur à l'aide de la console distante, cliquez sur **Alimentation** et sélectionnez l'une des commandes suivantes :

Mettre le serveur sous tension
Sélectionnez cette action pour mettre le serveur sous tension et démarrer le système d'exploitation.

Mettre le serveur hors tension normalement
Sélectionnez cette action pour arrêter le système d'exploitation et mettre le serveur hors tension.

Mettre le serveur hors tension immédiatement
Sélectionnez cette action pour mettre le serveur hors tension sans arrêter d'abord le système d'exploitation.

Redémarrer le serveur normalement
Sélectionnez cette action pour arrêter le système d'exploitation et effectuer un cycle d'alimentation du serveur.

Redémarrer le serveur immédiatement
Sélectionnez cette action pour éteindre et rallumer le serveur immédiatement, sans arrêter d'abord le système d'exploitation.

Démarrer le serveur pour configurer le système
Sélectionnez cet élément pour mettre sous tension le serveur ou le redémarrer en affichant automatiquement la configuration du système sans avoir besoin d'appuyer sur F1.

Écran de capture de console distante

Les informations de cette rubrique vous permettent de comprendre comment utiliser la fonction de capture d'écran de console distante.

La fonction de capture d'écran dans la fenêtre de console distante capture le contenu de l'affichage vidéo sur le serveur. Pour capturer et enregistrer une image écran, procédez comme suit :

Etape 1. Dans la fenêtre de la console distante, cliquez sur **Capturer l'écran**.

Etape 2. Dans la fenêtre contextuelle, cliquez sur **Enregistrez le fichier** et appuyez sur **OK**. Le fichier est nommé rpviewer.png et est enregistré dans le dossier de téléchargement par défaut.

Remarque : L'image de capture d'écran est enregistrée au format JPG.

Prise en charge du clavier de la console distante

Dans la fenêtre de la console distante, sous **Clavier**, les éléments suivants sont fournis :

- Cliquez sur **Clavier virtuel** pour lancer le clavier virtuel. Cette fonction est utile si vous utilisez une tablette dépourvue de clavier physique. Les options suivantes peuvent être utilisées pour créer des macros et des combinaisons de touches pouvant être envoyées au serveur. Le système d'exploitation sur le serveur client que vous utilisez peut intercepter certaines combinaisons de touches, telles que Ctrl+Alt+Suppr, au lieu de les transmettre au serveur. D'autres touches, comme F1 ou Esc, peuvent être interceptées par le programme ou le navigateur que vous utilisez. Les macros fournissent un mécanisme pour envoyer des touches au serveur que l'utilisateur peut ne pas pouvoir envoyer.
- Cliquez sur **Macros du serveur** pour utiliser les macros définies par le serveur. Certaines macros du serveur sont prédéfinies par le microprogramme XClarity Controller.

Modes d'écran de console distante

Les informations de cette rubrique vous permettent de configurer les modes d'écran de console distante.

Pour configurer les modes d'écran de console distante, cliquez sur **Mode écran**.

Les options de menu disponibles sont les suivantes :

Plein écran
Ce mode remplit le bureau du client avec l'affichage vidéo. Pour quitter le mode plein écran, appuyez sur la touche Esc. Étant donné que le menu de la console distante n'est pas visible en mode plein écran, vous devez quitter le mode plein écran pour utiliser l'une ou l'autre des fonctions fournies par le menu de la console distante telles que les macros clavier.

Ajustement de l'écran
Il s'agit du paramètre par défaut au lancement de la console distante. Dans ce paramètre, le bureau cible est complètement affiché sans barres de défilement. Le rapport hauteur/largeur est conservé.

Méthodes de montage de support

Les informations de cette rubrique vous permettent de comprendre comment effectuer des montages de support.

Trois mécanismes sont fournis pour monter les fichiers ISO et IMG en tant qu'unités virtuelles.

- Des unités virtuelles peuvent être ajoutées au serveur depuis la session de console distante en cliquant sur **Support**.
- Directement de la page Web de la console distante, sans établir de session de console distante.
- Outil autonome.

Les utilisateurs ont des privilèges **Accès console distante et disques distants** leur permettant d'utiliser les fonctions de support virtuel.

Les fichiers peuvent être montés sous la forme support virtuel depuis votre système local ou un serveur distant, et sont accessibles via le réseau ou téléchargés dans la mémoire XClarity Controller à l'aide de la fonctionnalité RDOC. Ces mécanismes sont décrits ci-après.

- Les supports locaux sont des fichiers ISO ou IMG qui sont situés sur le système que vous utilisez pour accéder au XClarity Controller. Ce mécanisme n'est disponible que via la session de console distante, pas directement depuis la page Web de la console distante, et uniquement avec les fonctionnalités de niveau Premier de XClarity Controller. Pour monter un support local, cliquez sur **Monter tous les supports locaux** dans la section **Monter un fichier de support local**. Jusqu'à quatre fichiers peuvent être montés simultanément sur le serveur.
- Les fichiers qui se trouvent sur un système distant peuvent également être montés en tant que support virtuel. Jusqu'à quatre fichiers peuvent être montés simultanément en tant qu'unités virtuelles. Le XClarity Controller prend en charge les protocoles de partage de fichiers suivants :
  - **CIFS - Common Internet File System** :
    - Entrez l'URL qui localise le fichier sur le système distant.
    - Si vous souhaitez que le fichier soit présenté sur le serveur en tant que support virtuel en lecture seule, cochez la case à cocher.
    - Entrez les données d'identification nécessaires pour permettre au XClarity Controller d'accéder au fichier sur le système distant.

      Remarque : Le XClarity Controller ne prend pas en charge les espaces dans le nom d'utilisateur, le mot de passe ou l'URL. Vérifiez que le serveur CIFS n'ait pas de données d'identification de connexion configurées avec un espace dans le nom d'utilisateur ou le mot de passe et que l'URL ne contient pas d'espace.
    - Les options de montage sont optionnelles et définies par le protocole CIFS.
    - Si le serveur distant appartient à un regroupement de serveurs, où la sécurité est gérée de façon centralisée, entrez le nom de domaine auquel le serveur distant appartient.
  - **NFS - Network File System** :
    - Entrez l'URL qui localise le fichier sur le système distant.
    - Si vous souhaitez que le fichier soit présenté sur le serveur en tant que support virtuel en lecture seule, cochez la case à cocher.
    - Les options de montage sont optionnelles et définies par le protocole NFS. Les protocoles NFSv3 et NFSv4 sont pris en charge. Par exemple, pour utiliser le protocole NFSv3, vous devez indiquer l'option 'nfsvers=3'. Si le serveur NFS utilise la version de sécurité AUTH_SYS pour authentifier les opérations NFS, vous devez indiquer l'option 'sec=sys'.
  - **HTTPFS - HTTP Fuse-based File System** :
    - Entrez l'URL qui localise le fichier sur le système distant.
    - Si vous souhaitez que le fichier soit présenté sur le serveur en tant que support virtuel en lecture seule, cochez la case à cocher.

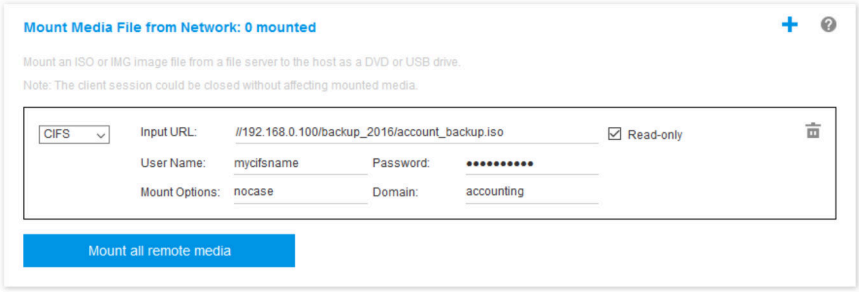
    Remarque : Des erreurs peuvent se produire lors du processus de montage pour les certificats de sécurité générés par Microsoft IIS. Si cela se produit, voir « Problèmes liés aux erreurs de montage de support » à la page 77.

  Cliquez sur **Monter tous les supports distants** pour monter le fichier en tant que support virtuel. Pour supprimer le support virtuel, cliquez sur l'icône de corbeille à droite du support monté.
- Jusqu'à deux fichiers peuvent être téléchargés dans la mémoire de XClarity Controller et être montés en tant que support virtuel à l'aide de la fonctionnalité RDOC de XClarity Controller. La taille totale des deux fichiers ne doit pas dépasser 100 Mo. Ces fichiers resteront dans la mémoire de XClarity Controller

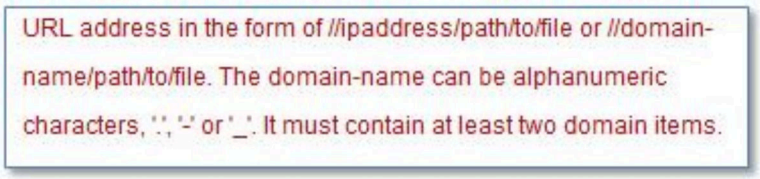
jusqu'à ce qu'ils soient supprimés, même si la session de console distante est terminée. La fonction RDOC prend en charge les mécanismes suivants lors du téléchargement des fichiers :

– **CIFS - Common Internet File System** : Voir la description ci-dessus pour des détails. **Exemple** :

  Pour monter un fichier ISO nommé account_backup.iso qui se trouve dans le répertoire backup_2016 d'un serveur CIFS à l'adresse IP 192.168.0.100 en tant qu'unité virtuelle en lecture seule sur le serveur, vous devez remplir les champs comme indiqué dans la figure ci-dessous. Dans cet exemple, le serveur qui se trouve à l'adresse 192.168.0.100 fait partie d'un ensemble de serveurs sous le domaine « comptabilité ». Le nom de domaine est facultatif. Si votre serveur CIFS ne fait pas partie d'un domaine, laissez le champ **Domaine** vide. L'option de montage CIFS « nocase » est proposée dans le champ **Options de montage** dans cet exemple, indiquant au serveur CIFS que la vérification des majuscules/minuscules du nom de fichier est à ignorer. Le champ **Options de montage** est facultatif. Les informations fournies par l'utilisateur dans ce champ ne sont pas utilisées par le module BMC mais simplement transmises au serveur CIFS lors de la demande de montage. Consultez la documentation de votre implémentation de serveur CIFS pour déterminer quelles options sont prises en charge par votre serveur CIFS.

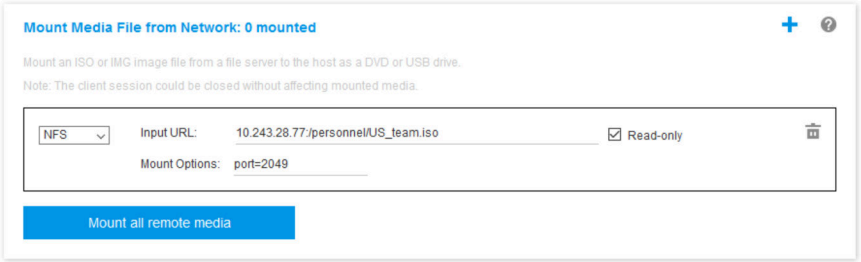


  Le module BMC fournit des conseils lors de la spécification de l'URL. Si l'URL entrée n'est pas valide, le bouton de montage apparaîtra grisé et du texte rouge sera affiché sous le champ URL montrant le format attendu de l'URL.

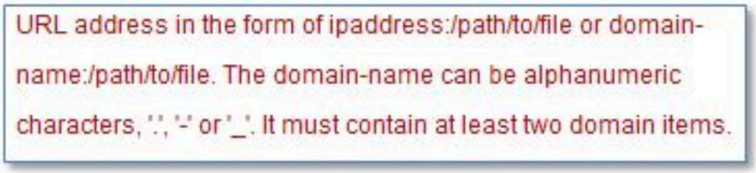


– **NFS - Network File System** : Voir la description ci-dessus pour des détails. **Exemple** :

  Pour monter un fichier ISO nommé US_team.iso qui se trouve dans le répertoire « personnel » d'un serveur NFS à l'adresse IP 10.243.28.77 en tant qu'unité virtuelle en lecture seule sur le serveur, vous devez remplir les champs comme indiqué dans la figure ci-dessous. L'option de montage « port= 2049 » du NFS spécifie que le port réseau 2049 doit être utilisé pour transférer les données. Le champ **Options de montage** est facultatif. Les informations fournies par l'utilisateur dans ce champ sont transmises au serveur NFS lors de la demande de montage. Consultez la documentation de votre implémentation de serveur NFS pour déterminer quelles options sont prises en charge par votre serveur NFS.



Le module BMC fournit des conseils lors de la spécification de l'URL. Si l'URL entrée n'est pas valide, le bouton de montage apparaîtra grisé et du texte rouge sera affiché sous le champ URL montrant le format attendu de l'URL.

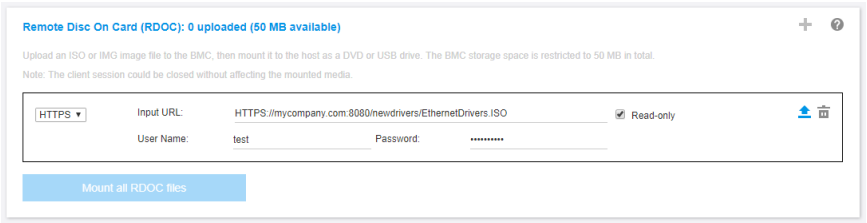


- **HTTPS - Hypertext Transfer Protocol Secure** :
  - Entrez l'URL qui localise le fichier sur le système distant.
  - Si vous souhaitez que le fichier soit présenté sur le serveur en tant que support virtuel en lecture seule, cochez la case à cocher.
  - Entrez les données d'identification nécessaires pour permettre au XClarity Controller d'accéder au fichier sur le système distant.

  Remarques :

  - Des erreurs peuvent se produire lors du processus de montage pour les certificats de sécurité générés par Microsoft IIS. Si cela se produit, voir « Problèmes liés aux erreurs de montage de support » à la page 77.
  - Le XClarity Controller ne prend pas en charge les espaces dans le nom d'utilisateur, le mot de passe ou l'URL. Vérifiez que le serveur CIFS n'ait pas de données d'identification de connexion configurées avec un espace dans le nom d'utilisateur ou le mot de passe et que l'URL ne contient pas d'espace. **Exemple** :

    Pour monter un fichier ISO nommé EthernetDrivers.ISO qui se trouve dans le répertoire « newdrivers » d'un serveur HTTPS avec le nom de domaine « mycompany.com » à l'aide de port de réseau 8080 en tant qu'unité virtuelle en lecture seule sur le serveur, vous devez remplir les champs comme indiqué dans la figure ci-dessous.



    Le module BMC fournit des conseils lors de la spécification de l'URL. Si l'URL entrée n'est pas valide, le bouton de montage apparaîtra grisé et du texte rouge sera affiché sous le champ URL montrant le format attendu de l'URL.

URL address in the form of https://ipaddress[:port]/path/to/file or HTTPS://domain-name[:port]/path/to/file. The domain-name can be alphanumeric characters, '.', '-' or '_'. It must contain at least two domain items. The port number is optional

- **SFTP - SSH File Transfer Protocol**
  - Entrez l'URL qui localise le fichier sur le système distant.
  - Si vous souhaitez que le fichier soit présenté sur le serveur en tant que support virtuel en lecture seule, cochez la case à cocher.
  - Entrez les données d'identification nécessaires pour permettre au XClarity Controller d'accéder au fichier sur le système distant.

  Remarques :

  - Le XClarity Controller ne prend pas en charge les espaces dans le nom d'utilisateur, le mot de passe ou l'URL. Vérifiez que le serveur CIFS n'ait pas de données d'identification de connexion configurées avec un espace dans le nom d'utilisateur ou le mot de passe et que l'URL ne contient pas d'espace.
  - Lorsque le XClarity Controller se connecte à un serveur HTTPS, une fenêtre contextuelle apparaît affichant des informations sur le certificat de sécurité utilisé par le serveur HTTPS. Le XClarity Controller n'est pas en mesure de vérifier l'authenticité du certificat de sécurité.
- **LOCAL - Common Internet File System** :
  - Parcourez le système pour rechercher le fichier ISO ou IMG que vous souhaitez monter.
  - Si vous souhaitez que le fichier soit présenté sur le serveur en tant que support virtuel en lecture seule, cochez la case.

Cliquez sur **Monter tous les fichiers RDOC** pour monter le fichier en tant que support virtuel. Pour supprimer le support virtuel, cliquez sur l'icône de corbeille à droite du support monté.

Outil autonome

Pour les utilisateurs qui ont besoin d'effectuer le montage de périphériques ou d'images(.iso/.img) à l'aide de XClarity Controller, ils peuvent utiliser la partie du code autonome rdmount du paquet OneCLI. Spécifiquement, rdmount ouvrira une connexion vers XClarity Controller et montera l'unité ou les images sur l'hôte.

rdmount présente la syntaxe suivante :

```
rdmount -s ip_address -d <iso or device path> -l <userid> -p <password> -w port (443)
```

Exemple de montage d'un fichier iso :

```
$sudo ./rdmount -s 10.243.11.212 -d /home/user/temp/SLE-15-Installer-DVD-x86_64-RC2-DVD1.iso -l userid -p password -w 443
```

Problèmes liés aux erreurs de montage de support

Les informations de cette rubrique vous permettent de dépanner les problèmes liés aux erreurs de montage de support.

Lors de l'utilisation de certificats de sécurité générés par Microsoft IIS, vous pouvez rencontrer des erreurs pendant le processus de montage. Dans ce cas, remplacez le certificat de sécurité par un nouveau généré par openssl. En particulier, le fichier pfx nouvellement généré est chargé sur le serveur Microsoft IIS.

Voici un exemple qui illustre comment le nouveau certificat de sécurité est généré via openssl sur le système d'exploitation Linux.

```
$ openssl
OpenSSL>

$ openssl genrsa 1024 > server.key
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)

$ openssl req -new -key server.key > server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:BJ
Locality Name (eg, city) []:HD
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Lenovo
Organizational Unit Name (eg, section) []:Lenovo
Common Name (e.g. server FQDN or YOUR name) []:10.245.18.66
Email Address []:test@test.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:LNV

$ ls
server.csr  server.key

$ openssl req -x509 -days 3650 -key server.key -in server.csr > server.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:BJ
Locality Name (eg, city) []:BJ
Organization Name (eg, company) [Internet Widgits Pty Ltd]:LNV
Organizational Unit Name (eg, section) []:LNV
Common Name (e.g. server FQDN or YOUR name) []:10.245.18.66
Email Address []:test@test.com

$ ls
server.crt  server.csr  server.key

$ openssl pkcs12 -export -out server.pfx -inkey server.key -in server.crt
Enter Export Password:
Verifying - Enter Export Password:

$ ls
server.crt  server.csr  server.key  server.pfx
```

Sortie de la session de console distante

Cette rubrique explique comment mettre fin à la session de console distante.

Pour quitter la session de console distante, fermez les fenêtres de console distante et de support virtuel.

Chapitre 7. Configuration du stockage

Les informations de ce chapitre vous permettent de comprendre les options disponibles pour les configurations du stockage.

Lors de la configuration du stockage, les options suivantes sont disponibles :

- Détail du stockage
- Configuration RAID

Détail du stockage

Pour utiliser la fonction de détail du stockage, utilisez les informations de cette rubrique.

Cette fonction affiche la structure physique et la configuration de stockage des dispositifs de stockage, ainsi que des détails, tels que leur emplacement, le nom du fabricant, le nom du produit, l'état, la capacité, l'interface, le support, le format et d'autres informations.

Un avertissement ou un événement critique est déclenché lorsque la valeur de la durée de vie restante du disque SSD atteint le seuil ou est inférieure. La valeur de durée restante par défaut pour l'avertissement et l'événement critique est respectivement de 8 % et 4 %. Cliquez sur l'icône d'engrenage à côté de **Détail du stockage** afin de définir la valeur du seuil.

Pour configurer des fonds de panier SAS/SATA/NVMe (AnyBay) qui prennent en charge le mode **Voie PCIe x1**, cliquez sur l'icône d'engrenage à côté de **Fond de panier**, puis sélectionnez le groupe de baies d'unité et cliquez sur le bouton **Appliquer** pour enregistrer la configuration.

Configuration RAID

Pour exécuter des fonctions de configuration RAID, utilisez les informations de cette rubrique.

Les informations de cette rubrique vous permettent d'afficher et de configurer des pools de stockage, des disques virtuels associés et des unités pour l'adaptateur RAID. Si le système est hors tension, mettez-le sous tension afin d'afficher les informations RAID.

Affichage et configuration des unités virtuelles

Les informations de cette rubrique vous permettent d'afficher et de configurer les unités virtuelles.

Lorsque vous sélectionnez **Configuration RAID** sous **Configuration du serveur**, l'onglet **Configuration de grappe** est choisi et les disques virtuels existants sont affichés par défaut. Les unités logiques sont triées par grappes de disques et par contrôleurs. L'onglet affiche également des informations détaillées sur le disque virtuel, par exemple sur le démarrage et la taille de bande du disque virtuel.

Pour configurer les paramètres RAID, cliquez sur **Activer le mode édition**.

Dans passer en mode, vous pouvez cliquer sur le menu Action du contrôleur, afficher les disques virtuels RAID en cours et créer de nouveaux disques virtuels RAID.

Le menu Actions du contrôleur vous permet d'effectuer les actions suivantes :

Effacer la configuration RAID

Efface toute la configuration et les données sur le contrôleur sélectionné.

Importer des disques étrangers
Importez toutes les unités externes qui ont été détectées. Une unité externe est une unité qui a été déplacée d'une configuration RAID différente sur le contrôleur RAID en cours

Remarque : Vous serez informé si aucune unité externe n'est détectée.

Gérer la configuration externe
Importez toutes les unités externes qui ont été détectées. Une unité externe est une unité qui a été déplacée d'une configuration RAID différente sur le contrôleur RAID en cours

Remarque : Vous serez informé si aucune unité externe n'est détectée.

Les informations des disques virtuels RAID actuels d'un contrôleur spécifique sont affichées en tant que « cartes de disques virtuels ». Chaque carte affiche des informations telles que le nom, l'état, la capacité et les actions du disque virtuel. L'icône de crayon vous permet de modifier les informations, l'icône de corbeille vous permet de supprimer la « carte de disque virtuel ».

Remarque : La capacité et le niveau RAID ne sont pas modifiables.

Si vous cliquez sur le nom du disque virtuel, une fenêtre de ses propriétés s'affiche.

Créer un nouveau disque RAID virtuel

Pour créer un nouveau disque virtuel RAID, suivez les étapes indiquées ci-dessous :

Remarque : S'il ne reste aucune capacité de stockage, vous ne pouvez pas créer de nouveau disque virtuel.

1. **Sélectionnez les unités ou une grappe de disques qui dispose de capacité de stockage**
   a. En créant un disque virtuel dans une nouvelle grappe de disques, vous devez indiquer le niveau RAID.

      Remarque : Si vous n'avez pas suffisamment d'unités à sélectionner, et que vous cliquez sur **Suivant**, un message d'erreur apparaît dans la zone de niveau RAID.

   b. Pour certains niveaux RAID, la répartition des données sur plusieurs disques est requise. Une quantité minimale d'unités doivent également être présentes dans la répartition. Pour ces types de situations, précisez le numéro de portée dans le champ **Numéro de portée**, sélectionnez **Membre** ou **Unité de secours** dans le menu déroulant à côté des unités, puis cochez la case à côté des unités qui seront utilisées pour créer le disque virtuel.
   c. Pour créer des disques virtuels dans une grappe de disques existante, vous devez sélectionner une grappe de disques disposant de capacité.
2. **Créez un disque virtuel**
   a. Par défaut, la création d'un disque virtuel utilise toute la capacité de stockage. L'icône **Ajouter** est désactivée lorsque tout le stockage est utilisé. Vous pouvez cliquer sur l'icône de crayon pour modifier la capacité ou d'autres propriétés.
   b. Lorsque vous modifiez le premier disque virtuel pour utiliser uniquement une partie de la capacité de stockage, l'icône **Ajouter** est activée. Cliquez sur l'icône pour afficher la fenêtre **Ajouter un disque virtuel**.
   c. Cliquez sur l'icône **Retirer** pour retirer un disque virtuel. Cette icône n'est pas affichée s'il n'existe qu'un seul disque virtuel. Lorsque vous cliquez sur l'icône **Supprimer**, la ligne sélectionnée est immédiatement supprimée. Aucune fenêtre de confirmation ne s'affichera puisque le disque virtuel n'a pas encore été créé.
   d. Cliquez sur **Commencer à créer** pour démarrer le processus.

Remarque : Lorsque le contrôleur n'est pas pris en charge, un message apparaît.

Affichage et configuration de l'inventaire de stockage

Les informations de cette rubrique vous permettent d'afficher et de configurer l'inventaire de stockage.

Sous l'onglet **Inventaire de stockage**, vous pouvez afficher et configurer les grappes de disques, les unités virtuelles associées et les unités pour le contrôleur RAID.

- **Pour les unités de stockage qui prennent en charge la configuration RAID** :
  1. Si le contrôleur inclut les grappes de disques configurées, il affiche les unités installées d'après la grappe de disques. Ci-après les éléments qui apparaissent dans la fenêtre.
     - **Titre du tableau** : Afficher l'ID de la grappe de disques, le niveau RAID et le nombre total d'unités.
     - **Contenu du tableau** : Répertorier les propriétés de base telles que le nom de l'unité, l'état de l'unité, le type, le produit, le fabricant, le numéro de série et les actions. Vous pouvez aller à la page **Inventaire** pour afficher toutes les propriétés que le XClarity Controller peut détecter.
     - **Actions** : Ci-après les actions pouvant être réalisées. Certaines mesures ne sont pas disponibles lorsque l'unité est dans un autre état.
       - **Affecter une unité de secours** : Signaler l'unité comme unité de secours globale ou dédiée.
       - **Retirer une unité de secours** : Supprimer l'unité de cette fonction.
       - **Marquer l'unité de disque comme hors ligne** : Définir l'unité à l'état hors ligne.
       - **Marquer l'unité de disque comme en ligne** : Définir l'unité à l'état en ligne.
       - **Démarrer la reconstruction** : Reconstruire le RAID.
       - **Rendre l'unité de disque réutilisable** : Définir l'unité comme réutilisable.
       - **Rendre l'unité de disque manquante** : Définir l'unité comme manquante.
       - **Rendre l'unité correcte pour JBOD** : Ajouter l'unité dans l'agencement de disque JBOD.
       - **Rendre l'unité non configurée correcte** : Rendre l'unité configurable en grappe ou utilisable comme unité de secours.
       - **Rendre l'unité non configurée incorrecte** : Rendre l'unité comme défectueuse, l'empêchant d'être utilisée en grappe ou comme unité de secours.
       - **Rendre l'unité de disque en préparation pour le retrait** : Définir l'unité en vue de son retrait.
  2. Si le contrôleur comporte des unités qui n'ont pas encore été configurées, elles seront affichées dans le tableau **Unités de disque non RAID**. En cliquant sur l'option **Convertir JBOD en Prêt pour configuration**, une fenêtre apparaîtra, affichant toutes les unités qui prennent en charge cette action. Vous pouvez sélectionner une ou plusieurs unités à convertir.

Pour les unités de stockage qui ne prennent pas en charge la configuration RAID : XClarity Controller peut ne pas pouvoir détecter les propriétés de certaines unités.

Chapitre 8. Mise à jour du microprogramme de serveur

Les informations de cette rubrique vous permettent de mettre à jour le microprogramme de serveur.

Présentation de la mise à jour du microprogramme

Informations générales sur la mise à jour du microprogramme de serveur.

En cliquant sur **Mise à jour du microprogramme** dans le panneau de navigation de gauche, une vue d'ensemble des informations sur le microprogramme s'affiche.

- **Mise à jour depuis le référentiel :** Synchronisation du microprogramme de serveur avec le référentiel CIFS/NFS distant en vue de la mise à jour par lot, voir « Mise à jour à partir du référentiel » à la page 86.
- **Microprogramme du système :** Aperçu de l'état du microprogramme du système, de la version et de la mise à jour du microprogramme du système.

  Remarque : Cliquez sur **Synchronisation automatique** pour activer ou désactiver la **promotion automatique du BMC principal vers la sauvegarde**. Lorsque ce paramètre est activé, le microprogramme du banc de sauvegarde en attente est synchronisé à partir du banc principal une fois que le banc principal a réussi la mesure ISM (Image Stability Metric).
- **Microprogramme de l'adaptateur :** Aperçu des microprogrammes d'adaptateur installés, de leur état, leur version et de la mise à jour du microprogramme des adaptateurs.
- **Microprogramme du bloc d'alimentation :** Aperçu de la version du microprogramme du bloc d'alimentation et de la mise à jour du microprogramme du bloc d'alimentation.
- **Microprogramme PSoc du fond de panier d'unité :** Aperçu de la version du microprogramme du fond de panier. Et pour effectuer la mise à jour du microprogramme du système.

Le statut et les versions en cours des microprogrammes du module BMC, UEFI, LXPM, des pilotes LXPM, du système d'exploitation intégré et de FPGA sont affichés, y compris la version principale et la version de secours du module BMC. Il existe trois catégories de statut de microprogramme :

- **Actif :** Le microprogramme est actif.
- **Inactif :** Le microprogramme est inactif.
- **En attente de redémarrage :** L'image du microprogramme a été mise à jour et prendra effet après le redémarrage du serveur du BMC.
- **S/O :** Aucun microprogramme n'a été installé pour ce composant.

Attention :

- XCC et IMM doivent être mis à jour vers la dernière version avant la mise à jour de UEFI. La mise à jour dans un autre ordre peut entraîner un comportement incorrect.
- L'installation d'une mise à jour de microprogramme erronée peut entraîner un dysfonctionnement du serveur. Avant d'installer une mise à jour de microprogramme ou de pilote de périphérique, lisez le fichier Readme et les fichiers d'historique des changements qui sont fournis avec la mise à jour téléchargée. Ces fichiers contiennent des informations importantes sur la mise à jour et les procédures d'installation associées, notamment une procédure spéciale relative à la mise à jour d'une ancienne version de microprogramme ou de pilote de périphérique vers la version la plus récente. Étant donné que le navigateur Web peut contenir des données du cache XCC, il est recommandé de recharger la page Web après la mise à jour du microprogramme XCC.
- À l'exception de l'adaptateur SATA M.2, les serveurs de processeur AMD ne prennent pas en charge la mise à jour hors bande du microprogramme de l'adaptateur.

- Certaines mises à jour du microprogramme requièrent le redémarrage du système, ce qui exécute l'activation du microprogramme ou sa mise à jour interne. Ce processus dans l'amorçage du système est appelé « mode de maintenance du système » ; il n'autorise temporairement pas les actions d'alimentation par l'utilisateur. Le mode est également activé lors de la mise à jour du microprogramme. L'utilisateur ne doit pas déconnecter l'alimentation en courant alternatif lorsque le système entre en mode de maintenance.

Mise à jour du microprogramme du système, de l'adaptateur et du bloc d'alimentation

Étapes de mise à jour du microprogramme du système, du microprogramme de l'adaptateur et du microprogramme du bloc d'alimentation.

Pour appliquer manuellement une mise à jour du **microprogramme du système**, du **microprogramme de l'adaptateur** et du **microprogramme du bloc d'alimentation**, procédez comme suit :

1. Cliquez sur **Mise à jour du microprogramme** pour chaque caractéristique. La fenêtre de mise à jour du microprogramme de serveur s'affiche.
2. Cliquez sur **Parcourir...** pour sélectionner le fichier de mise à jour du microprogramme à utiliser.
3. Naviguez vers le fichier que vous souhaitez sélectionner et cliquez sur **Ouvrir**. Vous retournez à la fenêtre de mise à jour du microprogramme de serveur avec le fichier sélectionné affiché.
4. Cliquez sur **Suivant** pour commencer le téléchargement et vérifier le processus pour le fichier sélectionné. Une barre de progression s'affiche pendant toute la durée du téléchargement et de la vérification du fichier. Vous pouvez afficher cette fenêtre d'état pour vérifier que le fichier que vous avez sélectionné pour la mise à jour est bien le fichier correct. Pour le **microprogramme du système**, la fenêtre d'état contiendra des informations sur le type de fichier de microprogramme devant être mis à jour, tel que BMC, UEFI ou LXPM. Une fois le fichier de microprogramme téléchargé et vérifié, cliquez sur **Suivant** pour sélectionner l'unité que vous souhaitez mettre à jour.
5. Pour lancer la mise à jour du microprogramme, cliquez sur **Mettre à jour**. Une barre de progression affiche la progression de la mise à jour. Une fois la mise à jour du microprogramme terminée, cliquez sur **Terminer**. Si la mise à jour nécessite le redémarrage de XClarity Controller, un message d'avertissement s'affiche. Pour plus d'informations sur le redémarrage de XClarity Controller, voir « Actions d'alimentation » à la page 63.

Mise à jour à partir du référentiel

Mise à jour du microprogramme de serveur à partir d'un référentiel distant

Présentation

Remarque : La fonctionnalité d'historique du microprogramme CIFS/NFS/HTTPS/intégré nécessite une licence XCC Premier.

XCC a présenté la mise à jour du microprogramme sur un serveur à l'aide d'un module de lots de mises à jour (Service Packs). Cette fonctionnalité permet de simplifier le processus à l'aide d'un outil client API ou Redfish unique afin de mettre à jour l'ensemble du microprogramme du système, y compris les modules de microprogramme OOB et IB. Le processus implique l'identification des modules de microprogramme qui peuvent être appliqués, le téléchargement et l'extraction de ces derniers à partir d'un serveur HTTP/HTTPS distant, leur chargement vers le stockage interne BMC par le biais d'un navigateur Web, ou bien leur montage à partir d'un répertoire partagé CIFS ou NFS.

Si vous utilisez le montage CIFS ou NFS, les fichiers de métadonnées (format JSON) doivent être placés dans le répertoire racine du système de fichiers partagés du réseau, avec les charges utiles de

microprogramme spécifiées dans les métadonnées. L'appareil microSD du serveur permet de stocker les référentiels historiques, ce qui permet aux utilisateurs de restaurer certains niveaux du microprogramme.

Si les modules de microprogramme contiennent des fichiers de charge utile qui ne prennent pas en charge la mise à jour du microprogramme hors bande, alors le BMC démarre le serveur et le configure à partir de l'image SE intégrée et installée dans BMC avant d'effectuer la mise à jour.

Lot de mises à jour et métadonnées

Le lot de mises à jour (Services Packs) est un fichier compressé composé d'un lot de microprogrammes. Il contient un ou plusieurs modules de microprogrammes destinés aux composants d'un système. La mise à jour de XCC depuis la fonctionnalité Référentiel utilise le fichier de lot de mises à jour. Le fichier de lot non zippé contient des métadonnées et des fichiers binaires de charge utile. Les fichiers de métadonnées JSON fournissent des informations à XCC au sujet du type d'images de microprogramme que le fichier de lot contient. Les fichiers binaires de charge utile, quant à eux, fournissent ces images de microprogramme.

Référentiel du microprogramme à l'intérieur de XCC

Le lot de mises à jour peut contenir plusieurs modules de microprogramme et XCC réserve 2 Go d'espace de sa mémoire flash pour de nouvelles fonctionnalités. Lorsqu'un nouveau lot est reçu, XCC efface les anciennes données. Certaines plateformes utilisent une carte MicroSD afin d'offrir un espace de stockage supplémentaire. XCC déplace alors le dernier lot de mises à jour vers le référentiel historique de la carte SD. Le référentiel d'historique du microprogramme peut stocker jusqu'à trois lots. Les utilisateurs peuvent utiliser la fonctionnalité de restauration du microprogramme afin de revenir à un précédent lot.

Remarques :

- Si le lot de mises à jour inclut uniquement le module de microprogramme OOB disponible pour le système, XCC ne modifie pas l'état d'alimentation du système. Pour mettre à jour le microprogramme de l'appareil PCI, le système doit être mis sous tension.
- Si le lot de mises à jour inclut le module de microprogramme IB disponible pour le système, XCC stocke l'état d'alimentation du système avant de mettre à jour et de restaurer l'état d'alimentation une fois la mise à jour du lot de mises à jour effectuée. Lors du processus de mise à jour, XCC réamorce l'hôte dans le SE intégré.
- Si le lot de mises à jour inclut un niveau prérequis pour le microprogramme UEFI, et si la version UEFI actuellement installée ne satisfait pas à ce niveau, XCC met le système hors tension afin de tout d'abord effectuer une mise à jour du microprogramme UEFI.
- Si le lot de mises à jour comprend un niveau prérequis pour le microprogramme XCC, et si la version XCC actuellement installée ne satisfait pas à ce niveau, XCC redémarre une fois sa mise à jour effectuée.

Mise à jour avec l'interface graphique Web

Avec **Mettre à jour depuis le référentiel**, l'utilisateur peut configurer XCC afin de synchroniser le microprogramme du serveur avec un stockage interne. Le référentiel du microprogramme doit contenir des modules qui comprennent des fichiers binaires et de métadonnées, ou des JSON de métadonnées de lots mises à jour ainsi que les fichiers binaires correspondants. XCC analyse les fichiers JSON de métadonnées afin de récupérer des modules de microprogramme qui prennent en charge la mise à jour OOB destinée au matériel système concerné, puis lance une mise à jour par lot.

Pour effectuer une mise à jour à partir du référentiel, procédez comme suit :

1. Lorsque vous utilisez le stockage interne, cliquez sur **Importer le module de microprogramme** et parcourez le module de microprogramme (format .tgz ou zip).
2. Cliquez sur **Mettre à jour le système** pour démarrer la mise à jour par lot.
3. Cliquez sur **Afficher les détails** pour afficher l'état de la mise à jour.
   - **Coche verte** : La mise à jour du microprogramme s'est terminée avec succès.

- **X rouge**  **:** La mise à jour du microprogramme a échoué.
- **Mise à jour :** La mise à jour du microprogramme est en cours.
- **Annuler :** La mise à jour du microprogramme est annulée.
- **En attente :** La mise à niveau du microprogramme est en attente de déploiement.

Remarque : Cliquez sur **Arrêter la mise à jour** pour annuler les mises à jour placées en file d'attente, et ce, dès la fin de la mise à jour du module d'installation en cours.

4. Lorsque vous utilisez CIFS ou NFS, cliquez sur **Démonter** pour vous déconnecter du référentiel distant.
5. Si la mise à jour nécessite le redémarrage de XClarity Controller, un message d'avertissement s'affiche. Pour plus d'informations sur le redémarrage de XClarity Controller, voir « Actions d'alimentation » à la page 63.

Remarque : Si le système est doté d'une carte MicroSD, vous pouvez consulter l'historique des mises à jour du lot de mises à jour, puis sélectionner l'indice du lot de mises à jour afin de restaurer un microprogramme antérieur. Le processus est similaire à la mise à jour à partir du référentiel ; la seule différence étant que le lot de mises à jour historique est placé dans la carte MicroSD.

Chapitre 9. Gestion des licences

La gestion des licences de Lenovo XClarity Controller vous permet d'installer et de gérer les fonctions en option de gestion du serveur et des systèmes.

Plusieurs niveaux de fonctions et fonctionnalités de XClarity Controller sont disponibles sur votre serveur. Le niveau de fonctions du microprogramme installé sur votre serveur varie en fonction du type de matériel.

Vous pouvez mettre à niveau la fonctionnalité XClarity Controller en achetant et en installant une clé d'activation.

Pour commander une clé d'activation, contactez votre représentant ou partenaire commercial.

Utilisez l'interface Web de XClarity Controller ou l'interface de ligne de commande XClarity Controller pour installer manuellement une clé d'activation vous permettant d'utiliser la fonction facultative achetée. Avant d'activer une clé :

- La clé d'activation doit être sur le système que vous utilisez pour vous connecter à XClarity Controller.
- Vous devez avoir commandé la clé de licence et reçu son code d’autorisation par courrier ou e-mail.

Pour obtenir des informations sur la gestion d’une clé d’activation à l’aide de l’interface Web de XClarity Controller, voir « Installation d'une clé d'activation » à la page 89, « Retrait d'une clé d'activation » à la page 89 ou « Exportation d'une clé d'activation » à la page 90. Pour obtenir des informations sur la gestion d’une clé d’activation à l’aide de l’interface de ligne de commande XClarity Controller, voir « Commande keycfg » à la page 119.

Pour enregistrer un identifiant dans l’administration de votre licence XClarity Controller, cliquez sur le lien suivant : https://fod.lenovo.com/lkms/angular/app/pages/index.htm#/welcome

Les informations sur la gestion des licences pour les serveurs Lenovo sont disponibles sur le site Web suivant de **Lenovo Press** :

https://lenovopress.com/redp4895-using-lenovo-features-on-demand

Installation d'une clé d'activation

Les informations de cette rubrique vous permettent d'ajouter une fonction en option à votre serveur.

Pour installer une clé d'activation, procédez comme suit :

Etape 1. Cliquez sur **Licence** sous **Configuration BMC**.

Etape 2. Cliquez sur **Mettre à niveau la licence**.

Etape 3. Dans la fenêtre **Ajouter une licence**, cliquez sur **Parcourir**, puis sélectionnez le fichier de clé d’activation à ajouter dans la fenêtre Téléchargement de fichier, puis cliquez sur **Ouvrir** pour ajouter le fichier. Pour terminer l’ajout de la clé, cliquez sur **Importer** dans la fenêtre Ajouter une clé d’activation.

Remarque : Si la clé d'activation n'est pas valide, une fenêtre d'erreur s'affiche.

Retrait d'une clé d'activation

Les informations de cette rubrique vous permettent de supprimer une fonction facultative de votre serveur.

Pour supprimer une clé d'activation, procédez comme suit :

Etape 1. Cliquez sur **Licence** sous **Configuration BMC**.

Etape 2. Sélectionnez la clé d'activation à supprimer, puis cliquez sur **Supprimer**.

Etape 3. Dans la fenêtre Confirmer la suppression de la clé d’activation, cliquez sur **OK** pour confirmer la suppression de la clé d’activation. La clé d’activation sélectionnée sera supprimée du serveur et n’apparaîtra plus à la page Gestion des licences.

Exportation d'une clé d'activation

Les informations de cette rubrique vous permettent d'exporter une fonction facultative de votre serveur.

Pour exporter une clé d'activation, procédez comme suit :

Etape 1. Cliquez sur **Licence** sous **Configuration BMC**.

Etape 2. A partir de la page Gestion des licences, sélectionnez la clé d'activation à exporter, puis cliquez sur **Exporter**.

Etape 3. Dans la fenêtre **Exporter la licence sélectionnée**, cliquez sur **Exporter** pour confirmer la demande d’exportation de la clé d’activation.

Etape 4. Sélectionnez le répertoire de sauvegarde du fichier. La clé d’activation sélectionnée sera exportée depuis le serveur.

Chapitre 10. Interface de ligne de commande

Les informations de cette rubrique vous permettent de sélectionner les commandes qui gèrent et surveillent XClarity Controller sans avoir à utiliser l'interface Web de XClarity Controller.

Vous pouvez utiliser l'interface de ligne de commande (CLI) XClarity Controller pour accéder au module XClarity Controller sans avoir à utiliser l'interface Web. Cette interface fournit un sous-ensemble des fonctions de gestion disponibles dans l'interface Web.

Vous pouvez accéder à l'interface CLI via une **session SSH**. Vous **devez** être authentifié par XClarity Controller avant de pouvoir lancer des commandes CLI.

Accès à l'interface de ligne de commande

Les informations de cette rubrique vous permettent d'accéder à l'interface de ligne de commande.

Pour accéder à l'interface de ligne de commande, ouvrez une session SSH à l'adresse IP XClarity Controller (voir « Configuration de la redirection série à SSH » à la page 91 pour plus d'informations).

Connexion à la session de ligne de commande

Les informations de cette rubrique vous permettent de vous connecter à la session de ligne de commande.

Pour vous connecter à l'interface de ligne de commande, procédez comme suit :

Etape 1. Établissez une connexion avec XClarity Controller.

Etape 2. À l'invite du nom d'utilisateur, entrez l'ID utilisateur.

Etape 3. À l'invite de mot de passe, entrez le mot de passe que vous utilisez pour vous connecter à XClarity Controller.

> **Remarque :** L'invite de ligne de commande est `system>`. La session de ligne de commande se poursuit jusqu'à ce que vous saisissiez `exit` depuis la ligne de commande. Vous êtes déconnecté (e) et la session prend fin.

Configuration de la redirection série à SSH

Cette rubrique fournit des informations sur l'utilisation de XClarity Controller comme un serveur de terminal série.

La redirection série à SSH permet à un administrateur système d'utiliser XClarity Controller comme un serveur de terminal série. Un port série serveur peut être joint depuis une connexion SSH lorsque la redirection série est activée.

Remarque : La commande d'interface de ligne de commande **console 1** permet de lancer une session de redirection série avec le port COM.

Exemple de session

```
$ ssh USERID@10.240.1.12
Password:

system>
```

Tout le trafic en provenance de la session SSH est acheminé à COM2.

```
ESC (
```

Entrez la séquence de touches de sortie pour revenir à l'interface de ligne de commande. Dans cet exemple, appuyez sur la touche Esc, puis entrez une parenthèse gauche. L'invite CLI s'affiche pour indiquer le retour à l'interface de ligne de commande IMM CLI.

```
system>
```

Syntaxe de commande

Les instructions de cette rubrique vous permettent de comprendre comment entrer des commandes dans l'interface de ligne de commande (CLI).

Consultez les instructions suivantes avant d'utiliser les commandes :

- Le format de toutes les commandes est le suivant :
  `command [`**`arguments`**`] [-`**`options`**`]`
- La syntaxe de commande est sensible à la casse.
- Le nom de la commande doit figurer en minuscules.
- Tous les arguments doit suivre immédiatement la commande. Les options suivent immédiatement les arguments.
- Chaque option est toujours précédée par un tiret (-). Une option peut figurer au format court (lettre unique) ou long (plusieurs lettres).
- Si une option comporte un argument, l'argument est obligatoire, par exemple :
  `ifconfig eth0 -i 192.168.70.34 -g 192.168.70.29 -s 255.255.255.0`
  Où **ifconfig** est la commande, **eth0** est un argument, et -i, -g, -s sont des options. Dans cet exemple, les trois options ont des arguments.
- Des crochets indiquent que l'argument ou l'option est facultatif. Les crochets ne font pas partie de la commande que vous saisissez.

Fonctionnalités et limitations

Cette rubrique contient des informations sur les fonctions et les limitations de l'interface de ligne de commande.

L'interface CLI se caractérise par les fonctionnalités et limitations suivantes :

- Plusieurs sessions CLI simultanées sont autorisées via SSH.
- Une seule commande est autorisée par ligne (limitée à 1024 caractères, y compris les espaces).
- Aucun caractère de continuation n'est disponible pour les commandes longues. La seule fonction d'édition est la touche Retour arrière qui efface le caractère que vous venez de saisir.
- Les touches de direction Flèche vers le haut et Flèche vers le bas peuvent être utilisées pour parcourir les huit dernières commandes. La commande **history** affiche la liste des huit dernières commandes, que vous pouvez ensuite utiliser comme raccourci pour exécuter une commande, comme dans l'exemple suivant :

```
system > history
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
```

```
system > !0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n XClarity ControllerA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system >
```

- Dans l'interface de ligne de commande, la mémoire tampon de sortie est limitée à 2 Ko. Aucune mise en mémoire tampon n'a lieu. La sortie d'une commande ne peut pas dépasser 2048 caractères. Cette limite ne s'applique pas en mode de redirection série (les données sont mises en mémoire tampon lors de la redirection série).
- Des messages texte simples sont utilisés pour indiquer le statut d'exécution de la commande, comme dans l'exemple suivant :
  ```
  system> power on
  ok
  system> power state
  Power: On
  State: System power off/State unknown
  system>
  ```
- La syntaxe de commande est sensible à la casse.
- Au moins un espace doit figurer entre une option et son argument. Par exemple, la syntaxe `ifconfig eth0 -i192.168.70.133` est incorrecte. La syntaxe correcte est `ifconfig eth0 -i 192.168.70.133`.
- Toutes les commandes admettent les options `-h`, `-help` et `?`, lesquelles fournissent une aide concernant la syntaxe. Tous les exemples suivants débouchent sur le même résultat :
  ```
  system> power -h
  system> power -help
  system> power ?
  ```
- Certaines des commandes décrites dans les sections ci-dessous peuvent ne pas être disponibles dans la configuration de votre système. Pour afficher la liste des commandes prises en charge par votre configuration, utilisez l'option `help` ou l'option `?`, comme illustré dans les exemples ci-dessous :
  ```
  system> help
  system> ?
  ```

Liste des commandes par ordre alphabétique

Cette rubrique contient une liste des commandes CLI dans l'ordre alphabétique. Des liens sont fournis vers les rubriques de chaque commande. Chaque rubrique de commande fournit des informations sur la commande, sa fonction, sa syntaxe et son utilisation.

Vous trouverez ci-dessous la liste complète de toutes les commandes CLI de XClarity Controller, par ordre alphabétique :

Commandes d'utilitaire

Cette rubrique fournit une liste alphabétique des commandes CLI d'utilitaire.

Il existe actuellement 3 commandes d'utilitaire :

Commande exit

Utilisez cette commande pour vous déconnecter de la session CLI,

Utilisez la commande **exit** pour vous déconnecter et mettre fin à la session d'interface CLI.

Commande help

Cette commande affiche une liste de toutes les commandes.

Utilisez la commande **help** pour afficher la liste et une brève description de chacune des commandes. Vous pouvez également entrer ? depuis l'invite de commande.

Commande history

Cette commande permet d'afficher la liste des commandes précédemment émises.

Utilisez la commande **history** pour afficher une liste historique indexée des huit dernières commandes émises. Les index peuvent ensuite être utilisés en tant que raccourcis (précédés de !) pour émettre de nouveau des commandes de la liste historique.

Exemple :

```
system> history
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
HISTORY-g 0.0.0.0
-s 255.255.255.0
-n XCCA00096B9E003A
-r auto
-d auto
```

```
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system>
```

Commandes de surveillance

Cette rubrique fournit une liste alphabétique des commandes CLI de surveillance.

Il existe actuellement 11 commandes de surveillance :

Commande clearlog

Cette commande permet d'effacer le journal des événements du module IMM.

Utilisez la commande **clearlog** pour effacer le journal des événements du module IMM. Vous devez être habilité à effacer les journaux d'événements pour émettre cette commande.

Remarque : L'utilisation de cette commande est réservée au personnel de support technique.

Syntaxe :
```
clearlog [-options]
```

Tableau 4. Options clearlog

Option	Description	Valeurs
-t	Type d'événement ; choisissez le type d'événement à effacer. Si rien n'est spécifié, tous les types d'événement sont sélectionnés.	all, platform, audit • all : Tout type d'événement, y compris les événements de plate-forme et les événements d'audit. • platform : Type d'événement de plateforme. • audit : Type d'événement d'audit.

Exemple :
```
system> clearlog
All event log cleared successfully
system>
system> clearlog -t all
All event log cleared successfully
system>
system> clearlog -t platform
Platform event log cleared successfully
system>
system> clearlog -t audit
Audit event log cleared successfully
system>
```

Commande fans

Cette commande permet d'afficher la vitesse des ventilateurs du serveur.

Utilisez la commande **fans** pour afficher la vitesse de chacun des ventilateurs du serveur.

Exemple :
```
system> fans
```

```
fan1 75%
fan2 80%
fan3 90%
system>
```

Commande mhlog

Utilisez cette commande pour afficher les entrées du journal d'activité de l'historique de maintenance.

Syntaxe :
```
mhlog [-options]
```

Tableau 5. Options mhlog

Option	Description	Valeurs
-c	Afficher le nombre d'entrées	Entre 1 et 250
-i	Afficher les entrées à partir de l'index	Entre 1 et 250
-f	Nom de fichier distant du fichier journal	Nom de fichier valide pour le nom de fichier du fichier journal
-ip	Adresse du serveur tftp/sftp	Adresse IP valide du serveur TFTP/SFTP
-pn	Numéro de port du serveur tftp/sftp	Numéro de port valide du serveur TFTP/SFTP (69/22 par défaut)
-u	Nom d'utilisateur du serveur sftp	Nom d'utilisateur valide du serveur SFTP
-pw	Mot de passe du serveur sftp	Mot de passe valide du serveur SFTP

Exemple :
```
system> mhlog
Type             Message                                                    Time
-------------    ------------                                               ----
Hardware         SAS Backplane1(SN: XXXX9CE009L) is added.                 05/08/2020,04:23:18
Hardware         CPU 1(SKU NO: 50844440) is added.                          05/08/2020,04:23:22
Hardware         CPU 2(SKU NO: 50844440) is added.                          05/08/2020,04:23:22
Hardware         M2 Card(SN: R1SH9AJ0037) is added.                        05/08/2020,04:23:22
Firmware         Primary XCC firmware is updated to TGBT99T by XCC Web.    05/08/2020,06:40:37
Firmware         Primary XCC firmware is activated to TGBT99T.             05/08/2020,06:41:26
Hardware         PSU1(SN: D1DG94C0075) is added.                            05/08/2020,06:43:28
system>
```

Commande led

Utilisez cette commande pour afficher et définir les états de voyants.

La commande **led** affiche et définit les états des voyants du serveur.

- L'exécution de la commande **led** sans option affiche l'état des voyants du panneau frontal.
- L'option de commande **led -d** doit être utilisée avec l'option de commande **led -identify on**.

Le tableau suivant présente les arguments pour les options.

Syntaxe :
```
led [-options]
```

Tableau 6. Options led

Option	Description	Valeurs
-l	Obtenir l'état de tous les voyants du système et de ses sous-composants	
-identify	Changer l'état du voyant d'identification du boîtier	off, on, blink
-d	Activer le voyant d'identification pour la période spécifiée	Période (secondes)

Exemple :

```
system> led
Fault                 Off
Identify              On            Blue
Chklog                Off
Power                 Off

system> led -l
Label                 Location                  State         Color
Battery               Planar                    Off
BMC Heartbeat         Planar                    Blink         Green
BRD                   Lightpath Card            Off
Channel A             Planar                    Off
Channel B             Planar                    Off
Channel C             Planar                    Off
Channel D             Planar                    Off
Channel E             Planar                    Off
Chklog                Front Panel               Off
CNFG                  Lightpath Card            Off
CPU                   Lightpath Card            Off
CPU 1                 Planar                    Off
CPU 2                 Planar                    Off
DASD                  Lightpath Card            Off
DIMM                  Lightpath Card            Off
DIMM 1                Planar                    Off
DIMM 10               Planar                    Off
DIMM 11               Planar                    Off
DIMM 12               Planar                    Off
DIMM 13               Planar                    Off
DIMM 14               Planar                    Off
DIMM 15               Planar                    Off
DIMM 16               Planar                    Off
DIMM 2                Planar                    Off
DIMM 3                Planar                    Off
DIMM 4                Planar                    Off
DIMM 5                Planar                    Off
DIMM 6                Planar                    Off
DIMM 7                Planar                    Off
DIMM 8                Planar                    Off
DIMM 9                Planar                    Off
FAN                   Lightpath Card            Off
FAN 1                 Planar                    Off
FAN 2                 Planar                    Off
FAN 3                 Planar                    Off
Fault                 Front Panel (+)           Off
Identify              Front Panel (+)           On            Blue
LINK                  Lightpath Card            Off
LOG                   Lightpath Card            Off
```

```
NMI                  Lightpath Card            Off
OVER SPEC            Lightpath Card            Off
PCI 1                FRU                        Off
PCI 2                FRU                        Off
PCI 3                FRU                        Off
PCI 4                FRU                        Off
Planar               Planar                    Off
Power                Front Panel (+)           Off
PS                   Lightpath Card            Off
RAID                 Lightpath Card            Off
Riser 1              Planar                    Off
Riser 2              Planar                    Off
SAS ERR              FRU                        Off
SAS MISSING          Planar                    Off
SP                   Lightpath Card            Off
TEMP                 Lightpath Card            Off
VRM                  Lightpath Card            Off
system>
```

Commande readlog

Cette commande permet d'afficher les journaux des événements IMM.

Utilisez la commande **readlog** pour afficher les entrées du journal des événements IMM. Cinq journaux des événements à la fois sont affichés. Les entrées sont affichées à partir de la plus récente jusqu'à la plus ancienne.

Remarques :

- R - non valide
- I - info
- W - avertissement
- E - critique

Syntaxe :
```
readlog [-options]
```

Tableau 7. Options readlog

Option	Description	Valeurs
-a	Afficher toutes les entrées du journal des événements, en commençant par la plus récente.	
-f	Réinitialiser le compteur et afficher les 5 premières entrées du journal des événements, en commençant par la plus récente.	
-date	Afficher les entrées du journal des événements pour la date spécifiée	Utilisez le format suivant : mm/jj/aaaa
-sev	Afficher les entrées du journal des événements pour le niveau de gravité spécifié.	R, I, W, E

Tableau 7. Options readlog (suite)

Option	Description	Valeurs
-i	Définir l'adresse IP IPv4 ou IPv6 du serveur TFTP ou SFTP sur lequel le journal des événements est enregistré. Les options de commande **-i** et **-l** sont utilisées conjointement pour indiquer l'emplacement.	Adresse IP valide
-l	Définir le nom du fichier journal des événements. Les options de commande **-i** et **-l** sont utilisées conjointement pour indiquer l'emplacement.	Nom de fichier valide
-pn	Afficher ou définir le numéro de port du serveur TFTP ou SFTP.	Numéro de port valide (par défaut 69/22)
-u	Spécifier le nom d'utilisateur du serveur SFTP.	Nom d'utilisateur valide
-pw	Spécifier le mot de passe du serveur SFTP.	Mot de passe valide
-di	Capacité étendue de journal d'audit	none, ipmi

Exemple :
```
system> readlog -f
1 I 2017-06-17T09:31:59.217  Remote Login Successful. Login ID: USERID
from SSH at IP address 10.134.78.180
2 I 2017-06-17T07:23:04.685  Remote Login Successful. Login ID: USERID
from webguis at IP address 10.134.78.180.
3 I 2017-06-16T11:00:35.581  Login ID: USERID from webguis at IP address 10.134.78.180 has logged off.
4 I 2017-06-16T11:00:15.174  Login ID: USERID from webguis at IP address 10.104.209.144 has logged off.
5  I 2017-06-16T10:40:14.352  Login ID: USERID from webguis at IP address 10.104.209.144 has logged off.
system> readlog
6 E SERVPROC 12/18/03 10:09:31 Fan 2 Fault. Multiple fan failures
7 E SERVPROC 12/18/03 10:09:31 Fan 1 Fault. Single fan failure
8 I SERVPROC 12/18/03 10:09:25 Ethernet[0] Link Established at 100Mb, Full Duplex.
9 I SERVPROC 12/18/03 10:09:24 Ethernet[0] configured to do Auto Speed/Auto Duplex.
10 I SERVPROC 12/18/03 10:09:24 Ethernet[0] MAC Address currently
being used: 0x00-09-6B-CA-0C-80
system>
```

commande servicelog

Cette commande permet de générer un nouveau fichier de données de maintenance.

Remarque : Cette commande était auparavant **ffdc**.

Utilisez la commande **servicelog** pour générer et transférer des données de maintenance vers le support.

La liste suivante montre les commandes pouvant être utilisées avec la commande **servicelog** :

Le tableau suivant présente les arguments pour les options.

Syntaxe :
```
servicelog [subset_command] [-options]
```

Tableau 8. commandes servicelog subset

Option	Description
générer	Créer un nouveau fichier de données de maintenance
status	Vérifier l'état du fichier de données de maintenance
copier	Copier les données de maintenance existantes
supprimer	Supprimer les données de maintenance existantes

Tableau 9. Options servicelog

Option	Description	Valeurs
-t	Type de journal de maintenance	1, 2, 3 • **1** : Journal de débogage (FFDC, par défaut) • **2** : Journal de données de maintenance • **3** : Journal de données de maintenance associées au journal de débogage, qui n'est valide que lors de la copie des fichiers de journaux
Options supplémentaires pour la commande generate		
-c	Videz la sélection de la catégorie de données. La catégorie de données ne sera pas contenue si elle n'est pas spécifiée avec cette option.	• Pour le type 1 (ffdc) : corefile • Pour le type 2 (journal des données de maintenance) : audit, telemetry, osscreen
Options supplémentaires pour les commandes generate et copy		
-f	Répertoire cible sftp ou nom de fichier distant.	Pour sftp, utilisez le chemin d'accès complet ou le signe / de fin sur le nom de répertoire (~/ ou /tmp/). La valeur par défaut est le nom généré par le système.
-ip	Adresse du serveur tftp/sftp.	Adresse IP valide
-pn	Numéro de port du serveur tftp/sftp.	Numéro de port valide (par défaut 69/22)
-u	Nom d'utilisateur du serveur sftp.	Nom d'utilisateur valide
-pw	Mot de passe du serveur sftp.	Mot de passe valide
-timeout	Minutes pour permettre la copie en premier plan.	Entre 1 et 5 (1 par défaut)

Exemple :

```
system> servicelog generate
Generating ffdc...
system> servicelog status
Type 1 ffdc: in progress
system> servicelog copy -t 1 -ip 192.168.70.230 -u User2 -pw Passw0rd -f /tmp/
Waiting for ffdc.....
Copying ffdc...
ok
system> servicelog status
Type 1 ffdc: completed
```

```
8737AC1_DSY0123_xcc_120317-153327.tgz


system> servicelog generate
Generating ffdc...
system> servicelog status
Type 1 ffdc: in progress
system> servicelog status
Type 1 ffdc: in progress
system> servicelog copy -ip 192.168.70.230
Copying ffdc...
ok
system> servicelog status
Type 1 ffdc: completed
8737AC1_DSY0123_xcc_120926-105320.tgz
system>
```

Commande syshealth

Cette commande fournit un récapitulatif de l'état d'intégrité ou des événements actifs.

Utilisez la commande **syshealth** pour afficher un récapitulatif de l'état d'intégrité ou des événements actifs du serveur. L'état d'alimentation, l'état du système, l'état du matériel (dont le ventilateur, le bloc d'alimentation, le stockage, le processeur, la mémoire), le nombre de redémarrages, et l'état du logiciel IMM sont affichés.

Syntaxe :
```
syshealth [arguments]
```

Tableau 10. Arguments syshealth

Arguments	Description
summary	Afficher le récapitulatif de l'état du système.
activeevents	Afficher les événements actifs.
cooling	Afficher l'état d'intégrité des périphériques de refroidissement.
power	Afficher l'état d'intégrité des modules d'alimentation.
storage	Afficher l'état d'intégrité du stockage local.
processors	Afficher l'état d'intégrité des processeurs.
memory	Afficher l'état d'intégrité de la mémoire.

Exemple :
```
system> syshealth summary
Power    On
State    OS booted
Restarts 29

system> syshealth activeevents
No Active Event Available!
```

Commande temps

Cette commande permet d'afficher toutes les informations relative aux températures et aux seuils de température.

Utilisez la commande **temps** pour afficher toutes les températures et les seuils de température. Le groupe de températures affiché est le même que dans l'interface Web.

Syntaxe :
```
temps
```

Exemple :
```
system> temps
Temperatures are displayed in degrees Fahrenheit/Celsius
               WR           W      T             SS             HS
-----------------------------------------------------------------------
Ambient Temp  109.40/43    N/A    78.80/26.00  109.40/43.00  122.00/50.00
Exhaust Temp  N/A           N/A    32.00/0 .00  116.60/47.00  N/A
system>
```

Remarques :

1. La sortie comporte les en-têtes de colonnes suivants :

   WR : avertissement réinitialisation (Positif- allant la valeur d'hystérésis de seuil)

   W : avertissement (Seuil non critique supérieur)

   T: temperature (Current value)

   SS: soft shutdown (Upper critical Threshold)

   HS : arrêt immédiat (Seuil supérieur non récupérable)
2. Toutes les valeurs de température sont affichées en degrés Fahrenheit et Celsius.
3. N/A indique que ce n'est pas applicable.

Commande volts

Utilisez cette commande pour afficher les informations relatives à la tension du serveur.

Utilisez la commande **volts** pour afficher toutes les tensions et leurs seuils. Le groupe de tensions affiché est le même que dans l'interface Web.

Syntaxe :
```
volts
```

Exemple :
```
system> volts
               HSL  SSL   WL    WRL   V     WRH   WH   SSH   HSH
-------------------------------------------------------------------
CMOS Battery  N/A  2.25  2.39  0.03  3.12  0.03  N/A  N/A   N/A
system>
```

Remarque : La sortie comporte les en-têtes de colonnes suivants :

HSL : arrêt immédiat faible (Seuil non récupérable inférieur)

SSL : arrêt graduel faible (Seuil critique inférieur)

WL : avertissement faible (Seuil non critique inférieur)

WRL : réinitialisation avertissement faible (Valeur Hysteresis de seuil à tendance négative)

V : voltage (valeur actuelle)

WRH : réinitialisation avertissement élevé (Valeur Hysteresis de seuil à tendance positive)

WH : avertissement élevé (Seuil supérieur non critique)

SSH : arrêt graduel élevé (Seuil supérieur critique)

HSH : arrêt immédiat élevé (Seuil non récupérable supérieur)

Commande vpd

Cette commande permet d'afficher la configuration et les données d'informations (données techniques essentielles) associées au matériel et aux logiciels du serveur.

Utilisez la commande **vpd** pour afficher les données techniques essentielles pour le système (sys), pour IMM (bmc), pour le système BIOS du serveur (uefi), pour le Lenovo XClarity Provisioning Manager (lxpm), pour le microprogramme serveur (fw) et pour les composants serveur (comp) et les périphériques PCIe (pcie). Les informations qui s'affichent sont les mêmes que dans l'interface Web.

Syntaxe :
```
vpd [arguments]
```

Tableau 11. Arguments vpd

Arguments	Description
vpd sys	Afficher les données produit essentielles pour le système.
vpd bmc	Afficher les données produit essentielles pour le contrôleur de gestion.
vpd uefi	Afficher les données produit essentielles pour le BIOS du système.
vpd lxpm	Afficher les données produit essentielles pour le LXPM du système.
vpd fw	Afficher les données produit essentielles pour le microprogramme du système.
vpd comp	Afficher les données produit essentielles pour les composants du système.
vpd pcie	Afficher les données produit essentielles pour les périphériques PCIe.

Exemple :
```
system> vpd bmc
Type             Status       Version    Build       ReleaseDate
-------------    -------      -------    ------      ------------
BMC (Primary)   Active      0.00       DVI399T    2017/06/06
BMC (Backup)    Inactive    1.00       TEI305J    2017/04/13
system>
```

Commande de contrôle de l'alimentation et du redémarrage du serveur

Cette rubrique fournit une liste alphabétique des commandes CLI d'alimentation et de redémarrage.

Il existe actuellement 4 commandes d'alimentation et de redémarrage du serveur :

Commande power

Cette commande décrit comment contrôler le serveur d'alimentation.

Utilisez la commande **power** pour contrôler l'alimentation du serveur. Pour lancer des commandes **power**, vous devez disposer du niveau de droit d'accès Remote Server Power/Restart Access (alimentation et redémarrage à distance du serveur).

Syntaxe :
```
power on [-options]
```

```
power off [-options]
power cycle [-options]
power uefi
power state
```

Tableau 12. commandes power

Commande	Description
power on	Utilisez cette commande pour mettre le serveur sous tension.
power off	Utilisez cette commande pour mettre le serveur hors tension.
power cycle	Utilisez cette commande pour mettre le serveur hors puis sous tension.
power uefi	Utilisez cette commande pour démarrer dans la configuration F1 de l'UEFI.
power state	Utilisez cette commande pour afficher l'état d'alimentation du système, ainsi que l'état en cours du serveur.

Tableau 13. Options power

Option	Description	Valeurs
-s	Utilisez cette option pour arrêter le système d'exploitation avant la mise hors tension du serveur. **Remarque :** L'option **-s** est impliquée lors de l'utilisation de l'option **-every** pour les commandes **power off** et **power cycle**.	
-every	Utilisez cette option avec les commandes **power on**, **power off** et **power cycle** pour contrôler l'alimentation serveur. Vous pouvez configurer les dates, les heures, ainsi que la fréquence (quotidienne ou hebdomadaire) de la mise sous tension, hors tension, ou du cycle d'alimentation de votre serveur.	Dim, Lun, Mar, Mer, Jeu, Ven, Sam, Jour, effacer
-t	Utilisez cette option pour spécifier la durée en heures et minutes de la mise sous tension du serveur, de l'arrêt du système d'exploitation, et de la mise hors tension ou du redémarrage du serveur.	Utilisez le format suivant : hh:mm
-d	Utilisez cette option pour spécifier la date de mise sous tension du serveur. Il s'agit d'une option supplémentaire pour la commande **power on**. **Remarque :** Les options **-d** et **-every** ne peuvent pas être utilisées ensemble dans la même commande.	Utilisez le format suivant : mm/jj/aaaa
-clear	Utilisez cette option pour effacer la date de mise sous tension planifiée. Il s'agit d'une option supplémentaire pour la commande **power on**.	

Les informations suivantes constituent des exemples de commande **power**.

Pour arrêter le système d'exploitation et mettre le serveur hors tension tous les dimanches à 1:30, entrez la commande suivante :

```
system> power off -every Sun -t 01:30
```

Pour arrêter le système d'exploitation et redémarrer le serveur hors tension tous les jours à 1:30, entrez la commande suivante :

```
system> power cycle -every Day -t 01:30
```

Pour mettre le serveur sous tension tous les lundis à 1:30, entrez la commande suivante :
```
system> power on -every Mon -t 1:30
```

Pour mettre le serveur sous tension le 31 décembre 2013 à 23:30, entrez la commande suivante :
```
system> power on -d 12/31/2013 -t 23:30
```

Pour effacer un cycle d'alimentation hebdomadaire, entrez la commande suivante :
```
system> power cycle -every clear
```

Commande reset

Cette commande décrit comment réinitialiser le serveur.

Utilisez la commande **reset** pour redémarrer le serveur. Pour utiliser cette commande, vous devez être habilité à contrôler l'alimentation et le redémarrage du serveur.

Syntaxe :
```
reset [-options]
```

Tableau 14. Options reset

Option	Description	Valeurs
-s	Arrêter le système d'exploitation avant la réinitialisation du serveur.	
-d	Retarder la réinitialisation durant un nombre de secondes défini.	0 - 120
-nmi	Générer une interruption non masquable (NMI) sur le serveur.	

Commande fuelg

Cette commande permet d'afficher des information sur l'alimentation du serveur.

Utilisez la commande **fuelg** pour afficher les informations sur l'utilisation de l'alimentation serveur et configurer la gestion de l'alimentation du serveur. Cette commande permet également de configurer des stratégies relatives à la perte de redondance de l'alimentation.

Syntaxe :
```
fuelg [-options]
```

Tableau 15. Options fuelg

Option	Description	Valeurs
-pme	Activer ou désactiver la gestion de l'alimentation et le plafonnement sur le serveur.	on, off
-pcapmode	Définir le mode de plafonnement énergétique pour le serveur.	output, input
-pcap	Valeur numérique incluse dans la plage des valeurs de plafonnement énergétique affichées lors de l'exécution de la commande fuelg, sans option, sur la cible.	valeur numérique en watt
-history	Afficher l'historique de la consommation d'énergie ou des performances.	pc, perf

Tableau 15. Options fuelg (suite)

Option	Description	Valeurs
-period	Valeur numérique pour afficher l'historique.	1, 6, 12, 24 heures
-pm	Définir le mode de stratégie pour la perte de l'alimentation de secours.	• **bt**- de base avec régulation • **rt**- redondant avec régulation (par défaut)
-zm	Activer ou désactiver le mode zéro sortie. Ce paramètre ne peut être défini que lorsque le mode de stratégie est défini sur Redondant avec régulation.	on, off
-perf	Afficher l'utilisation de l'ordinateur actuelle, y compris le système, le processeur, le module de mémoire et l'E-S.	
-pc	Afficher la consommation électrique actuelle	• **output**- Afficher la consommation d'énergie en sortie actuelle du système, du processeur, du module de mémoire et d'autres composants. • **input**- Afficher la consommation d'énergie actuelle, y compris la consommation d'énergie du système. **Remarque :** Pour les serveurs AMD, la consommation d'énergie en sortie actuelle n'affichera pas certains composants.

Commande pxeboot

Cette commande permet d'afficher et de définir la condition du PXE (Preboot eXecution Environment).

Syntaxe :
```
pxeboot [-options]
```

Tableau 16. Options pxeboot

Option	Description	Valeurs
-en	Définit la condition du Preboot eXecution Environment pour le prochain redémarrage du système.	enabled, disabled

Commandes de configuration

Cette rubrique fournit une liste alphabétique des commandes CLI de configuration.

Il existe actuellement 41 commandes de configuration :

Commande accseccfg

Utilisez cette commande pour afficher et configurer les paramètres de sécurité de compte.

Syntaxe :

```
accseccfg [-options]
```

Tableau 17. Options accseccfg

Option	Description	Valeurs
-am	Définit la méthode d'authentification utilisateurs.	local, ldap, localldap, ldaplocal
-lp	Période de verrouillage après le nombre maximum d'échecs de connexion (minutes).	Entre 0 et 2880, 0 = période de verrouillage n'a pas expiré
-pe	Délai d'expiration du mot de passe (jours).	Entre 0 et 365, 0 = n'expire jamais
-pew	Période d'avertissement d'expiration du mot de passe **Remarque :** La période d'avertissement d'expiration du mot de passe doit être inférieure à la période d'expiration du mot de passe.	Entre 0 et 30, 0 = aucun avertissement
-pc	Règles de complexité des mots de passe activées.	on, off
-pl	Longueur du mot de passe.	Si les règles de complexité des mots de passe sont activées, la longueur du mot de passe est comprise entre 8 et 32. Dans le cas contraire, elle est comprise entre 0 et 32.
-ci	Intervalle de modification du mot de passe minimum (heures).	entre 0 et 240, 0 = immédiatement modification
-lf	Nombre maximum d'échecs de connexion.	Entre 0 et 10, 0 = jamais verrouillé
-chgnew	Modifier le mot de passe du nouvel utilisateur après la première connexion.	on, off
-rc	Cycle de réutilisation du mot de passe.	Entre 0 et 10, 0 = réutilise immédiatement
-wt	Délai d'attente d'inactivité de session Web et Secure Shell (minutes).	Entre 0 et 1440

Exemple :

```
system> accseccfg
  -am: local
  -lp: 60
  -pe: none
  -pew: 0
  -pc: on
  -pl: 10
  -ci: 0
  -lf: 5
  -chgnew: on
  -rc: 5
  -wt: 20
system>
```

Commande asu

Cette commande permet de configurer les paramètres UEFI.

Les commandes ASU (Advanced Settings Utility) sont utilisées pour configurer les paramètres UEFI. Le système hôte doit être redémarré pour que les modifications des paramètres UEFI prennent effet.

Syntaxe :
```
asu [subset_command]
```

Tableau 18. commandes asu subset

Commande	Description	Valeur
help	Utilisez cette commande pour afficher des informations d'aide pour un ou plusieurs paramètres.	**setting_name**
set	Utilisez cette commande pour modifier la valeur d'un paramètre. Définissez le paramètre UEFI à la valeur d'entrée. **Remarques :** • Définissez une ou plusieurs paires paramètre/valeur. • Le paramètre peut contenir des caractères génériques s'il se développe en un seul paramètre. • La valeur doit être placée entre guillemets si elle contient des espaces. • Les valeurs de liste triées sont séparées par le symbole égal (=). Par exemple, définissez B*.Bootorder « CD/DVD Rom=Hard Disk 0=PXE Network. »	**setting_name=value**
show	Utilisez cette commande pour afficher la valeur actuelle d'un ou plusieurs paramètres.	**setting_name**
showvalues	Utilisez cette commande pour afficher toutes les valeurs possibles d'un ou plusieurs paramètres. **Remarques :** • Cette commande affiche des informations sur les valeurs admises pour le paramètre. • Le minimum et le maximum d'instances autorisé pour le paramètre s'affiche. • La valeur par défaut s'affiche, si disponible. • La valeur par défaut est entourée des signes inférieur et supérieur (< et >). • Les valeurs textuelles affichent la longueur minimale et maximale et l'expression régulière.	**setting_name**
showgroups	Utilisez cette commande pour afficher les groupes de paramètres disponibles. Cette commande affiche les noms des groupes connus. Les noms de groupes peuvent varier en fonction des périphériques installés.	
Remarques : • Dans la syntaxe de commande, **setting_name** est le nom d'un paramètre que vous souhaitez afficher ou modifier, et **value** est la valeur que vous placez sur le paramètre. • **setting_name** peut contenir plus d'un nom, sauf lorsque vous utilisez la commande **set**. • **setting_name** peut contenir des caractères génériques, par exemple un astérisque (*) ou un point d'interrogation (?). • **setting_name** peut être un groupe, un nom de paramètre ou **all**.		

Exemples :

- Pour afficher toutes les options de commande asu, entrez `asu help`.
- Pour afficher l'aide d'une commande, entrez `asu help setting_name`.
- Pour modifier une valeur, entrez `asu set setting_name=value`.
- Pour afficher la valeur en cours, entrez `asu show setting_name`.
- Pour afficher toutes les valeurs possibles pour un paramètre, entrez `asu showvalues setting_name`.
  Exemple de commande show values :
  ```
  system> asu showvalues S*.POST*
  SystemRecovery.POSTWatchdogTimer==<Disable>=Enable
  SystemRecovery.POSTWatchdogTimerValue=numeric min=5 max=20 step=1 default=5
  system>
  ```
- Pour afficher les groupes de paramètres disponibles, entrez `asu showgroups`.

Le tableau suivant présente les arguments pour les options.

Tableau 19. Options asu

Le tableau suivant, à plusieurs lignes et trois colonnes, comporte les options, les descriptions d'option, ainsi que les valeurs associées pour les options.

Option	Description	Valeurs
-b	Afficher au format par lots.	
-help[1]	Afficher l'utilisation de la commande et de ses options. L'option -help est placée avant la commande, par exemple **asu -help show**.	
-l	Nom de paramètre au format long (inclure le jeu de configuration).	
-m	Nom de paramètre au format mixte (utiliser l'ID de configuration).	
-v[2]	Sortie détaillée.	

1. L'option -help peut être utilisée avec n'importe quelle commande.
2. L'option -v est uniquement utilisée entre **asu** et la commande.

Syntaxe :
```
asu [-options] command [cmdopts]
options:
   -v verbose output
   -help display main help
cmdopts:
   -help help for the command
```

Remarque : Pour plus d'options de commandes, voir les commandes individuelles.

Utilisez les commandes de transaction asu pour définir plusieurs paramètres UEFI et créer et exécuter les commandes en mode de traitement par lots. Utilisez les commandes **tropen** et **trset** pour créer un fichier de transaction contenant plusieurs paramètres à appliquer. Une transaction avec un ID donné est ouverte à l'aide de la commande **tropen**. Les paramètres sont ajoutés au jeu à l'aide de la commande **trset**. La transaction terminée est validée à l'aide de la commande **trcommit**. Une fois la transaction terminée, vous pouvez la supprimer à l'aide de la commande **trrm**.

Remarque : L'opération de restauration des paramètres UEFI créera une transaction avec un ID utilisant un numéro aléatoire à trois chiffres.

Le tableau suivant contient les commandes de transaction pouvant être utilisées avec la commande **asu**.

Tableau 20. Commandes de transaction asu

Le tableau suivant, à plusieurs lignes et trois colonnes, comporte les commandes de transaction, les descriptions de commande, ainsi que les valeurs associées pour les commandes.

Commande	Description	Valeur
tropen **id**	Cette commande crée un nouveau fichier de transaction contenant plusieurs paramètres à définir.	**Id** est la chaîne identifiante, 1 à 3 caractères alphanumériques.
trset **id**	Cette commande ajoute un ou plusieurs paramètres ou paires de valeurs à une transaction.	**Id** est la chaîne identifiante, 1 à 3 caractères alphanumériques.
trlist **id**	Cette commande affiche d'abord le contenu du fichier de transaction. Cela peut être utile lorsque le fichier de transaction est créé dans l'interpréteur de ligne de commande.	**Id** est la chaîne identifiante, 1 à 3 caractères alphanumériques.
trcommit **id**	Cette commande valide et exécute le contenu du fichier de transaction. Les résultats de l'exécution et les erreurs seront affichés.	**Id** est la chaîne identifiante, 1 à 3 caractères alphanumériques.
trrm **id**	Cette commande supprime le fichier de transaction après avoir été validé.	**Id** est la chaîne identifiante, 1 à 3 caractères alphanumériques.

Exemple d'établissement de plusieurs paramètres UEFI :

```
asu tropen TR1
asu trset TR1 UEFI.BootModes.SystemBootMode "UEFI and Legacy"
asu trset TR1 BootOrder.BootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 BootOrder.WolBootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 UEFI.DevicesandIOPorts.Com1BaudRate 115200
asu trset TR1 UEFI.DevicesandIOPorts.Com1DataBits 8
asu trset TR1 UEFI.DevicesandIOPorts.Com1FlowControl Disable
asu trset TR1 UEFI.DevicesandIOPorts.Com1Parity None
asu trset TR1 UEFI.DevicesandIOPorts.Com1StopBits 1
asu trset TR1 UEFI.DevicesandIOPorts.COMPort1 Enable
asu trcommit TR1
```

Commande backup

Utilisez cette commande pour créer un fichier de sauvegarde contenant les paramètres de sécurité actuels du système.

Syntaxe :

```
backup [-options]
```

Tableau 21. Options backup

Option	Description	Valeurs
-f	Nom du fichier de sauvegarde	Nom de fichier valide
-pp	Mot de passe ou phrase valide, délimitée par des apostrophes pour chiffrer les mots de passe dans le fichier de sauvegarde	Mot de passe ou phrase passe valide, délimitée par des apostrophes

Tableau 21. Options backup (suite)

Option	Description	Valeurs
-ip	Adresse IP du serveur TFTP/SFTP	Adresse IP valide
-pn	Numéro de port du serveur TFTP/SFTP	Numéro de port valide (par défaut 69/22)
-u	Nom d'utilisateur du serveur SFTP	Nom d'utilisateur valide
-pw	Mot de passe du serveur SFTP	Mot de passe valide
-fd	Nom de fichier pour la description XML des commandes CLI de sauvegarde	Nom de fichier valide

Exemple :
```
system> backup -f xcc-back.cli -pp xxxxxx -ip 192.168.70.200
ok
system>
```

Commande dhcpinfo

Utilisez cette commande pour afficher la configuration IP affectée au serveur DHCP pour eth0.

Utilisez la commande **dhcpinfo** pour afficher la configuration IP affectée par le serveur DHCP pour eth0 si l'interface est configurée automatiquement par un serveur DHCP. Vous pouvez utiliser la commande **ifconfig** pour activer ou désactiver DHCP.

Syntaxe :
```
dhcpinfo [ethernet_number]
```

Exemple :
```
dhcpinfo eth1
```

Le tableau suivant décrit la sortie de cet exemple.

Tableau 22. sortie dhcpinfo

Zone	Description
-server	Serveur DHCP ayant affecté la configuration
-n	Nom d'hôte affecté
-i	Adresse IPv4 affectée
-i6	Adresse IPv6 affectée
-g	Adresse de passerelle affectée
-s	Masque de sous-réseau affecté
-d	Nom de domaine IPv4 affecté
-d6	Nom de domaine IPv6 affecté
-dns1	Adresse IP du serveur DNS IPv4 principal
-dns2	Adresse IP du serveur DNS IPv4 secondaire
-dns3	Adresse IP du serveur DNS IPv4 tertiaire
-i6	Adresse IPv6
-d6	Nom de domaine IPv6

Tableau 22. sortie dhcpinfo (suite)

Zone	Description
-dns61	Adresse IP du serveur DNS IPv6 principal
-dns62	Adresse IP du serveur DNS IPv6 secondaire
-dns63	Adresse IP du serveur DNS IPv6 tertiaire

Commande dns

Utilisez cette commande pour afficher et définir la configuration DNS du module IMM.

Syntaxe :

```
dns [-options]
```

Tableau 23. Options dns

Option	Description	Valeurs
-state	État DNS	on, off
-i1	Adresse IP du serveur DNS IPv4 principal	Adresse IP au format d'adresse IP à notation décimale à point.
-i2	Adresse IP du serveur DNS IPv4 secondaire	Adresse IP au format d'adresse IP à notation décimale à point.
-i3	Adresse IP du serveur DNS IPv4 tertiaire	Adresse IP au format d'adresse IP à notation décimale à point.
-i61	Adresse IP du serveur DNS IPv6 principal	Adresse IP au format IPv6.
-i62	Adresse IP du serveur DNS IPv6 secondaire	Adresse IP au format IPv6.
-i63	Adresse IP du serveur DNS IPv6 tertiaire	Adresse IP au format IPv6.
-ddns	État DDNS	enabled, disabled
-dnsrc	Nom de domaine DDNS préféré	dhcp, manuel
-ddn	DDN spécifié manuellement	
-ddncur	DDN en cours (lecture seule)	
-p	Serveurs DNS préférés (ipv4, ipv6)	ipv4, ipv6
-dscvry	Reconnaissance des adresses LXCA	enabled, disabled
-dsclist	Liste LXCA des SRV DNS	
-dscxm	Configuration de XClarity Manager	

L'exemple suivant présente une configuration du module IMM dans laquelle DNS est désactivé :

```
system> dns
   -state   :  disabled
   -i1      :  0.0.0.0
   -i2      :  0.0.0.0
   -i3      :  0.0.0.0
   -i61     :  ::
   -i62     :  ::
   -i63     :  ::
   -ddns    :  enabled
   -dnsrc   :  DHCP
   -ddn     :
```

```
   -ddncur  :  labs.lenovo.com
   -p       :  ipv6
   -dscvry  :  enabled
system>
```

Commande encaps

Utilisez cette commande pour que le contrôleur BMC quitte le mode d'encapsulation.

Syntaxe :
```
encaps [arguments]
```

Tableau 24. Arguments encaps

Arguments	Description
lite off	Permet à BMC de quitter le mode d'encapsulation et d'ouvrir l'accès global ouvert à tous les utilisateurs

Commande ethtousb

Utilisez la commande **ethtousb** pour afficher et configurer le mappage de port Ethernet vers Ethernet-via-USB.

La commande vous permet de mapper un numéro de port Ethernet externe à un numéro de port différent Ethernet-via-USB.

Syntaxe :
```
ethtousb [-options]
```

Tableau 25. Commande ethtousb

Option	Description	Valeurs
-en	État de l'interface Ethernet sur USB.	enabled, disabled **Remarque :** Activez l'interface Ethernet sur USB via **<usbeth>** pour rendre le mappage des ports efficace.
-m**[x] port1:port2**	Configurer le mappage de port pour l'index **x**.	Où : • Le numéro d'index de port, **x**, est spécifié en tant que nombre entier compris entre 1 et 10 dans l'option de commande. • **port1** de la paire de ports correspond au numéro de port Ethernet externe. • **port2** de la paire de ports correspond au numéro de port Ethernet-via-USB.
-rm **map_ index**	Supprimer le mappage de port pour l'index indiqué.	Le numéro d'index du port, **map_index**, est spécifié sous la forme d'un entier compris entre 1 et 10 dans l'option de commande. **Remarque :** Les index de mappage de port sont affichés à l'aide de la commande **ethtousb** sans option.

Exemple :
```
system> ethtousb -en enabled -m1 100:200 -m2 101:201
system> ethtousb
        ethtousb : On
        ===============
         1:   100:  200
         2:   101:  201
system>
```

Commande firewall

Cette commande permet de configurer le pare-feu afin de limiter l'accès à partir de certaines adresses et de limiter éventuellement la durée d'accès. Si aucune option n'est spécifiée, les paramètres actuels s'affichent.

Syntaxe :
```
firewall [-options]
```

Tableau 26. Options firewall

Option	Description	Valeurs
L'option suivante concerne la liste blanche des adresses IP		
-wips	Afficher/configurer les adresses IP de la liste blanche.	<Adresses IP valides>, clr • **Valid IP addresses** : Autoriser 1 à 3 adresses IP (séparées par des virgules, CIDR ou plage) **Remarque :** Les adresses IPv4 et IPv6 peuvent utiliser le format CIDR pour bloquer une plage d'adresses. • **-clr** : Effacer la liste blanche
Les options suivantes concernent la liste de blocage et la restriction de temps		
-bips	Bloquer les adresses IP 1-3 (séparées à l'aide de virgules, CIDR ou plage)	Adresses IP valides **Remarque :** Les adresses IPv4 et IPv6 peuvent utiliser le format CIDR pour bloquer une plage d'adresses.
-bmacs	Bloquer 1 à 3 adresses MAC (séparées à l'aide de virgules)	Adresses MAC valides **Remarque :** Le filtrage d'adresses MAC fonctionne uniquement avec des adresses spécifiques.
-bbt	Heure de début du blocage, doit être postérieure à l'heure actuelle	Date et heure au format<YYYY-MM-DD HH:MM>
-bet	Heure de fin du blocage, doit être postérieure à l'heure de début	Date et heure au format<YYYY-MM-DD HH:MM>
-bti	Bloquer 1 à 3 intervalles de temps (séparés par des virgules) par exemple, **firewall - bti 01:00–02:00,05:05–10:30** bloquera l'accès de 01:00 à 02:00 et 05:05 à 10:30, tous les jours	Plage horaire au format <HH:MM-HH:MM>
-clr	Effacer la règle de pare-feu pour un type donné	ip, mac, datetime, interval, all
Les options suivantes concernent le blocage d'adresses IP		
-iplp	Période de verrouillage de l'adresse IP en minutes.	Valeur numérique comprise entre 0 et 2 880, 0 = n'expire jamais

Tableau 26. Options firewall (suite)

Option	Description	Valeurs
-iplf	Nombre maximum d'échecs de connexion avant le verrouillage de l'adresse IP.	Valeur numérique comprise entre 0 et 32, 0 = aucun verrouillage **Remarque :** Si cette valeur est différente de 0, elle doit être supérieure ou égale à la valeur **<Nombre maximum d'échecs de connexion>**, définie par **<accseccfg -lf>**
-ipbl	Afficher/configurer la liste des adresses IP verrouillées.	del, clrall, show • **-del** : supprimer une adresse IPv4 ou IPv6 de la liste de blocage • **-clrall** : effacer toutes les adresses IP de la liste de blocage • **-show** : afficher toutes les adresses IP de la liste de blocage

Liste d'exemples de syntaxe pour la commande **firewall** :

- Pour afficher la valeur de toutes les options et la liste de blocage des adresses IP, saisissez `firewall`.
- Pour bloquer l'accès de plusieurs adresses IP, saisissez `firewall -bips 192.168.1.1,192.168.1.0/24,192.168.1.1-192.168.1.5`.
- Pour bloquer tous les accès de 1 h à 2 h, 05 h 05 à 10 h 30, 14 h 15 à 20 h 00 tous les jours, saisissez `firewall -bti 01:00-02:00,05:05-10:30,14:15-20:00`.
- Pour effacer toutes les règles de la liste de blocage et des restrictions d'heure, saisissez `firewall –clr all`.
- Pour définir la période de verrouillage de l'adresse IP sur 60 minutes, saisissez `firewall -iplp 60`.
- Pour définir le nombre maximal d'échecs de connexion à 5 fois, saisissez `firewall -iplf 5`.
- Pour supprimer 192.168.100.1 de la liste de blocage des adresses IP, saisissez `firewall -ipbl -del 192.168.100.1`.
- Pour supprimer 3fcc:1234::2 de la liste de blocage des adresses IP, saisissez `firewall –ipbl -del 3fcc:1234::2`.
- Pour supprimer toutes les adresses IP bloquantes, saisissez `firewall –ipbl –clrall`.
- Pour afficher toutes les adresses IP bloquantes, saisissez `firewall –ipbl –show`.

Commande hashpw

Utilisez cette commande avec l'option -sw pour activer/désactiver la fonction de mot de passe tiers ou avec l'option -re pour activer/désactiver l'autorisation de récupération de mots de passe tiers.

Syntaxe :
```
hashpw [-options]
```

Tableau 27. Options hashpw

Option	Description	Valeurs
-sw	État de commutation de mot de passe tiers	enabled, disabled
-re	État de lecture de mot de passe tiers **Remarque :** La lecture peut être définie si la commutation est activée.	enabled, disabled

Exemple :

```
system> hashpw -sw enabled -re enabled
system> users -5 -n guest5 -shp ef92b778bafe771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f - r Administrator
system> users -5 ghp
ef92b778bafe771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f
system> users
Account      Login ID      Advanced Attribute            Role               Password Expires
-------      --------      ------------------            ------               ----------------
1            USERID        Native                         Administrator      Password doesn't expire
5            guest5        Third-party Password          Administrator      90 day(s)
```

Commande ifconfig

Utilisez cette commande pour configurer l'interface Ethernet.

Utilisez la commande **ifconfig** pour afficher la configuration actuelle de l'interface Ethernet. Pour modifier la configuration de l'interface Ethernet, entrez les options voulues, suivies par leurs valeurs. Pour modifier la configuration de l'interface, vous devez disposer au moins de l'autorisation Adapter Networking and Security Configuration.

Syntaxe :

```
ifconfig [ethernet_number] [-options]
```

Exemple :

```
dhcpinfo eth1 -b
```

Tableau 28. Options ifconfig

Option	Description	Valeurs
-state	État de l'interface	disabled, enabled
-c	Méthode de configuration	dhcp, static, dthens (dthens correspond à **essayer le serveur dhcp, en cas d'échec utiliser l'option static config** sur l'interface Web)
-ghn	Obtention du nom d'hôte auprès de DHCP	disabled, enabled
-i	Adresse IP statique	Adresse avec format valide.
-g	Adresse de passerelle	Adresse avec format valide.
-s	Masque de sous-réseau	Adresse avec format valide.
-n	Nom d'hôte	Chaîne pouvant comprendre jusqu'à 63 caractères. La chaîne peut inclure des lettres, des chiffres, des points, des traits de soulignement et des tirets.
-auto	Paramètre de négociation automatique qui détermine si les paramètres réseau Data rate et Duplex sont configurables	true, false
-vlan	Activation ou désactivation du marquage VLAN	enabled, disabled
-vlanid	ID VLAN	Valeur numérique comprise entre 1 et 4094.
-r	Vitesse de transfert	10, 100, 1000
-d	Mode duplex	intégral, semi

Tableau 28. Options ifconfig (suite)

Option	Description	Valeurs
-m	MTU	Valeur numérique comprise entre 60 et 1500.
-l	LAA	Format d'adresse MAC. Les adresses de multidiffusion ne sont pas autorisés (le premier octet doit être pair).
-b	Adresse MAC gravée (lecture seule)	
-dn	Nom de domaine (lecture seule)	
-ipv6	État IPv6	disabled, enabled
-ipv6static	État IPv6 statique	disabled, enabled
-i6	Adresse IP statique	Adresse IP statique pour canal Ethernet 0 au format IPv6.
-p6	Longueur de préfixe d'adresse	Valeur numérique comprise entre 1 et 128.
-g6	Passerelle ou route par défaut	Adresse IP pour la passerelle ou la route par défaut pour le canal Ethernet 0 dans IPv6.
-dhcp6	Mode DHCP IPv6	enabled, disabled
-sa6	Mode sans état IPv6	enabled, disabled
-lla	Adresse locale de liaison (lecture seule)	
-ncsi	Sélection du port NIC NCSI	nic[x]:port[y] **Remarque :** Utilisez la virgule comme délimiteur s'il existe deux paramètres ou plus.
-nic	Modification du mode de la carte d'interface réseau (NIC)[1]	shared, dedicated, shared:nic[x][2]
-failover[2]	Mode de basculement	none, shared, shared:nic[x]
-nssync[3]	Synchronisation des paramètres réseau	enabled, disabled

Tableau 28. Options ifconfig (suite)

Option	Description	Valeurs
-address_table	Tableau des adresses IPv6 générées automatiquement et de leurs longueurs de préfixe (lecture seule) **Remarque :** Cette option n'est visible que si IPv6 et la configuration automatique sans état sont activés.	

Remarques :

1. -nic indique également l'état de la carte d'interface réseau. [active] indique la carte d'interface réseau actuellement utilisée par XCC.

   Par exemple :
   ```
   -nic: shared:nic3
   nic1: dedicate
   nic2: ext card slot #3
   nic3: ext card slot 5 [active]
   ```
   Indique que nic3 est en mode partagé, dans l'emplacement 5, que nic2 est dans l'emplacement 3, que nic1 est un port dédié XCC et que XCC utilise nic3.
2. La valeur shared:nic[x] est disponible sur les serveurs ayant une carte réseau mezzanine installée en option. Cette carte réseau mezzanine peut être utilisée par le module IMM.
3. Si le module IMM est configuré pour utiliser le port du réseau de gestion dédié, l'option -failover demandera au module IMM de basculer sur le port réseau partagé en cas de déconnexion du port dédié.
4. Si le mode de basculement est activé, l'option -nssync demande au module IMM d'utiliser les mêmes paramètres réseau que ceux utilisés sur le port réseau de gestion dédié pour le port réseau partagé.

Exemple :
```
system> ifconfig eth0 -c static -i 192.168.70.133
These configuration changes will become active after the next reset of the IMM.
system>
```

Commande keycfg

Utilisez cette commande pour afficher, ajouter ou supprimer les clés d'activation.

Les clés d'activation contrôlent l'accès à la fonctionnalité IMM en option.

Remarques :

- Ajoutez de nouvelles clés d'activation par le biais de transfert de fichier.
- Supprimez d'anciennes clés en indiquant le numéro de la clé ou le type de clé. Lorsque les clés sont supprimées par type, seule la première clé d'un type défini est supprimée.

Syntaxe :
```
keycfg [-options]
```

Tableau 29. Options keycfg

Option	Description	Valeurs
-add	Ajouter une clé d'activation	ip, pn, u, pw, f • **-ip** : Adresse IP du serveur TFTP/SFTP avec clé d'activation à ajouter • **-pn** : Numéro de port pour le serveur TFTP/SFTP avec clé d'activation à ajouter (par défaut : 69/22) • **-u** : Nom d'utilisateur du serveur SFTP avec clé d'activation à ajouter • **-pw** : Mot de passe du serveur SFTP avec clé d'activation à ajouter • **-f** : Nom de fichier pour la clé d'activation à ajouter
-del	Supprimer une clé d'activation par numéro d'index	Numéro d'index de la clé d'activation valide de la liste **keycfg**
-deltype	Supprimer une clé d'activation par type de clé	Valeur de type de clé valide

Lorsque la commande **keycfg** est exécutée sans option, la liste des clés d'activation installées s'affiche. L'information sur les clés qui s'affiche inclut un numéro d'index pour chaque clé d'activation, le type de clé d'activation, la date à laquelle la clé a été validée, le nombre d'utilisations restantes, l'état de la clé et une description de la clé.

Exemple :
```
system> keycfg
ID  Type  Valid           Uses           Status    Description
1   4     10/10/2010      5              "valid"   "IMM remote presence"
2   3     10/20/2010      2              "valid"   "IMM feature
3   32796 NO CONSTRAINTS  NO CONSTRAINTS "valid"   "IBM Security Key Lifecycle Manager for SEDs FoD"
system>
```

Remarque : La zone **Description** pour le numéro d'ID 3 s'affiche sur des lignes distinctes en raison de restrictions d'espace.

Commande ldap

Utilisez cette commande pour afficher et configurer les paramètres de configuration du protocole LDAP.

Syntaxe :
```
ldap [-options]
```

Tableau 30. Options ldap

Option	Description	Valeurs
-aom	Mode d'authentification uniquement pour les utilisateurs Active Directory	enabled, disabled
-a	Méthode d'authentification utilisateur	• **loc** : local uniquement • **ldap** : LDAP uniquement • **locld** : local d'abord, puis LDAP • **ldloc** : LDAP d'abord, puis local
-b	Méthode de liaison	• **anon** : anonyme • **client** : liaison avec ClientDN et mot de passe • **login** : liaison avec les identifiants de connexion
-c	Nom distinctif du client	Chaîne pouvant comprendre jusqu'à 127 caractères pour **client_dn**
-d	Domaine de recherche	Chaîne pouvant comprendre jusqu'à 63 caractères pour **search_domain**
-fn	Nom de la forêt	Pour les environnements Active Directory. Chaîne pouvant comprendre jusqu'à 127 caractères.
-f	Filtre de groupe	Chaîne pouvant comprendre jusqu'à 127 caractères pour **group_filter**
-g	Attribut de recherche de groupe	Chaîne pouvant comprendre jusqu'à 63 caractères pour **group_search_attr**
-l	Attribut de permission de connexion	Chaîne pouvant comprendre jusqu'à 63 caractères pour **string**
-p	Mot de passe du client	Chaîne pouvant comprendre jusqu'à 15 caractères pour **client_pw**
-pc	Confirmation du mot de passe du client	Chaîne pouvant comprendre jusqu'à 15 caractères pour **confirm_pw** Syntaxe de la commande : ldap -p **client_pw** -pc **confirm_pw** Cette option est requise lorsque vous modifiez le mot de passe du client. Elle compare l'argument **confirm_pw** à l'argument **client_pw**. La commande échoue si les arguments ne concordent pas.
-r	Nom distinctif d'entrée racine (DN)	Chaîne pouvant comprendre jusqu'à 127 caractères pour **root_dn**
-s1ip	Nom d'hôte/adresse IP de Server 1	Chaîne pouvant comporter jusqu'à 127 caractères ou adresse IP pour **host name/ip_addr**
-s2ip	Nom d'hôte/adresse IP de Server 2	Chaîne pouvant comporter jusqu'à 127 caractères ou adresse IP pour **host name/ip_addr**
-s3ip	Nom d'hôte/adresse IP de Server 3	Chaîne pouvant comporter jusqu'à 127 caractères ou adresse IP pour **host name/ip_addr**
-s4ip	Nom d'hôte/adresse IP de Server 4	Chaîne pouvant comporter jusqu'à 127 caractères ou adresse IP pour **host name/ip_addr**
-s1pn	Numéro de port de Server 1	Numéro de port pouvant comporter jusqu'à 5 chiffres pour **port_number**

Tableau 30. Options ldap (suite)

Option	Description	Valeurs
-s2pn	Numéro de port de Server 2	Numéro de port pouvant comporter jusqu'à 5 chiffres pour **port_number**
-s3pn	Numéro de port de Server 3	Numéro de port pouvant comporter jusqu'à 5 chiffres pour **port_number**
-s4pn	Numéro de port de Server 4	Numéro de port pouvant comporter jusqu'à 5 chiffres pour **port_number**
-u	Attribut de recherche du nom de connexion de l'utilisateur	Chaîne pouvant comprendre jusqu'à 63 caractères pour **search_attrib**
-v	Obtention de l'adresse du serveur LDAP via DNS	off, on
-h	Affichage de la syntaxe et des options de la commande	

Exemple :
```
system> ldap
   -aom enable
   -a   locld
   -b   client
   -c   cn=admin,dc=lenovo,dc=com
   -d
   -fn
   -f   example.com
   -g   cn
   -l   XCC3RBSPermissions
   -r
   -s1ip 10.241.99.94
   -s2ip
   -s3ip
   -s4ip
   -s1pn 389
   -s2pn 389
   -s3pn 389
   -s4pn 389
   -u uid
   -v off
system>
```

Commande ntp

Utilisez cette commande pour afficher et configurer le protocole NTP (Network Time Protocol).

Syntaxe :
```
ntp [-options]
```

Tableau 31. Commande ntp

Option	Description	Valeurs
-en	Active ou désactive le protocole NTP (Network Time Protocol).	enabled, disabled
-i**[x]**	Nom ou adresse IP du serveur Network Time Protocol pour l'index **-x**.	Nom du serveur NTP à utiliser pour la synchronisation d'horloge. L'intervalle des numéros d'index du serveur NTP est de -i1 à -i4. **Remarque :** -i correspond à i1.
-f	La fréquence (en minutes) à laquelle l'horloge IMM est synchronisée avec le serveur Network Time Protocol.	3 à 1440 minutes
-synch	Demande une synchronisation immédiate avec le serveur Network Time Protocol.	Aucune valeur n'est spécifiée avec ce paramètre.

Exemple :
```
system> ntp
-en: disabled
-f: 3 minutes
-i: not set
```

Commande portcontrol

Utilisez cette commande pour activer ou désactiver un port de service réseau.

Syntaxe :
```
portcontrol [-options]
```

Tableau 32. Options portcontrol

Option	Description	Valeurs
-ipmi	Activer ou désactiver l'accès IPMI via LAN	on, off
-ipmi-kcs	Activer à la demande, activer ou désactiver l'accès ipmi à partir du serveur	auto, on, off
-rest	Activer ou désactiver la reconnaissance REST	on, off
-snmp	Activer ou désactiver la reconnaissance SNMP	on, off
-ssdp	Activer ou désactiver la reconnaissance SSDP	on, off
-cli	Activer ou désactiver la reconnaissance CLI	on, off
-web	Activer ou désactiver la reconnaissance WEB	on, off
-all	Activer ou désactiver toutes les interfaces et tous les protocoles de reconnaissance.	on, off

Exemple :

```
system> portcontrol
ipmi : on
ipmi-kcs : on
rest : on
snmp : off
ssdp : on
cli : on
web : on
system>
```

Commande ports

Utilisez cette commande pour afficher et configurer les ports IMM.

Syntaxe :

```
ports [-options]
```

Tableau 33. Options ports

Option	Description	Valeurs
-open	Afficher les ports ouverts (lecture seule)	
-reset	Réinitialiser les ports aux paramètres par défaut (lecture uniquement)	
-http	Numéro de port HTTP	Numéro de port par défaut : 80
-https	Numéro de port HTTPS	Numéro de port par défaut : 443
-ssh	Numéro de port CLI existant SSH	Numéro de port par défaut : 22
-snmpa	Numéro de port de l'agent SNMP	Numéro de port par défaut : 161
-snmpt	Numéro de port d'alertes SNMP	Numéro de port par défaut : 162
-rp	Numéro de port de Présence à distance	Numéro de port par défaut : 3900

Exemple :

```
system> ports
  -http 80
  -https 443
  -rp 3900
  -snmpa 161
  -snmpt 162
  -ssh 22
system>
```

Commande rdmount

Utilisez cette commande pour monter des images disque ou des partages réseau à distance

Remarques :

- Jusqu'à deux fichiers peuvent être téléchargés dans la mémoire de XClarity Controller et être montés en tant que support virtuel à l'aide de la fonctionnalité RDOC de XClarity Controller. La taille totale des deux fichiers ne doit pas dépasser 50 Mo. Les images téléchargés en mode lecture uniquement, sauf si l’option –rw est utilisée.

- Lors de l'utilisation des protocoles HTTP, FTP ou SFTP pour monter ou mapper les images, la taille totale pour toutes les images ne doit pas dépasser 50 Mo. Il n'est pas de taille limite si les protocoles NFS ou SAMBA sont utilisés.

Syntaxe :
```
rdmount [-options]
```

Tableau 34. Options rdmount

Option	Description
-r	Opération rdoc (si utilisée, doit être la première option) -r -mappage : monter les images RDOC -r -unmap <filename> : démonter les images RDOC montées -r -maplist : présente les images montées RDOC via le navigateur Web XClarity Controller et l'interface CLI
-map	-t <samba|nfs|http|sftp|ftp> type de système de fichiers -ro read-only -rw read-write -u user -p password -l file location (format URL) -o option (chaîne d'option supplémentaire pour les montages samba et nfs) -d domain (domaine pour montage samba)
-maplist	Afficher les images mappés
-unmap	<id|fname> utiliser l'id avec des images de réseau, nom de fichier rdoc
-mount	Monter les images mappées
-unmount	Démonter les images montées

Commande restore

Utilisez cette commande pour restaurer les paramètres systèmes à partir d'un fichier de sauvegarde.

Syntaxe :
```
restore [-options]
```

Tableau 35. Options restore

Option	Description	Valeurs
-f	Nom du fichier de sauvegarde	Nom de fichier valide
-pp	Mot de passe ou phrase passe utilisé (e) pour chiffrer les mots de passe dans le fichier de sauvegarde	Mot de passe ou phrase passe valide, délimitée par des apostrophes
-ip	Adresse IP du serveur TFTP/SFTP	Adresse IP valide

Tableau 35. Options restore (suite)

Option	Description	Valeurs
-pn	Numéro de port du serveur TFTP/ SFTP	Numéro de port valide (par défaut 69/22)
-u	Nom d'utilisateur du serveur SFTP	Nom d'utilisateur valide
-pw	Mot de passe du serveur SFTP	Mot de passe valide

Exemple :
```
system> restore f xcc-back.cli pp xxxxxx ip 192.168.70.200
ok
system>
```

Commande roles

Utilisez cette commande pour afficher ou configurer les rôles.

Syntaxe :
```
roles role_account[3-31] [-options]
```

Tableau 36. Options roles

Option	Description	Valeurs
-n	Nom du rôle	Limite de 32 caractères
-p	Définir des privilèges	custom:am, rca, rcvma, pr, cel, bc, nsc, ac, us • **am** : Accès à la gestion de compte utilisateur • **rca** : Accès à distance à la console • **rcvma** : Accès à la console distante et au disque distant (support virtuel) • **pr** accès à distance au démarrage/ redémarrage du serveur • **cel** : Possibilité d'effacer les journaux d'événements • **bc** : Configuration de l'adaptateur (de base) • **nsc** : Configuration de l'adaptateur (réseau et activité) • **ac** : Configuration de l'adaptateur (avancée) • **us** : Sécurité UEFI **Remarque :** Les indicateurs d'autorisation personnalisés ci-dessus peuvent être utilisés dans n'importe quelle combinaison
-d	Supprimer une ligne	

Exemple :
```
system> roles -3 -n test1 -p custom:am|rca|rcvma
ok


system> roles
```

```
Account              Role                              Privilege                    Assigned To
------- ----------------------------------   -------------------------     -------------------------------
    0                    Administrator                    all                          USERID
    1                         ReadOnly                      none
    2                         Operator              custom:pr|cel|bc|nsc
    3                            test1               custom:am|rca|rcvma
```

Commande rtd

Utilisez cette commande pour restaurer tous les paramètres BMC aux paramètres d'usine par défaut.

Remarque : Cette commande était auparavant **restoredefaults** et **clearcfg**.

Syntaxe :
```
rtd [-options]
```

Tableau 37. Options rtd

Option	Description
-all	Réinitialiser tous les paramètres BMC aux paramètres d'usine par défaut.
-eu	Réinitialiser tous les paramètres BMC aux paramètres d'usine, sauf les paramètres utilisateur
-en	Réinitialiser tous les paramètres BMC aux paramètres d'usine, sauf les paramètres réseau.
-eun	Réinitialiser tous les paramètres BMC aux paramètres d'usine, sauf les paramètres utilisateur et réseau.

Exemple :
```
system> rtd -all

This action will cause all IMM settings to be set to factory defaults.

If this is the local system, you will lose your TCP/IP connection as a result.
You will need to reconfigure the IMM network interface to restore connectivity.
After the IMM configuration is cleared, the IMM will be restarted.

Proceed? (y/n)
Y
Restoring defaults
```

Commande seccfg

Utilisez cette commande pour effectuer une annulation de microprogramme.

Syntaxe :
```
seccfg [-options]
```

Tableau 38. Options seccfg

Option	Description	Valeur
-fwrb	Permettre l'annulation du microprogramme et un retour à une version antérieure.	enabled, disabled
-aubp	Activer ou désactiver la fonction de promotion du principal à la sauvegarde automatique.	enabled, disabled

Commande securityinfo

Cette commande permet d'afficher les informations relatives à la sécurité.

Syntaxe :
```
securityinfo [-options]
```

Tableau 39. Options securityinfo

Option	Description
-event	Afficher les événements de sécurité.
-cryptomode	Afficher l'état du mode crypto de sécurité.
-service	Afficher l'état de sécurité des services et des ports.
-cert	Afficher l'état de sécurité du certificat.
-account	Afficher l'état de sécurité des comptes utilisateur.

Commande securitymode

Cette commande permet de générer un nouveau fichier de données de maintenance.

Syntaxe :
```
securitymode [-options]
```

Tableau 40. Options securitymode

Option	Description	Valeurs
-mode	Permet de sélectionner le mode de sécurité. • CNSA - Enterprise Strict • FIPS - Standard • COMPAT- Compatibilité	CNSA, FIPS, COMPAT • **CNSA** : Seuls les services qui prennent en charge le chiffrement de niveau Enterprise Strict sont autorisés ; nécessite la clé Feature on Demand pour être activé. • **FIPS** : Les services nécessitant un chiffrement ne prennent pas en charge le chiffrement de niveau Enterprise Strict, lequel est désactivé par défaut. • **COMPAT** : Lorsque ce mode est activé, XCC ne fonctionne PAS en mode standard validé ; permet à tous les services d'être activés.
-h	Permet d'afficher la liste des utilisations et des options.	

Commande set

Utilisez cette commande pour modifier des paramètres du module IMM.

- Certains paramètres du module IMM peuvent être modifiés à l'aide d'une simple commande **set**.
- Certains de ces paramètres, tels que les variables d'environnement, sont utilisés par l'interface de ligne de commande.

Le tableau suivant présente les arguments pour les options.

Tableau 41. Commande set

Le tableau suivant, comportant une seule ligne et trois colonnes, fournit une description de la commande et des informations associées.

Option	Description	Valeurs
value	Définir une valeur pour le chemin d'accès ou le paramètre spécifié	Valeur appropriée pour le chemin d'accès ou le paramètre spécifié.

Syntaxe :
```
set [-options]
option:
  value
```

Commande snmp

Utilisez cette commande pour afficher et configurer les informations sur l'interface SNMP.

Syntaxe :
```
snmp [-options]
```

Tableau 42. Options snmp

Option	Description	Valeurs
-a3	Agent SNMPv3	on, off **Remarques :** Pour activer l'agent SNMPv3, les critères suivants doivent être remplis : • Contact du module IMM spécifié à l'aide de l'option de commande -cn. • Emplacement du module IMM spécifié à l'aide de l'option de commande -l.
-t	Interruptions SNMPv3	on, off
-tn	Nom d'utilisateur d'interruption SNMPv3	Nom d'utilisateur valide
-tauth	Protocole d'authentification d'interruption SNMPv3	none, HMAC-SHA
-tapw	Mot de passe d'authentification d'interruption SNMPv3	Mot de passe valide
-tpriv	Protocole de confidentialité d'interruption SNMPv3	none, CBC-DES, AES
-tppw	Mot de passe de confidentialité d'interruption SNMPv3	Mot de passe valide
-tix	Adresse IP ou nom d'hôte de la communauté **x**	Adresse IP ou nom d'hôte valide (limite de 63 caractères, **x** peut être compris entre 1 et 3). **Remarques :** • Une adresse IP ou un nom d'hôte peut uniquement contenir des points, traits de soulignement, signes moins, lettres et chiffres. Les espaces imbriqués ou points consécutifs ne sont pas autorisés. • Pour effacer un nom d'hôte ou une adresse IP de communauté, ne spécifiez aucun argument.

Tableau 42. Options snmp (suite)

Option	Description	Valeurs
-l	Emplacement du module IMM	Chaîne (47 caractères maximum). **Remarques :** • Les arguments contenant des espaces doivent figurer entre guillemets. Ils ne peuvent pas contenir d'espace de début ou de fin. • Pour effacer l'emplacement du module IMM, ne spécifiez aucun argument ou spécifiez une chaîne vide comme argument (par exemple «»).
-cn	Nom du contact IMM	Chaîne (47 caractères maximum). **Remarques :** • Les arguments contenant des espaces doivent figurer entre guillemets. Ils ne peuvent pas contenir d'espace de début ou de fin. • Pour effacer le nom de contact du module IMM, ne spécifiez aucun argument ou spécifiez une chaîne vide comme argument (par exemple "").
-t1	Interruptions SNMPv1	on, off
-c	Nom de communauté SNMP	Chaîne (15 caractères maximum). **Remarques :** • Les arguments contenant des espaces doivent figurer entre guillemets. Ils ne peuvent pas contenir d'espace de début ou de fin. • Pour effacer un nom de communauté SNMP, ne spécifiez aucun argument ou spécifiez une chaîne vide comme argument (par exemple «»).
-ci	Adresse IP de la communauté/nom d'hôte 1	Nom d'hôte ou adresse IP valide (63 caractères maximum). **Remarques :** • Une adresse IP ou un nom d'hôte peut uniquement contenir des points, traits de soulignement, signes moins, lettres et chiffres. Les espaces imbriqués ou points consécutifs ne sont pas autorisés. • Pour effacer un nom d'hôte ou une adresse IP de communauté, ne spécifiez aucun argument.
-c1iy	Adresse IP de la communauté/nom d'hôte **y**	Adresse IP ou nom d'hôte valide (limite de 63 caractères, **y** peut être compris entre 2 et 3). **Remarques :** • Une adresse IP ou un nom d'hôte peut uniquement contenir des points, traits de soulignement, signes moins, lettres et chiffres. Les espaces imbriqués ou points consécutifs ne sont pas autorisés. • Pour effacer un nom d'hôte ou une adresse IP de communauté, ne spécifiez aucun argument.
-t2	Alertes SNMPv2	on, off
-ct	Nom de la communauté d'alerte SNMPv2	Chaîne (15 caractères maximum). **Remarques :** • Les arguments contenant des espaces doivent figurer entre guillemets. Ils ne peuvent pas contenir d'espace de début ou de fin. • Pour effacer le nom de contact du module IMM, ne spécifiez aucun argument ou spécifiez une chaîne vide comme argument (par exemple "").

Tableau 42. Options snmp (suite)

Option	Description	Valeurs
-cti	Adresse IP de la communauté d'interruption SNMPv2/nom d'hôte 1	Nom d'hôte ou adresse IP valide (63 caractères maximum). **Remarques :** • Une adresse IP ou un nom d'hôte peut uniquement contenir des points, traits de soulignement, signes moins, lettres et chiffres. Les espaces imbriqués ou points consécutifs ne sont pas autorisés. • Pour effacer un nom d'hôte ou une adresse IP de communauté SNMP, ne spécifiez aucun argument.
-eid	ID moteur SNMP	Chaîne (de 1 à 27 caractères maximum)
-send	Envoyer un test d'informations sur les interruptions	

Exemple :
```
system> snmp
-t enabled
-a3 enabled
-l ZhangjiangMansion
-cn Kelvin
-t1 enabled
-c community1
-ci host1
-t2 enabled
-ct community2
-cti host2
-eid XCC-7Z70-DSYM09X
system>
```

Commande snmpalerts

Utilisez cette commande snmpalerts pour gérer les alertes envoyées via SNMP.

Syntaxe :
```
snmpalerts [-options]
```

Tableau 43. Options snmpalerts

Option	Description	Valeurs
-status	État de l'alerte SNMP	on, off
-crt	Définir les événements critiques devant envoyer des alertes	all, none, custom:te|vo|po|di|fa|cp|me|in|re|ot|pc Les paramètres d'alertes critiques personnalisés sont spécifiés à l'aide d'une liste de valeurs séparées par des barres verticales au format **snmpalerts -crt custom:te|vo**, où les valeurs personnalisées sont : • te : seuil de température critique dépassé • vo : seuil de tension critique dépassé • po : coupure d'alimentation critique • di : panne de l'unité de disque dur • fa : panne de ventilateur • cp : panne du microprocesseur • me : panne de mémoire • in : incompatibilité matérielle • re : défaillance de la redondance de l'alimentation • ot : tous les autres événements critiques • pc : événements critiques PCIe

Tableau 43. Options snmpalerts (suite)

Option	Description	Valeurs
-wrn	Définir les événements d'avertissement envoyant des alertes	all, none, custom:rp|te|vo|po|fa|cp|me|ot|pw Les paramètres d'alerte des avertissements personnalisés sont spécifiés à l'aide d'une liste de valeurs séparées par des barres verticales au format **snmpalerts -wrn custom:rp|te**, où les valeurs personnalisées sont : • rp : avertissement de redondance de l'alimentation • te : seuil de température d'avertissement dépassé • vo : seuil de tension d'avertissement dépassé • po : seuil d'alimentation d'avertissement dépassé • fa : événement de ventilateur non critique • cp : microprocesseur dégradé • me : avertissement de mémoire • ot : tous les autres événements d'avertissement • pw : événements d'avertissement PCIe
-sys	Définir les événements de routine envoyant des alertes	all, none, custom:lo|tio|ot|po|bf|til|pf|el|ne|nl|dh|oa Les paramètres d'alerte de routine personnalisés sont spécifiés à l'aide d'une liste de valeurs séparées par des barres verticales au format **snmpalerts -sys custom:lo|tio**, où les valeurs personnalisées sont : • lo : connexion à distance réussie • tio : délai d'attente du système d'exploitation • ot : tous les autres événements d'information et de système • po : alimentation système on/off • bf : échec d'amorçage du système d'exploitation • til : délai d'attente du programme de surveillance du chargeur de système d'exploitation • pf : échec prévu (PFA) • el : journal des événements complet à 75 % • ne : changement de réseau • nl : liaison NIC de l'hôte vers le bas/vers le haut • dh : remplacement à chaud de l'unité • oa : tous les autres événements d'audit

Commande sshcfg

Utilisez cette commande pour afficher et configurer les paramètres SSH.

Syntaxe :
```
sshcfg [-options]
```

Tableau 44. Options sshcfg

Option	Description	Valeurs
-cstatus	État de l'interface de ligne de commande SSH	enabled, disabled
-hk	Clé de serveur	gen, all • **gen** : Générer la clé privée du serveur SSH • **all** : Afficher la clé publique RSA du serveur

Exemple :
```
system> sshcfg
-cstatus enabled
CLI SSH port 22
ssh-rsa 2048 bit fingerprint: b4:a3:5d:df:0f:87:0a:95:f4:d4:7d:c1:8c:27:51:61
1 SSH public keys installed
system>
```

Commande sslcfg

Utilisez cette commande pour afficher et configurer SSL pour le module IMM et gérer les certificats.

La commande **sslcfg** permet de générer une nouvelle clé de chiffrement et un certificat autosigné ou une demande de signature de certificat (CSR).

Syntaxe :
```
sslcfg [-options]
```

Tableau 45. Options sslcfg

Option	Description	Valeurs
-server	État Web sur HTTPS	enabled, disabled **Remarques :** • Le Web sur HTTPS ne peut être activé que si un certificat est en place. • Utilisez **-rm** pour désactiver complètement le certificat.
-client	État LDAP sécurisé	enabled, disabled **Remarque :** Le client SSL peut uniquement être activé si un certificat client ou serveur valide est en place.
-cert	Générer un certificat auto-signé	server, client, sysdir, storekey **Remarques :** • Les valeurs des options de commande **-c**, **-sp**, **-cl**, **-on** et **-hn** sont requises lors de la génération d'un certificat auto-signé. • Les valeurs des options de commande **-cp**, **-ea**, **-ou**, **-s**, **-gn**, **-in** et **-dq** sont facultatives lors de la génération d'un certificat auto-signé.
-csr	Générer une demande de signature de certificat	server, client, sysdir, storekey **Remarques :** • Les valeurs des options de commande **-c**, **-sp**, **-cl**, **-on** et **-hn** sont requises lors de la génération d'une demande de signature de certificat. • Les valeurs des options de commande **-cp**, **-ea**, **-ou**, **-s**, **-gn**, **-in**, **-dq**, **-cpwd** et **-un** sont facultatives lors de la génération d'une demande de signature de certificat.

Tableau 45. Options sslcfg (suite)

Option	Description	Valeurs
-form	Format de la CSR ou du certificat qui sera exporté.	der, pem (par défaut : pem)
-algo	Algorithme CSR	p256, p384, rsa2048, rsa3072, rsa4096 **Remarque :** Une valeur par défaut (p256) sera définie s'il n'y a pas d'option -algo.
-rm	Retirer le certificat	server, storekey **Remarque :** Un certificat autosigné par défaut (serveur) est généré automatiquement après la suppression du certificat actuel.
-i	Adresse IP du serveur TFTP/ SFTP	Adresse IP valide **Remarque :** Une adresse IP du serveur TFTP ou SFTP doit être spécifiée lors du téléchargement d'un certificat ou d'une demande de signature de certificat.
-pn	Numéro de port du serveur TFTP/SFTP	Numéro de port valide (par défaut 69/22)
-u	Nom d'utilisateur du serveur SFTP	Nom d'utilisateur valide
-pw	Mot de passe du serveur SFTP	Mot de passe valide
-l	Nom de fichier du certificat	Nom de fichier valide **Remarque :** Un nom de fichier est requis lors du téléchargement d'un certificat ou d'une demande de signature de certificat. Si aucun nom de fichier n'est spécifié pour un téléchargement, le nom par défaut du fichier est utilisé et affiché.
-dnld	Exporter le fichier spécifié vers l'hôte distant	Aucun argument n'est utilisée pour cette option ; mais elle doit être utilisée avec **-cert** ou **-csr** ; ainsi que les options de commande **-i** et **-l**.
-upld	Importer le fichier de certificat	Cette option ne prend aucun argument mais doit également spécifier des valeurs pour les options de commande **-cert**, **-i** et **-l**.
-tc**x**	Certificat sécurisé **x** pour client SSL	import, download, remove **Remarque :** Le numéro de certificat sécurisé, **x**, est spécifié en tant que nombre entier allant de 1 à 4 dans l'option de commande.
Options requises pour la génération d'un certificat autosigné ou d'une demande de signature de certificat **Remarque :** Requis lors de la génération d'un certificat auto-signé ou d'une demande de signature de certificat.		
-c	Pays	Code pays (2 lettres)
-sp	Département ou province	Chaîne entre guillemets (60 caractères maximum)
-cl	Ville ou localité	Chaîne entre guillemets (50 caractères maximum)
-on	Nom de l'organisation	Chaîne entre guillemets (60 caractères maximum)
-hn	Nom d'hôte du BMC	Chaîne (60 caractères maximum)
Options facultatives pour la génération d'un certificat autosigné ou d'une demande de signature de certificat **Remarque :** Facultatif lors de la génération d'un certificat auto-signé ou d'une demande de signature de certificat.		
-cp	Personne de contact	Chaîne entre guillemets (60 caractères maximum)
-ea	Adresse électronique de la personne à contacter	Adresse e-mail valide (60 caractères maximum)
-ou	Unité organisationnelle	Chaîne entre guillemets (60 caractères maximum)

Tableau 45. Options sslcfg (suite)

Option	Description	Valeurs
-s	Nom de famille	Chaîne entre guillemets (60 caractères maximum)
-gn	Prénom	Chaîne entre guillemets (60 caractères maximum)
-in	Initiales	Chaîne entre guillemets (20 caractères maximum)
-dq	Qualificatif du nom de domaine	Chaîne entre guillemets (60 caractères maximum)
Options facultatives pour la génération d'une demande de signature de certificat **Remarque :** Facultatif lors de la génération d'une demande de signature de certificat.		
-cpwd	Mot de passe de demande d'authentification	Chaîne (6 caractères minimum, 30 caractères maximum)
-un	Nom non structuré	Chaîne entre guillemets (60 caractères maximum)

Exemples :

```
system> sslcfg
-server enabled
-client disabled
-sysdir enabled
SSL Server Certificate status:
 A self-signed certificate is installed
SSL Client Certificate status:
 A self-signed certificate is installed
SSL Client Trusted Certificate status:
 Trusted Certificate 1: Not available
 Trusted Certificate 2: Not available
 Trusted Certificate 3: Not available
 Trusted Certificate 4: Not available
```

Exemples de certificats client :

- Pour générer une demande de signature de certificat, entrez la commande suivante :
  ```
  system> sslcfg -csr storekey -c US -sp NC -cl rtp -on LNV -hn XCC-5cf3fc -cp Contact -ea "" -ou""
  ok
  ```
- Pour télécharger un certificat du module IMM vers un autre serveur, saisissez la commande suivante :
  ```
  system> sslcfg -csr storekey -dnld -i 192.168.70.230 -l storekey.csr
  ok
  ```
- Pour télécharger le certificat traité par l'autorité de certification, entrez la commande suivante :
  ```
  system> sslcfg -cert storekey -upld -i 192.168.70.230 -l tklm.der
  ```
- Pour générer un certificat autosigné, entrez la commande suivante :
  ```
  system> sslcfg -cert storekey -c US -sp NC -cl rtp -on LNV -hn XCC-5cf3fc -cp Contact -ea "" -ou "
  ok
  ```

Exemple de certificat du serveur SKLM :

- Pour importer le certificat de serveur SKLM, entrez la commande suivante :
  ```
  system> storekeycfg -add -ip 192.168.70.200 -f tklm-server.der
  ok
  ```

Commande syslock

Utilisez cette commande pour afficher et configurer les paramètres de verrouillage du système.

Syntaxe :
```
syslock [-options]
```

Tableau 46. Options syslock

Option	Description	Valeurs
-en	Activer ou désactiver la fonction de verrouillage de la configuration système. **Remarque :** Activer avec l'option **-e** peut promouvoir l'inventaire actuel en tant qu'instantané de confiance.	enabled, disabled
-e	Activer les paramètres de verrouillage de la configuration système avec ou sans application de l'inventaire actuel dans un instantané fiable. **Remarque :** Une valeur par défaut sera définie s'il n'y a pas d'option **-e**.	enabled, disabled
-l **[x]**	Répertorier l'inventaire d'un instantané spécifique à l'index **x**.	Le numéro d'index, x, est spécifié sous la forme d'un entier dans l'option de commande.
-m	Prendre un instantané manuel.	
-d	Description de l'instantané manuel.	Chaîne pouvant comprendre jusqu'à 32 caractères.
-c	Répertorier la différence d'inventaire par rapport à l'instantané de confiance.	
-po	Définir une politique de verrouillage. **Remarque :** Cette action empêche l'amorçage du serveur si la protection du système est dans un état non conforme.	none, osboot, pperm
-cpu	Définir le verrouillage de l'UC.	on, off
-dimm	Définir le verrouillage DIMM.	on, off
-pci	Définir le verrouillage PCI.	on, off
-drive	Définir le verrouillage de l'unité.	on, off
-riser	Définir le verrouillage de la carte mezzanine.	on, off
-bp	Définir le verrouillage du fond de panier.	on, off

Commande thermal

Utilisez cette commande pour afficher et configurer les règles du mode thermal du système hôte.

L'exécution de la commande **thermal** sans option affiche les règles du mode thermal. Le tableau suivant présente les arguments pour les options.

Syntaxe :
```
thermal [-options]
```

Tableau 47. Options thermal

Option	Description	Valeurs
-mode	Permet d'afficher la stratégie du mode thermique et de configurer le tableau thermique des systèmes hôte (en lecture uniquement)	• Calcul général - Efficacité de l'alimentation • Calcul général - Fréquence de crête • Calcul général - Performances maximales • Virtualisation - Efficacité de l'alimentation • Virtualisation - Performances maximales • Base de données - Traitement des transactions • Faible latence • Calcul haute performance • Personnalisé • Inconnu
-table **table_number**	**table_number** permet d'indiquer le tableau thermique différent qui doit être utilisé.	1 = Faible : Légère augmentation de la vitesse du ventilateur 2 = Intermédiaire : Augmentation modérée de la vitesse du ventilateur 3 = Élevé : Augmentation importante de la vitesse du ventilateur 0 = Normal : Aucune augmentation de la vitesse du ventilateur

Exemple :
```
system> thermal
-mode normal
-table 80860126 1 10DE0DFA 3
system>
```

Commande tls

Utilisez cette commande pour définir le niveau TLS minimal.

Syntaxe :
```
tls [-options]
```

Tableau 48. Options tls

Option	Description	Valeurs
-min	Sélectionner le niveau TLS minimal	1.2, 1.3 **Remarque :** Lorsque le mode de cryptographie est défini sur le mode de conformité NIST-800-131A, la version TLS doit être définie sur 1.2.
-h	Répertorier l'utilisation et les options	
Remarques : 1. Lorsque le mode de cryptographie est défini sur le mode de conformité NIST-800-131A, la version TLS doit être définie sur 1.2.		

Exemples :

Pour pouvoir utiliser la commande tls, exécutez la commande suivante :
```
system> tls
-h
```

```
system>
```

Pour obtenir la version tls actuelle, exécutez la commande suivante :
```
system> tls
-min 1.2
system>
```

Pour remplacer la version tls en cours par la version 1.2, exécutez la commande suivante :
```
system> tls -min 1.2
ok
system>
```

Commande trespass

Utilisez cette commande pour afficher et configurer les messages Trespass.

La commande **trespass** peut être utilisée pour afficher et configurer les messages Trespass. Les messages Trespass s'affichent lorsqu'un utilisateur se connecte via l'interface WEB ou CLI.

Syntaxe :
```
trespass [-options]
```

Tableau 49. Options trespass

Option	Description
-s	Configurer les messages Trespass
-h	Afficher les utilisations et les options

Exemple :
```
system> trespass -s testingmessage
ok
system> trespass
testingmessage
system>
system> trespass -s "testing message"
ok
system> trespass
testing message
system>
```

commande uefipw

Utilisez cette commande pour configurer les mots de passe administrateur UEFI. Le mot de passe est en écriture seule.

La commande **uefipw** peut être utilisée avec l'option « -p » pour configurer le mot de passe administrateur UEFI pour XCC ou avec l'option « -ep » pour LXCA pour configurer le mot de passe administrateur UEFI par l'interface CLI. Le mot de passe est en écriture seule.

Syntaxe :
```
uefipw [-options]
```

Tableau 50. Options uefipw

Option	Description
-cp	Mot de passe actuel (limité à 20 caractères)
-p	Nouveau de passe (limité à 20 caractères)

Commande usbeth

Utilisez cette commande pour activer l'interface LAN over USB intrabande.

Remarques :

- Les paramètres de configuration IP du système d'exploitation ne sont pas utilisés pour définir l'adresse IP du système d'exploitation de l'interface Ethernet via USB, mais ils sont utilisés pour avertir le BMC que l'adresse IP du système d'exploitation de l'Ethernet via USB a été modifiée.
- Avant de configurer les paramètres IP pour Ethernet via USB, vous devez configurer manuellement l'adresse IP du système d'exploitation de Ethernet via l'interface USB sur votre système d'exploitation local.

Syntaxe :
```
usbeth [-options]
```

Tableau 51. Options usbeth

Option	Description	Valeurs
-en	Activer ou désactiver l'interface intrabande (Ethernet sur USB).	enabled, disabled
-am	Sélectionner le mode d'adresse IPv4 ou IPv6 LLA.	ipv4, ipv6lla
Remarque : Les options -ip, -sn et -ipos ne sont valides que lorsque le mode -am ipv4 est sélectionné		
-ip	Adresse IP de l'interface Ethernet sur USB pour BMC.	Adresse IP valide
-sn	Masque de sous-réseau d'interface Ethernet sur USB pour BMC.	Adresse IP valide
-ipos	Adresse IP de l'interface Ethernet sur USB pour le système d'exploitation.	Adresse IP valide

Exemple :
```
system> usbeth
-en : disabled
system> usbeth -en enabled
ok
system> usbeth
-en : disabled
system>
```

Commande users

Utilisez cette commande pour accéder à tous les comptes utilisateurs et à leurs niveaux d'autorisation.

La commande **users** est également utilisée pour créer de nouveaux comptes utilisateurs et modifier les comptes existants. L'exécution de la commande **users** sans option affiche une liste des utilisateurs et des informations de base les concernant.

Syntaxe :

```
users [-user_index] [-options]
```

Tableau 52. Options users

Option	Description	Valeurs
-user_index	Numéro d'index du compte utilisateur.	Où **user_index** est compris entre 1 et 12 (inclus) ou **all** pour tous les utilisateurs.
-l	Afficher les jours d'expiration du mot de passe	
-n	Nom du compte utilisateur	Chaîne unique contenant uniquement des chiffres, lettres, points et traits de soulignement. Minimum de 4 caractères et maximum de 16 caractères.
-p	Mot de passe du compte utilisateur	Chaîne qui contient au moins un caractère alphabétique et un caractère non alphabétique. Minimum de 6 caractères et maximum de 255 caractères. Null crée un compte sans mot de passe que l'utilisateur doit définir au cours de la première connexion.
-shp	Définir un mot de passe crypté	Total de 64 caractères
-ssalt	Définir le salt	Limite de 64 caractères
-ghp	Obtenir le mot de passe crypté	
-gsalt	Obtenir le salt	
-ep	Mot de passe de chiffrement (pour sauvegarde/restauration)	Mot de passe valide
-esalt	salt pour mot de passe chiffré	Uniquement pour la sauvegarde ou la restauration
-r	Nom du rôle	Administrateur, opérateur, lecture seule. Voir la commande « Commande roles » à la page 126.
-clear	Effacer le compte utilisateur spécifié	Le numéro d'index du compte utilisateur à effacer doit être spécifié au format : `users -clear -user_index` **Remarque :** Si vous êtes autorisé(e) à le faire, vous pouvez supprimer votre propre compte ou celui d'autres utilisateurs, même s'ils sont actuellement connectés, tant qu'il ne s'agit pas du dernier compte restant doté de privilèges de gestion de compte utilisateur. Les sessions qui sont déjà en cours au moment de la suppression des comptes utilisateur ne seront pas automatiquement terminées.
-curr	Afficher les utilisateurs actuellement connectés	
-ai	Interface accessible par l'utilisateur	web, ssh, redfish, ipmi, snmp, all **Remarque :** Une valeur par défaut (web|ssh|redfish) sera définie s'il n'y a pas d'option -ai.
-sauth	Protocole d'authentification SNMPv3	None, HMAC_MD5, HMAC_SHA96, HMAC128_SHA224, HMAC192_SHA256, HMAC256_SHA384, HMAC384_SHA512
-spriv	Protocole de confidentialité SNMPv3	None, CBC_DES, CFB128_AES128, AES192, AES256, AES192C, AES256C

Tableau 52. Options users (suite)

Option	Description	Valeurs
-spw	Mot de passe de confidentialité SNMPv3	Mot de passe valide
-sepw	Mot de passe de confidentialité SNMPv3 (chiffré)	Mot de passe valide
-sacc	Type d'accès SNMPv3	get
-strap1	Nom d'hôte d'interruption SNMPv3 1	Nom d'hôte valide
-strap2	Nom d'hôte d'interruption SNMPv3 2	Nom d'hôte valide
-strap3	Nom d'hôte d'interruption SNMPv3 3	Nom d'hôte valide
-pk	Afficher la clé publique SSH pour l'utilisateur	Numéro d'index du compte utilisateur. **Remarques :** • Chaque clé SSH assignée à l'utilisateur est affichée avec un numéro d'index de la clé d'identification. • Lors de l'utilisation des options de clé publique SSH, l'option `-pk` doit être utilisée après l'index d'utilisateur (option `-userindex`), au format : `users -2 -pk`. • Toutes les clés sont au format OpenSSH.
Les options suivantes sont utilisées avec l'option -pk		
-e	Afficher la clé SSH entière au format OpenSSH **(option de clé publique SSH)**	Cette option ne prend pas d'argument et son utilisation exclut toutes les autres options `users -pk`. **Remarque :** Lors de l'utilisation des options de clé publique SSH, l'option `-pk` doit être utilisée après l'index d'utilisateur (option `-userindex`), au format : `users -2 -pk -e`.
-remove	Supprimer la clé publique SSH de l'utilisateur **(option de clé publique SSH)**	Le numéro d'index de clé publique à supprimer doit être indiqué en tant que `-key_index` spécifique ou comme `-all` pour toutes les clés assignées à l'utilisateur. **Remarque :** Lors de l'utilisation des options de clé publique SSH, l'option `-pk` doit être utilisée après l'index d'utilisateur (option `-userindex`), au format : `users -2 -pk -remove -1`.
-add	Ajouter la clé publique SSH pour l'utilisateur **(option de clé publique SSH)**	Clé entre guillemets au format OpenSSH **Remarques :** • L'option `-add` est utilisée indépendamment de toutes les autres options de commande `users -pk`. • Lors de l'utilisation des options de clé publique SSH, l'option `-pk` doit être utilisée après l'index d'utilisateur (option `-userindex`), au format : `users -2 -pk -add "AAAAB3NzC1yc2EAAAABIwAAA QEAvfnTUzRF7pdBuaBy4dO/aIFasa/Gtc+o/wlZnuC4aD HMA1UmnMyLOCiIaNOy4OOICEKCqjKEhrYymtAoVtfKApv Y39GpnSGRC/ qcLGWLM4cmirKL5kxHNOqIcwbT1NPceoKH j46X7E +mqlfWnAhhjDpcVFjagM3Ek2y7w/tBGrwGgN7DP HJU1tzcJy68mEAnIrzjUoR98Q3/B9cJD77ydGKe8rPdI2 hIEpXR5dNUiupA1Yd8PSSMgdukASKEd3eRRZTBl3SAtMu cUsTkYjlXcqex1OQz4+N5OR6MbNcwlsx+mTEAvvcpJhug a7OUNPGhLJMl6k7jeJiQ8Xd2p XbOZQ=="`

Tableau 52. Options users (suite)

Option	Description	Valeurs
-upld	Télécharger une clé publique SSH au format OpenSSH ou RFC4716 **(option de clé publique SSH)**	Nécessite que les options `-i` et `-l` indiquent l'emplacement de la clé. **Remarques :** • L'utilisation de l'option `-upld` exclut toutes les autres options de commande `users -pk` (à l'exception de `-i` et ers -pk-`l`). • Pour remplacer une clé par une nouvelle clé, vous devez spécifier un `-key_index`. Pour ajouter une clé à la fin de la liste des clés en cours, n'indiquez aucun index de clé. • Lors de l'utilisation des options de clé publique SSH, l'option `-pk` doit être utilisée après l'index d'utilisateur (option `-userindex`), au format : `users -2 -pk -upld -i tftp://9.72.216.40/ -l file.key`.
-dnld	Télécharger la clé publique SSH spécifiée sur un serveur TFTP/SFTP **(option de clé publique SSH)**	Nécessite qu'une option `-key_index` indique la clé à télécharger et que les options `-i` et `-l` indiquent l'emplacement de téléchargement sur un autre ordinateur exécutant un serveur TFTP. **Remarques :** • L'utilisation de l'option `-dnld` exclut toutes les autres options de commande `users -pk` (à l'exception de `-i`, `-l` et `-key_index`). • Lors de l'utilisation des options de clé publique SSH, l'option `-pk` doit être utilisée après l'index d'utilisateur (option `-userindex`), au format : `users -2 -pk -dnld -1 -i tftp://9.72.216.40/ -l file.key`.
-i	Adresse IP du serveur TFTP/SFTP pour le téléchargement d'un fichier de clés **(option de clé publique SSH)**	Adresse IP valide **Remarque :** L'option `-i` est requise par les options de commande `users -pk -upld` et `users -pk -dnld`.
-pn	Numéro de port du serveur TFTP/SFTP **(option de clé publique SSH)**	Numéro de port valide (par défaut 69/22) **Remarque :** Un paramètre facultatif pour les options de commande `users -pk -upld` et `users -pk -dnld`.
-u	Nom d'utilisateur du serveur SFTP **(option de clé publique SSH)**	Nom d'utilisateur valide **Remarque :** Un paramètre facultatif pour les options de commande `users -pk -upld` et `users -pk -dnld`.
-pw	Mot de passe du serveur SFTP **(option de clé publique SSH)**	Mot de passe valide **Remarque :** Un paramètre facultatif pour les options de commande `users -pk -upld` et `users -pk -dnld`.
-l	Nom de fichier pour le téléchargement d'un fichier de clés via TFTP ou SFTP **(option de clé publique SSH)**	Nom de fichier valide **Remarque :** L'option `-l` est requise par les options de commande `users -pk -upld` et `users -pk -dnld`.

Tableau 52. Options users (suite)

Option	Description	Valeurs
-af	Accepter les connexions venant de l'hôte **(option de clé publique SSH)**	Une liste de noms d'hôte et adresses IP séparée par des virgules et limitée à 511 caractères. Les caractères valides incluent : les caractères alphanumériques, virgules, astérisques, points d'interrogations, points d'exclamation, points, traits d'union, deux points et le symbole pourcentage.
-cm	Commentaire **(option de clé publique SSH)**	Chaîne entre guillemets pouvant comprendre jusqu'à 255 caractères. **Remarque :** Lors de l'utilisation des options de clé publique SSH, l'option `-pk` doit être utilisée après l'index d'utilisateur (option `-userindex`), au format : `users -2 -pk -cm "This is my comment."`.

Exemple :

```
system> users
 Login ID     Name      Advanced Attribute     Role            Password Expires
 --------     ----      ------------------     ------          ----------------
    1         USERID                Native     Administrator          89 day(s)
system> users -2 -n sptest -p PasswOrd12 -r Administrator
The user is required to change the password when the user logs in to the management server for the first time
ok
system> users
 Login ID     Name      Advanced Attribute      Role              Password Expires
 --------     ----      ------------------      ------            ----------------
    1         USERID                Native      Administrator            90 day(s)
    2         sptest                Native      Administrator     Password expired
system> hashpw -sw enabled -re enabled
system> users -5 -n guest5 -shp 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee -ssalt abc -r  Administr
system> users -5 ghp
292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
system> users -5 gsalt
abc
system>
```

Commandes de contrôle du module IMM

La présente rubrique fournit une liste alphabétique des commandes CLI de contrôle du module IMM.

Il existe actuellement 7 commandes de contrôle du module IMM :

Commande batch

Utilisez cette commande pour exécuter une ou plusieurs commandes CLI contenues dans un fichier.

Remarques :

- Les lignes commentaires dans le fichier batch commencent par #.
- Lors de l'exécution d'un fichier de traitement par lots, les commandes qui échouent sont renvoyées avec un code de retour signalant l'échec.
- Les commandes de fichiers de traitement par lots qui contiennent des options de commandes non reconnues peuvent générer des avertissements.

Syntaxe :

```
batch [-options]
```

Tableau 53. Options batch

Option	Description	Valeurs
-f	Nom du fichier de traitement par lots	Nom de fichier valide
-ip	Adresse IP du serveur TFTP/SFTP	Adresse IP valide
-pn	Numéro de port du serveur TFTP/SFTP	Numéro de port valide (par défaut 69/22)
-u	Nom d'utilisateur du serveur SFTP	Nom d'utilisateur valide
-pw	Mot de passe du serveur SFTP	Mot de passe valide

Exemple :
```
system> batch -f sslcfg.cli -ip 192.168.70.200
1 : sslcfg client dnld ip 192.168.70.20
Command total/errors/warnings: 8 / 1 / 0
system>
```

Commande clock

Utilisez cette commande pour afficher la date et heure courantes. Vous pouvez définir le décalage UTC et les paramètres d'heure d'été.

Syntaxe :
```
clock [-options]
```

Tableau 54. Options clock

Option	Description	Valeurs
-u	Décalage UTC	Pour un décalage UTC de +2, -7, -6, -5, -4 et -3, des paramètres spéciaux d'heure d'été sont requis. • Pour +2, les options d'heure d'été sont les suivantes : off (désactivation), ee (Europe orientale), tky (Turquie), bei (Beyrouth), amm (Amman), jem (Jérusalem). • Pour -7, les options d'heure d'été sont les suivantes : off (désactivation), mtn (Mountain), maz (Mazatlan). • Pour -6, les options d'heure d'été sont les suivantes : off (désactivation), mex (Mexique), cna (Centre de l'Amérique du Nord). • Pour -5, les options d'heure d'été sont les suivantes : off (désactivation), cub (Cuba), ena (Est de l'Amérique du Nord). • Pour -4, les options d'heure d'été sont les suivantes : off (désactivation), asu (Asuncion), cui (Cuiaba), san (Santiago), cat (Canada - Atlantique). • Pour -3, les options d'heure d'été sont les suivantes : off (désactivation), gtb (Godthab), bre (Brésil - Est).
-dst	Heure d'été	on, off, special case
-host	Format de l'heure obtenu auprès de l'hôte (par défaut : utc)	local, utc **Remarque :** Les systèmes Windows utilisent local, tandis que Linux utilise utc

Remarques :

- Le contrôleur BMC utilise l'heure du serveur hôte ou du serveur NTP.
- L'heure provenant de l'hôte peut être l'heure locale ou l'heure UTC. L'option hôte doit être définie en UTC si NTP n'est pas utilisé et que l'hôte utilise le format UTC.
- Le décalage UTC peut être au format +0200, +2:00, +2 ou 2 pour un décalage positif et -0500, -5:00 ou -5 pour un décalage négatif.
- Le décalage UTC et les réglages d'heure d'été sont utilisés avec NTP ou lorsque le mode d'hôte est UTC.

Exemple :
```
system> clock
12/12/2011 13:15:23 GMT-5:00 dst on
```

Commande info

Utilisez cette commande pour afficher et configurer les informations sur le module BMC.

Syntaxe :
```
info [-options]
```

Tableau 55. Options info

Option	Description	Valeurs
-name	Nom BMC	Chaîne
-contact	Nom de la personne à contacter pour le module BMC	Chaîne
-location	Emplacement du module BMC	Chaîne
-postal	Adresse postale complète du module BMC	Chaîne
-room	Identificateur de la salle du module BMC	Chaîne
-rack	Identificateur de l'armoire du module BMC	Chaîne
-rup	Position du module BMC dans l'armoire	Chaîne

Exemple :
```
system> info
  -name: BMCName
  -location: location
  -contact: contact
  -rack: rack
  -room: room
  -postal: postal
  -rup: 1
system>
```

Commande spreset

Utilisez cette commande pour redémarrer le module IMM.

Vous devez disposer au moins des droits Configuration avancée de l'adaptateur pour émettre cette commande.

Syntaxe :
```
spreset
```

Commandes sans agent

Cette rubrique fournit une liste alphabétique des commandes sans agent.

Il existe actuellement 3 commandes sans agent :

Commande storage

Utilisez cette commande pour afficher et configurer (si la plateforme prend en charge cette commande) des informations sur les dispositifs de stockage du serveur qui sont gérés par le module IMM.

Syntaxe :
```
storage [-options]
```

Tableau 56. Options storage

Option	Description	Valeurs
-list	Afficher une liste des cibles de stockage gérées par le module IMM.	**controllers|pools|volumes|drives** • controllers : liste des contrôleurs RAID pris en charge[1] • pools : liste des pools de stockages associés au contrôleur RAID[1] • volumes : liste des volumes de stockage associés au contrôleur RAID[1] • drives : liste des unités de stockage associées au contrôleur RAID[1]
-list **storage cible** -target **target_id**	Afficher la liste des **cibles** de stockage gérées par le module IMM en fonction des **target_id**.	**pools|volumes|drives** et **ctrl[x]|pool[x]** Où les **storage targets** et **target_id** sont : • **pools** et **ctrl[x]** : répertorient les pools de stockage associés au contrôleur RAID, en fonction de la target_id[1] • **volumes** et **ctrl[x]|pool[x]** : liste des volumes de stockage associés au contrôleur RAID, en fonction de la target_id[1] • **drives** et **ctrl[x]|pool[x]** : liste des unités de stockage associées au contrôleur RAID, en fonction de la target_id[1]
-list devices	Afficher l'état de tous les disques gérés par le module IMM.	
-show **target_id**	Afficher les informations sur la cible sélectionnée, gérée par le module IMM.	Où **target_id** est **Ctrl[x]|vol[x]|disk[x]|pool[x]**[3]
-show **target_id** info	Afficher les informations détaillées sur la cible sélectionnée, gérée par le module IMM.	Où **target_id** est **Ctrl[x]|vol[x]|disk[x]|pool[x]**[3]
-show **target_id** firmware[3]	Afficher les informations du microprogramme sur la cible sélectionnée, gérée par le module IMM.	Où **target_id** est **Ctrl[x]|disk[x]**[2]
-showinfo **nvme**	Afficher les informations sur le microprogramme du disque NVMe.	

Tableau 56. Options storage (suite)

Option	Description	Valeurs
-wthre show	Afficher le seuil d'usure SSD critique et d'avertissement.	Valeur seuil (1 à 99)
-wthre -ct **threshold value**	Définir le seuil critique d'usure du SSD.	Valeur seuil (1 à 99)
-wthre -wt **threshold value**	Définir le seuil d'avertissement d'usure du SSD.	Valeur seuil (1 à 99) **Remarque :** La valeur d'avertissement doit être supérieure à la valeur critique.
-config ctrl -scanforgn -target **target_id**[3]	Détecter la configuration RAID externe.	Où **target_id** est **ctrl[x]**[5]
-config ctrl -imptforgn -target **target_id**[3]	Importer la configuration RAID externe.	Où **target_id** est **ctrl[x]**[5]
-config ctrl -clrforgn -target **target_id**[3]	Effacer la configuration RAID externe.	Où **target_id** est **ctrl[x]**[5]
-config ctrl -clrcfg -target **target_id**[3]	Effacer la configuration RAID.	Où **target_id** est **ctrl[x]**[5]
-config ctrl -bootdevice -vd **volume** -target **target_id**	Définir le périphérique d'amorçage par volume.	Où **target_id** est **ctrl[x]** et **volume** est une valeur dans la première colonne de la sortie « liste des volumes ».
-config ctrl -bootdevice -pd **drive** -target **target_id**	Définir le périphérique d'amorçage par unité.	Où **target_id** est **ctrl[x]** et **drive** est une valeur dans la première colonne de la sortie « liste des unités ».
-config ctrl -bootdevice -index **index** -target **target_id**	Définir le périphérique d'amorçage par index.	Où **target_id** est **ctrl[x]** et **index** est une valeur dans « [] » qui est la sortie de l'option « display ».
-config ctrl -bootdevice -display -target **target_id**	Afficher le périphérique amorçable.	
-config drv -mkoffline -target **target_id**[3]	Faire passer l'unité de l'état en ligne à l'état hors ligne.	Où **target_id** est **disk[x]**[5]
-config drv -mkonline -target **target_id**[3]	Faire passer l'unité de l'état hors ligne à l'état en ligne.	Où **target_id** est **disk[x]**[5]
-config drv -mkmissing -target **target_id**[3]	Définir l'unité hors ligne en tant qu'unité correcte non configurée.	Où **target_id** est **disk[x]**[5]
-config drv -prprm -target **target_id**[3]	Préparer une unité correcte non configurée en vue de son retrait.	Où **target_id** est **disk[x]**[5]
-config drv -undoprprm -target **target_id**[3]	Annuler la préparation d'une unité correcte non configurée en vue d'une opération de retrait.	Où **target_id** est **disk[x]**[5]
-config drv -mkbad -target **target_id**[3]	Remplacer une unité correcte non configurée par une unité incorrecte non configurée.	Où **target_id** est **disk[x]**[5]

Tableau 56. Options storage (suite)

Option	Description	Valeurs
-config drv -mkgood -target **target_id**[3]	Remplacer une unité incorrecte non configurée par une unité correcte non configurée. ou Convertir l'unité JBOD (simple ensemble de disques) en une unité correcte non configurée.	Où **target_id** est **disk[x]**[5]
-config drv -mkjbod -target **target_id**[3]	Faire du disque non configuré un JBOD.	Où **target_id** est **disk[x]**[5]
-config drv -rebuild -target **target_id**[3]	Démarrer la reconstruction de l'unité.	Où **target_id** est **disk[x]**[5]
-config drv -addhsp -target **target_id**[3]	Affecter l'unité sélectionnée en tant qu'unité de secours à un contrôleur ou à des pools de stockage existants.	Où **target_id** est **disk[x]**[5]
-config drv -dedicated pools -target **target_id**[3]	Affecter l'unité en tant que disque de secours dédié aux pools de stockage sélectionnés.	Où **target_id** est **disk[x]**[5]
-config drv -rmhsp -target **target_id**[3]	Retirer l'unité de secours.	Où **target_id** est **disk[x]**[5]
-config vol -remove -target**target_id**[3]	Retirer un volume.	Où **target_id** est **vol[x]**[5]

Tableau 56. Options storage (suite)

Option	Description	Valeurs
-config vol -set [-N] [-w] [-r] [-i] [-a] [-d] [-b] -target **target_id**[3]	Modifier les propriétés d'un volume.	• [-N **volume_name**] est le nom du volume • [-w **<0|1|2|3>**] est la stratégie d'écriture dans le cache : – Entrer **0** pour la stratégie d'écriture immédiate – Entrer **1** pour la stratégie de réécriture protégée – Entrer **2** pour la stratégie de réécriture non protégée – Entrer **3** en cas d'absence de politique • [-r **<0|1>**] est la stratégie de lecture dans le cache : – Entrer **0** pour la stratégie Pas de lecture anticipée – Entrer **1** pour la stratégie Lecture anticipée • [-i **<0|1>**] est la stratégie d'E-S du cache : – Entrer **0** pour la stratégie E/S directe – Entrer **1** pour la stratégie E/S en cache • [-a **<0|2|3>**] est la stratégie d'accès : – Entrer **0** pour la stratégie Lecture Écriture – Entrer **2** pour la stratégie Lecture seule – Entrer **3** pour la stratégie Bloqué • [-d **<0|1|2>**] est la stratégie du cache du disque : – Entrer **0** si la stratégie est inchangée – Entrer **1** pour activer la stratégie[6] – Entrer **2** pour désactiver la stratégie • [-b **<0|1>**] est l'initialisation en arrière-plan : – Entrer **0** pour activer l'initialisation – Entrer **1** pour désactiver l'initialisation • **-target_id** est **vol[x]**[5]
-config vol -add [-R] [-D disk] [-H disk] [-1 hole] [-N] [-w] [-r][3],[7]	Créer un volume pour un nouveau pool de stockage lorsque la cible est un contrôleur. ou Créer un volume avec un pool de stockage existant lorsque la cible est un pool de stockage.	• [-R **<0|1|5|1E|6|10|50|60|00>**] Cette option définit le niveau RAID et elle est uniquement utilisée avec un nouveau pool de stockage • [-D disk **[id11]:disk[id12]:..disk[id21]:disk[id22]:..**] Cette option définit le groupe d'unités (y compris les plages) et elle est utilisée uniquement avec un nouveau pool de stockage • [-H disk **[id1]:disk[id2]:..**] Cette option définit le groupe d'unités de secours et elle est utilisée uniquement avec un nouveau pool de stockage • [-1 hole] Cette option définit le numéro d'index de l'espace d'ouverture libre pour un pool de stockage existant • [-N **volume_name**] est le nom du volume

Tableau 56. Options storage (suite)

Option	Description	Valeurs
		• [-w **<0|1|2|3>**] est la stratégie d'écriture dans le cache : – Entrer **0** pour la stratégie d'écriture immédiate – Entrer **1** pour la stratégie de réécriture protégée – Entrer **2** pour la stratégie de réécriture non protégée – Entrer **3** en cas d'absence de politique • [-r **<0|1>**] est la stratégie de lecture dans le cache : – Entrer **0** pour la stratégie Pas de lecture anticipée – Entrer **1** pour la stratégie Lecture anticipée
-config vol -add[-i] [-a] [-d] [-f] [-S] [-P] -target **target_id**[3]	Créer un volume pour un nouveau pool de stockage lorsque la cible est un contrôleur. ou Créer un volume avec un pool de stockage existant lorsque la cible est un pool de stockage.	• [-i **<0|1>**] est la stratégie d'E-S du cache : – Entrer **0** pour la stratégie E/S directe – Entrer **1** pour la stratégie E/S en cache • [-a **<0|2|3>**] est la stratégie d'accès : – Entrer **0** pour la stratégie Lecture Écriture – Entrer **2** pour la stratégie Lecture seule – Entrer **3** pour la stratégie Bloqué • [-d **<0|1|2>**] est la stratégie du cache du disque : – Entrer **0** si la stratégie demeure inchangée – Entrer **1** pour activer la stratégie[6] – Entrer **2** pour désactiver la stratégie • [-f **<0|1|2>**] est le type d'initialisation : – Entrer **0** pour aucune initialisation – Entrer **1** pour une initialisation rapide – Entrer **2** pour une initialisation complète • [-S **volume_size**] est la taille du nouveau volume en Mo • [-P **strip_size**] est la taille de la bande de volume, par exemple, 512B, 4K, 128K, 1M, etc • -target **target_id** est : – **ctrl[x]** (nouveau pool de stockage)[5] – **pool[x]** (pool de stockage existant)[5]

Tableau 56. Options storage (suite)

Option	Description	Valeurs
-config vol -getfreecap [-R] [-D disk] [-H disk] -target **target_id**[3]	Obtenir le volume de capacité libre du groupe d'unités.	• [-R **<0|1|5|1E|6|10|50|60|00>**] Cette option définit le niveau RAID et elle est uniquement utilisée avec un nouveau pool de stockage • [-D disk **[id11]:[id12]:..[id21]:[id22]:..**] Cette option définit le groupe d'unités (y compris les plages) et elle est utilisée uniquement avec un nouveau pool de stockage • [-H disk **[id1]:[id2]:..**]Cette option définit le groupe d'unités de secours et elle est utilisée uniquement avec un nouveau pool de stockage • -target **target_id** est **ctrl[x]**[5]
-fgi **vol[idx]**	Initialiser rapidement un ou des volumes spécifiés	Où **vol[idx]** est **vol[id1],vol[id2] :..**
-help	Afficher l'utilisation de la commande et ses options	

Remarques :

1. Cette commande est uniquement prise en charge sur les serveurs où le module IMM peut accéder au contrôleur RAID.
2. Les informations sur les microprogrammes s'affichent uniquement pour les mémoires DIMM Flash, disques et contrôleurs associés. Les informations sur les microprogrammes ne s'affichent pas pour les pools et volumes associés.
3. Les informations sont affichées sur plusieurs lignes en raison du manque d'espace.
4. Cette commande est prise en charge uniquement sur les serveurs prenant en charge les journaux RAID.
5. Cette commande est prise en charge uniquement sur les serveurs prenant en charge les configurations RAID.
6. La valeur **Enable** ne prend pas en charge les configurations de niveau RAID 1.
7. Une liste partielle des options disponibles est indiquée ici. Les autres options de la commande **storage -config vol -add** sont répertoriées sur la ligne suivante.

Exemples :

```
system> storage -config ctrl -clrcfg -target ctrl[0]
ok
system>
system> storage -config ctrl -clrforgn -target ctrl[0]
ok
system>
system> storage -config ctrl -imptforgn -target ctrl[0]
ok
system>
system> storage -config ctrl -scanforgn -target ctrl[0]
Detect 1 foreign configuration(s) on controller ctrl[0]
system>
system> storage -config drv -addhsp -dedicated pool[0-1] -target disk[0-0]
ok
system>
system> storage -config drv -addhsp -target disk[0-0]
ok
system>
system> storage -config drv -mkbad -target disk[0-0]
ok
system>
system> storage -config drv -mkgood -target disk[0-0]
ok
system>
```

```
system> storage -config drv -mkmissing -target disk[0-0]
ok
system>
system> storage -config drv -mkoffline -target disk[0-0]
ok
system>
system> storage -config drv -mkonline -target disk[0-0]
ok
system>
system> storage -config drv -prprm -target disk[0-0]
ok
system>
system> storage -config drv -rmhsp -target disk[0-0]
ok
system>
system> storage -config drv -undoprprm -target disk[0-0]
ok
system>
system> storage -config vol -add -1 1 -target pool[0-1]
ok
system>
system> storage -config vol -add -R 1 -D
disk[0-0]:disk[0-1] -w 1 -r 2 -i 0 -a 0 -d 0 -f 0
-N LD_volume -S 100000 -P 64K -H disk[0-2] -target ctrl[0]
ok
system>
system> storage -config vol -getfreecap -R 1 -D
disk[0-0]:disk[0-1] -H disk[0-2] -target ctrl[0]
The drive group configuration is good with free capacity 500000MB
system>
system> storage -config vol -remove -target vol[0-1]
ok
system>
system> storage -config vol -set -N LD_volume
-w 0 -target vol[0-0]
ok
system>
system> storage -list controllers
ctrl[0]    ServerRAID M5110e(Slot No. 0)
ctrl[1]    ServerRAID M5110f(Slot No. 1)
system>
system> storage -list drives
disk[0-0]    Drive 0
disk[0-1]    Drive 1
disk[0-2]    Drive 2
system>
system> storage -list pools
pool[0-0]    Storage Pool 0
pool[0-1]    Storage Pool 1
system>
system> storage -list volumes
vol[0-0]    Volume 0
vol[0-1]    Volume 1
Vol[0-2]    Volume 2
system>
system> storage -list drives -target ctrl[0]
disk[0-0]    Drive 0
disk[0-1]    Drive 1
disk[0-2]    Drive 2
system>
system> storage -list drives -target pool[0-0]
```

```
disk[0-0]    Drive 0
disk[0-1]    Drive 1
system>
system> storage -list pools -target ctrl[0]
pool[0-0]    Storage Pool 0
system>
system> storage -list volumes -target ctrl[0]
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
system> storage -list volumes -target pool[0-0]
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
system> storage -show ctrl[0] firmware
Total Firmware number: 2
Name: RAID Firmware1
Description: RAID Firmware
Manfacture: IBM
Version: 4.01(3)T
Release Date: 01/05/2013
Name: RAID Firmware2
Description: RAID Firmware
system>
system> storage -show ctrl[0] info
Product Name: ServerRAID M5110e
Firmware Package Version: 23.7.0.1.2
Battery Backup: Installed
Manufacture: IBM
UUID: 1234567890123456
Model Type / Model: 1234AHH
Serial No.: 12345678901
FRU No.: 5005076049CC4
Part No.: LSI2004
Cache Model Status: Unknown
Cache Model Memory Size: 300MB
Cache Model Serial No.: PBKUDOXTA0P04Y
PCI Slot Number: 0
PCI Bus Number: 2
PCI Device Number: 2
PCI Function Number: 10
PCI Device ID: 0x1000
PCI Subsystem Device ID: 0x1413
Ports: 2
Port 1: 12345678901234
Port 2: 12345678901235
Storage Pools: 2
pool[0-0]    Storage Pool 0
pool[0-1]    Storage Pool 1
Drives: 3
disk[0-0]    Drive 0
disk[0-1]    Drive 1
disk[0-2]    Drive 2
system>
system> storage -show disk[0-0] firmware
Total Firmware number: 1
Name: Drive
Description:
Manufacture:
Version: BE24
Release Date:
```

```
system>
system> storage -show disk[0-0] info
Product Name: ST98394893
State: Online
Slot No.: 0
Disk Type: SATA
Media Type: HHD
Health Status: Normal
Capacity: 100.000GB
Speed: 6.0Gb/s
Current Temperature: 33C
Manufacture: ATA
Device ID: 5
Enclusure ID: 0x00FC
Machine Type:
Model:
Serial No.: 9XKJKL
FRU No.:
Part No.:
system>
system> storage -show pool[0-0]
RAID State: RAID 0
RAID Capacity: 67.000GB (0.000GB free)
Drives: 2
disk[0-0]    Drive 0
disk[0-1]    Drive 1
Volumes: 2
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
system> storage -show pool[0-1] info
RAID State: RAID 1
RAID Capacity: 231.898GB (200.000GB free)
Holes: 2
#1 Free Capacity: 100.000GB
#2 Free Capacity: 100.000GB

Drives: 2
disk[0-1]    Drive 1
disk[0-2]    Drive 2

Volume: 1
vol[0-1]    LD_volume
system>
system> storage -show vol[0-0]
Name: Volume 0
Stripe Size: 64KB
Status: Offline
Capacity: 100.000GB
system>
system> storage -show vol[0-0] info
Name: LD_volume
Status: Optimal
Stripe Size: 64KB
Bootable: Not Bootable
Capacity: 231.898GB
Read Policy: No Read Ahead
Write Policy: Write Through
I/O Policy: Direct I/O
Access Policy: Read Write
Disk Cache Policy: Unchanged
```

```
Background Initialization: Enable
system>
```

Commande adapter

Cette commande permet d'afficher des informations relatives à l'inventaire sur les adaptateurs PCIe.

Syntaxe :
```
adapter [-options]
```

Tableau 57. Options adapter

Option	Description	Valeurs
-list	Afficher une liste de tous les adaptateurs PCIe du serveur.	
-show **target_id**	Afficher des informations détaillées sur l'adaptateur PCIe cible.	**target_id [info|firmware|ports]** Où : • **info** : afficher des informations sur le matériel de l'adaptateur • **firmware** : afficher toutes les informations sur les microprogrammes de l'adaptateur • **ports** : afficher toutes les informations sur le port Ethernet de l'adaptateur

Si la commande **adapter** n'est pas prise en charge, le serveur répond par le message suivant lorsque la commande est émise :
```
Your platform does not support this command.
```

Remarque : Si vous supprimez, remplacez ou configurez un adaptateur, vous devez redémarrer le serveur (au moins une fois) pour afficher les informations actualisées sur l'adaptateur.

Exemples :
```
system> adapter -list
ob-1     Flex System CN4054 10Gbps Virtual Fabric Adapter
ob-2     GPU Card 1
slot-1   Raid Controller 1
slot-2   Adapter 01:02:03
system>
system> adapter -show ob-1 info
Product Name: Flex System CN4054 10Gbps Virtual Fabric Adapter
Card Interface: PCIe x 16
Function Count: 2
Function Name: xxx Emulx xx component1
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1
Class Code: 2
Sub Vendor: 334
Sub Device: 223
Slot Description: a slot
Slot Type: 23
Slot Data Bus Width: 0
```

```
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
Model: 345
Function Sku: 221
Fod Uid: 2355
Required Daughter: 0
Max Data Width: 0
Connector Layout: pci x
Package Type: dici
Function Name: xxx nVidia xx component2
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1
Class Code: 2
Sub Vendor: 334
Sub Device: 223
Slot Description: a slot
Slot Type: 23
Slot Data Bus Width: 0
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
Model: 345
Function Sku: 221
Fod Uid: 2355
Required Daughter: 0
Max Data Width: 0
Connector Layout: pci x
Package Type: dici
system>
```

Commandes de support

Cette rubrique fournit une liste alphabétique des commandes de support.

Une seule commande de support est disponible : la « Commande dbgshbmc » à la page 157.

Commande dbgshbmc

Utilisez cette commande pour déverrouiller l'accès réseau au shell de débogage sécurisé.

Remarque : Cette commande était auparavant la commande **dbgshimm**.

Important : L'utilisation de cette commande est réservée au personnel de support technique.

Le tableau suivant présente les arguments pour les options.

Syntaxe :

```
dbgshbmc [subset_command]
```

Tableau 58. commandes de sous-ensemble dbgshbmc

Option	Description
status	Afficher l'état
enable	Activer l'accès au débogage (valeur par défaut en l'absence d'option spécifiée)
disable	Désactiver l'accès au débogage

Chapitre 11. Interface IPMI

Ce chapitre décrit l'interface IPMI prise en charge par XClarity Controller.

Pour plus d'informations sur les commandes IPMI standards, reportez-vous aux spécifications figurant dans la documentation (version 2.0 ou ultérieure) de l'IPMI (Intelligent Platform Management Interface). Ce document décrit les paramètres OEM utilisés avec les commandes IPMI standards, ainsi que les commandes IPMI OEM prises en charge par le microprogramme XClarity Controller.

Gestion de XClarity Controller à l'aide d'IPMI

Les informations de cette rubrique vous permettent de gérer XClarity Controller à l'aide de l'interface IPMI.

Le module XClarity Controller est livré avec un ID utilisateur défini initialement avec le nom d'utilisateur USERID et le mot de passe PASSW0RD (le chiffre 0 et non pas la lettre O). Cet utilisateur dispose d'un accès Superviseur.

Important : Pour une sécurité accrue, modifiez ce nom d'utilisateur et ce mot de passe lors de votre configuration initiale.

Dans Flex System, un utilisateur peut configurer un module CMM Flex System pour gérer de façon centralisée les comptes utilisateur IPMI de XClarity Controller. Dans ce cas, vous ne pourrez peut-être pas accéder à XClarity Controller via l'IPMI tant que le module CMM n'aura pas configuré les ID utilisateur IPMI.

Remarque : Les droits d'accès de l'ID utilisateur configurés par le module CMM peuvent être différents de la combinaison USERID/PASSW0RD décrite ci-dessus. Si aucun ID utilisateur IPMI n'a été configuré par le module CMM, le port réseau associé au protocole IPMI est fermé.

XClarity Controller fournit également les fonctions suivantes de gestion du serveur à distance IPMI :

Interfaces de ligne de commande IPMI
L'interface de ligne de commande IPMI fournit un accès direct aux fonctions de gestion du serveur via le protocole IPMI 2.0. Vous pouvez utiliser IPMItool pour émettre des commandes de contrôle de l'alimentation du serveur, afficher des informations sur le serveur et identifier le serveur. Pour plus d'informations sur IPMItool, voir « Utilisation d'IPMItool » à la page 159.

Serial over LAN
Pour gérer des serveurs depuis un site distant, utilisez IPMItool afin d'établir une connexion SOL (Serial over LAN). Pour plus d'informations sur IPMItool, voir « Utilisation d'IPMItool » à la page 159.

Utilisation d'IPMItool

Les informations de cette rubrique permettent d'accéder aux informations sur IPMItool.

IPMItool fournit différents outils qui vous permettent de gérer et de configurer un système IPMI. Vous pouvez utiliser IPMItool en mode intrabande ou hors bande pour gérer et configurer XClarity Controller.

Pour plus d'informations sur IPMItool ou pour le télécharger, visitez le site https://github.com/ipmitool/ipmitool.

Commandes IPMI avec paramètres OEM

Obtention/définition des paramètres de configuration LAN

Afin de refléter les capacités fournies par XCC pour certains paramètres réseau, les valeurs pour certaines des données de paramètre sont définies comme indiqué ci-après.

DHCP

Outre les méthodes usuelles d'obtention d'une adresse IP, XCC fournit un mode qui tente d'obtenir une adresse IP à partir d'un serveur DHCP pendant une période donnée. Si cela échoue, il bascule vers l'utilisation d'une adresse IP statique.

Le tableau suivant, à plusieurs lignes et trois colonnes, comporte les options, les descriptions d'option, ainsi que les valeurs associées pour les options.

Paramètre	#	Données de paramètre
Source d'adresse IP	4	données 1 [7:4] – réservées [3:0] – source d'adresse 0h = non spécifiée 1h = adresse statique (configurée manuellement) 2h = adresse obtenue par XCC exécutant DHCP 3h = adresse obtenue par le BIOS ou le logiciel système 4h = adresse obtenue par XCC qui exécute un autre protocole d'affectation d'adresses. XCC utilise la valeur 4h pour indiquer le mode d'adresse de DHCP avec basculement vers une valeur statique.

Sélection d'interface Ethernet

Le matériel XCC contient deux interfaces MAC Ethernet 10/100 avec RMII. Le matériel XCC contient également deux interfaces MAC Ethernet 1 Gbit/s avec RGMII. L'un des MAC est généralement connecté à la carte réseau (NIC) du serveur partagé et l'autre MAC est utilisé en tant que port de gestion système dédié. Un seul port Ethernet est actif sur un serveur à un moment donné. Les deux ports ne sont pas activés simultanément.

Sur certains serveurs, les concepteurs système peuvent choisir de connecter uniquement l'une ou l'autre de ces interfaces Ethernet sur la carte système. Dans ces systèmes, seule l'interface Ethernet connectée sur la carte est prise en charge par XCC. Une demande d'utilisation du port non connecté renvoie un code achèvement CCh.

Les ID de module pour toutes les cartes réseau facultatives sont numérotés comme suit :

- carte facultative n° 1, ID de module = 03h (eth2),
- carte facultative n° 2, ID de module = 04h (eth3),

Le tableau suivant, à plusieurs lignes et trois colonnes, comporte les options, les descriptions d'option, ainsi que les valeurs associées pour les options.

Paramètre	#	Données de paramètre
Paramètre OEM Ce numéro de paramètre est utilisé par XCC pour indiquer les ports Ethernet possibles (modules logiques) qui devraient être utilisés. Ce paramètre de la commande Obtention/définition des paramètres de configuration LAN n'utilise pas de sélecteur d'ensemble ou ne nécessite pas de sélecteur de bloc. Ces zones doivent donc être définies sur 00h. Les données de réponse renvoient 3 octets, ou éventuellement 4 octets si le périphérique se trouve dans un module NCSI. Octet 1 = code achèvement Octet 2 = révision Octet 3 = 00h pour eth0 ou 01h pour eth1, etc. Octet 4 = (facultatif) numéro de canal, si le périphérique est un module NCSI	C0h	data1 00h = eth0 01h = eth1 02h = eth2 etc. FFh = désactiver tous les ports réseau externes XCC prend en charge un second octet de données facultatif pour indiquer le canal d'un module utilisé data2 00h = canal 0 01h = canal 1 etc. Si data2 n'est pas spécifiée dans la demande, le canal 0 est utilisé par défaut

L'octet de data1 est utilisé pour indiquer le module logique. Il peut s'agir d'une carte réseau de gestion de systèmes dédiée ou d'une interface NCSI dans la carte réseau partagée avec le serveur.

L'octet de data2 est utilisé pour indiquer le canal pour le module logique, si le module est un périphérique NCSI. Si les data2 ne sont pas indiquées dans la demande et si le module logique est un périphérique NCSI, le canal 0 est utilisé par défaut. Si les data2 ne sont pas indiquées dans la demande, mais que le module logique n’est pas un périphérique NCSI, les informations du canal sont ignorées.

Exemples :

Annexe A : Si le canal 2 de la carte réseau partagée sur la carte (ID du module = 0, eth0) doit être utilisé en tant que port de gestion, les données d'entrée sont les suivantes : 0xC0 0x00 0x02

Annexe B : Si le premier canal de la première carte mezzanine réseau doit être utilisé, l'entrée doit être : 0xC0 0x02 0x0

Activer/désactiver Ethernet sur USB

Le paramètre ci-après est utilisé pour activer ou désactiver l'interface XCC interne.

Le tableau suivant, à plusieurs lignes et trois colonnes, comporte les options, les descriptions d'option, ainsi que les valeurs associées pour les options.

Paramètre	#	Données de paramètre
Paramètre OEM (Ce numéro de paramètre est utilisé par XCC pour activer ou désactiver l'interface Ethernet sur USB). Ce paramètre de la commande Obtenir les paramètres de configuration LAN n'utilise pas de sélecteur d'ensemble ou ne nécessite pas de sélecteur de bloc. Ces zones doivent donc être définies sur 00h. Les données de réponse renvoient 3 octets : Octet 1 = code achèvement Octet 2 = révision Octet 3 = 00h (désactivé) ou 01h (activé)	C1h	données 1 0x00 = désactivé 0x01 = activé

L'octet de data1 est utilisé pour indiquer le module logique. Il peut s'agir d'une carte réseau de gestion de systèmes dédiée ou d'une interface NCSI dans la carte réseau partagée avec le serveur.

L'octet de data2 est utilisé pour indiquer le canal pour le module logique, si le module est un périphérique NCSI. Si les data2 ne sont pas indiquées dans la demande et si le module logique est un périphérique NCSI, le canal 0 est utilisé par défaut. Si les data2 ne sont pas indiquées dans la demande, mais que le module logique n'est pas un périphérique NCSI, les informations du canal sont ignorées.

Exemples :

Annexe A : Si le canal 2 de la carte réseau partagée sur la carte (ID du module = 0, eth0) doit être utilisé en tant que port de gestion, les données d'entrée sont les suivantes : 0xC0 0x00 0x02

Annexe B : Si le premier canal de la première carte mezzanine réseau doit être utilisé, l'entrée doit être : 0xC0 0x02 0x0

Option IPMI permettant d'obtenir le DUID-LLT

Le DUID est une autre valeur en lecture seule qui doit être exposée via IPMI. Selon RFC3315, ce format de DUID est basé sur l'adresse de couche de liaison plus le temps.

Paramètre	#	Données de paramètre
Paramètre OEM (Ce numéro de paramètre est utilisé par XCC pour activer ou désactiver l'interface Ethernet sur USB). Ce paramètre de la commande Obtenir les paramètres de configuration LAN n'utilise pas de sélecteur d'ensemble ou ne nécessite pas de sélecteur de bloc. Ces zones doivent donc être définies sur 00h. Les données de réponse renvoient 3 octets : Octet 1 = code achèvement Octet 2 = révision du paramètre (comme dans les spécifications IPMI) Octet 3 = longueur des octets de données suivants (16 octets actuellement) Byte 4 - n DUID_LLT	C2h	

Paramètres de configuration Ethernet

Les paramètres ci-après peuvent être utilisés pour configurer des paramètres Ethernet spécifiques.

Paramètre	#	Données de paramètre
Paramètre OEM (Ce numéro de paramètre est utilisé par XCC pour activer ou désactiver le paramètre de négociation automatique pour l'interface Ethernet). Les données de réponse renvoient 3 octets : Octet 1 = code achèvement Octet 2 = révision Octet 3 = 00h (désactivé) ou 01h (activé)	C3h	données 1 0x00 = désactivé 0x01 = activé Remarque : Sur les systèmes Flex et le boîtier ThinkSystem D2 (nœud de traitement ThinkSystem SD530), le paramètre de négociation automatique n'est pas modifiable. En effet, cela pourrait interrompre le chemin de communication réseau via le CMM et le SMM.
Paramètre OEM (Ce numéro de paramètre est utilisé par XCC pour obtenir ou définir la vitesse de transfert de l'interface Ethernet). Les données de réponse renvoient 3 octets : Octet 1 = code achèvement Octet 2 = révision Octet 3 = 00h (10 Mo) ou 01h (100 Mo)	C4h	données 1 0x00 = 10 Mbit 0x01 = 100 Mbit
Paramètre OEM (Ce numéro de paramètre est utilisé par XCC pour obtenir ou définir le paramètre duplex de l'interface Ethernet). Les données de réponse renvoient 3 octets : Octet 1 = code achèvement Octet 2 = révision Octet 3 = 00h (semi-duplex) ou 01h (duplex intégral)	C5h	données 1 0x00 = semi-duplex 0x01 = duplex intégral

Paramètre	#	Données de paramètre
Paramètre OEM (Ce numéro de paramètre est utilisé par XCC pour obtenir ou définir l'unité de transmission maximale (MTU) de l'interface Ethernet). Les données de réponse renvoient 3 octets : Octet 1 = code achèvement Octet 2 = révision Octet 3-4 = taille de la MTU	C6h	données 1 Taille de la MTU
Paramètre OEM (Ce numéro de paramètre est utilisé par XCC pour obtenir ou définir une adresse MAC administrée localement.) Les données de réponse renvoient 3 octets : Octet 1 = code achèvement Octet 2 = révision Octet 3 – 8 = adresse MAC	C7h	données 1 - 6 Adresse MAC

Option IPMI permettant d'obtenir l'adresse de liaison locale

Il s'agit d'un paramètre en lecture seule permettant d'extraire l'adresse IPv6 de liaison locale.

Paramètre	#	Données de paramètre
Paramètre OEM Ce paramètre est utilisé pour obtenir l'adresse de liaison locale du XCC : Les données de réponse renvoient les éléments suivants : Octet 1 = code achèvement Octet 2 = révision du paramètre (comme dans les spécifications IPMI) Octet 3 = longueur du préfixe d'adresse IPv6 Octet 4-19 = adresse de liaison locale au format binaire	C8h	

Option IPMI pour l'activation/désactivation d'IPv6

Il s'agit d'un paramètre de lecture/écriture pour activer/désactiver IPv6 dans XCC.

Paramètre	#	Données de paramètre
Paramètre OEM Ce paramètre est utilisé pour activer/désactiver IPv6 dans XCC Les données de réponse renvoient les éléments suivants : Octet 1 = code achèvement Octet 2 = révision du paramètre (comme dans les spécifications IPMI) Octet 3 = 00h (désactivé) ou 01h (activé)	C9h	données 1 0x00 = désactivé 0x01 = activé

Passerelle Ethernet sur USB vers un réseau externe

Le paramètre ci-après est utilisé pour configurer l'Ethernet sur USB vers une passerelle Ethernet externe.

Paramètre	#	Données de paramètre
Paramètre OEM Ce paramètre de la commande Obtention/définition des paramètres de configuration LAN n'utilise pas de sélecteur d'ensemble ou ne nécessite pas de sélecteur de bloc. Ces zones doivent donc être définies sur 00h. Les données de réponse d'obtention renvoient les éléments suivants : Octet 1 = code achèvement Octet 2 = révision Octet 3 = réservé (00h) Octets 4:5 = numéro de port Ethernet sur USB (octet de poids faible en premier) Octets 6:7 = numéro de port Ethernet externe (octet de poids faible en premier) Le nombre d'octets à suivre peut varier (1, 4 ou 16 octets) selon le mode d'adressage : • Octet 8 = modes prédéfinis : 00h = le transfert est désactivé 01h = l'adresse IP CMM est utilisée Octets 8:11 = adresse IP réseau externe IPv4 sous forme binaire Octets 8:23 = adresse IP réseau externe IPv6 sous forme binaire Codes achèvement : 00h – Succès 80h – Paramètre non pris en charge C1h – La commande n'est pas pris en charge C7h – La longueur des données de demande n'est pas valide	CAh	Définir les paramètres de configuration LAN : données 1 Réservé (= 00h) données 2:3 Numéro de port Ethernet sur USB, octet de poids faible en premier données 4:5 Numéro de port Ethernet externe, octet de poids faible en premier Le nombre d'octets à suivre peut varier (1, 4 ou 16 octets) selon le mode d'adressage : données 6 00h = désactiver le transfert 01h = utiliser l'adresse IP de CMM par défaut données 6:9 Adresse IP réseau externe IPv4 sous forme binaire données 6:21 Adresse IP réseau externe IPv6 sous forme binaire
Paramètre OEM Ce paramètre est utilisé pour définir et obtenir l'adresse IP et le masque de réseau LAN sur USB du XCC : Les données de réponse renvoient les éléments suivants : Octet 1 = code achèvement	CBh	Données 1:4 Adresse IP de l'interface LAN sur USB côté XCC. Données 5:8 Masque de réseau de l'interface LAN sur USB côté XCC.

Paramètre	#	Données de paramètre
Octet 2 = révision du paramètre (comme dans les spécifications IPMI) Octet 3:10 = adresse IP et valeur du masque de réseau (octet de poids fort) en premier		
Paramètre OEM Ce paramètre est utilisé pour définir et obtenir l'adresse IP LAN sur USB du SE hôte : Les données de réponse renvoient les éléments suivants : Octet 1 = code achèvement Octet 2 = révision du paramètre (comme dans les spécifications IPMI) Octet 3:6 = adresse IP (octet de poids fort) en premier	CCh	Données 1:4 Adresse IP de l'interface LAN sur USB côté hôte.

Interroger le module logique d'inventaire

Le paramètre ci-après est utilisé pour l'interrogation de l'inventaire du module NCSI.

Paramètre	#	Données de paramètre
Paramètre OEM Ce paramètre de la commande Obtention/définition des paramètres de configuration LAN n'utilise pas de sélecteur d'ensemble ou ne nécessite pas de sélecteur de bloc. Ces zones doivent donc être définies sur 00h. Opération d'interrogation d'inventaire du module L'opération d'interrogation d'informations de module est exécutée en émettant la demande avec deux octets de données 0x00 en plus du numéro de paramètre D3h. Interroger le module d'inventaire : --> 0x0C 0x02 0x00 0xD3 0x00 0x00 La réponse XCC inclut un octet d'informations pour chaque module présent : bits 7:4 = nombre de canaux NCSI dans le module bits 3:0 = nombre de modules logiques Réponse --> 0x00 0x00 0x40 0x01 0x32 Indique que 3 modules logiques sont présents : le module 0 comporte 4 canaux NCSI le module 1 n'est pas une carte réseau NCSI et ne prend pas en charge les canaux NCSI Le module 2 comporte 3 canaux NCSI	D3h	Obtention/définition des paramètres de configuration LAN :

Obtenir/définir des données de modules logiques

Le paramètre ci-après est utilisé pour lire et pour définir la priorité affectée à chaque module.

Paramètre	#	Données de paramètre
Paramètre OEM Ce paramètre de la commande Obtention/définition des paramètres de configuration LAN n'utilise pas de sélecteur d'ensemble ou ne nécessite pas de sélecteur de bloc. Ces zones doivent donc être définies sur 00h. La commande prend en charge 2 opérations : • Lire la priorité du module • Définir la priorité du module Opération de lecture de priorité du module L'opération de lecture de priorité de module est exécutée en émettant la demande avec deux octets de données 0x00 en plus du numéro de paramètre D4h. Lire la priorité du module : --> 0x0C 0x02 0x01 0xD4 0x00 0x00 Réponse --> 0x00 0x00 0x00 0x12 0x23 module logique 0 = priorité 0 module logique 2 = priorité 1 module logique 3 = priorité 2 Opération de définition de priorité du module L'opération de définition de priorité de module est exécutée en émettant la demande avec au moins un paramètre en plus du numéro de paramètre D4h. Définir la priorité du module : --> 0x0C 0x01 0x01 0xD4 0x00 0x12 0x23 définir le module logique 0 = priorité 0 définir le module logique 2 = priorité 1	D4	Obtention/définition des paramètres de configuration LAN : Bit [7-4] = priorité du module logique (1 = la plus élevée, 15 = la plus faible) Bit [3-0] = nombre de module logique

Paramètre	#	Données de paramètre
définir le module logique 3 = priorité 2 Réponse : code achèvement uniquement, aucune donnée supplémentaire		

Obtenir/définir l'état de synchronisation réseau XCC

Paramètre	#	Données de paramètre
Paramètre OEM L'octet est utilisé pour configurer la synchronisation des paramètres réseau entre le mode de carte réseau dédiée et partagée. Ce paramètre de la commande Obtenir les paramètres de configuration LAN n'utilise pas de sélecteur d'ensemble ou ne nécessite pas de sélecteur de bloc. Ces zones doivent donc être définies sur 00h. Les données de réponse renvoient 3 octets : Octet 1 = code achèvement Octet 2 = révision Octet 3 = 00h (activé) ou 01h (désactivé)	D5h	données 1 0x00 = Synchronisation 0x01 = Indépendance

L'octet est utilisé pour configurer la synchronisation des paramètres réseau entre le mode de carte réseau dédiée et partagée. Ici, la valeur par défaut était 0h, ce qui signifie que XCC va mettre à jour automatiquement les paramètres réseau entre le changement de mode et utiliser la carte réseau partagée (sur la carte) comme référence majeure. Si la valeur est définie sur 1h, chaque paramètre réseau sera ici indépendant, ce qui signifie que nous pouvons configurer un paramètre réseau différent pour chaque mode, comme par exemple, activer VLAN en mode carte réseau dédiée et désactiver VLAN en mode carte réseau partagée.

Obtenir/définir le mode réseau XCC

Paramètre	#	Données de paramètre
Paramètre OEM Ce paramètre est utilisé pour obtenir/définir le mode réseau de la carte réseau de gestion XCC. Les données de réponse renvoient 4 octets : Octet 1 = code achèvement Octet 2 = révision Octet 3 = mode réseau appliqué/indiqué Octet 4 = ID de module du mode réseau appliqué Octet 5 = ID de canal du mode réseau appliqué	D6h	Définir les paramètres de configuration LAN : données 1 Mode réseau pour la définition Obtenir les paramètres de configuration LAN : données 1 Mode réseau pour l'obtention. Il s'agit de données facultatives, par défaut pour l'interrogation du mode réseau actuel

Commandes IPMI OEM

Le XCC prend en charge les commandes IPMI OEM suivantes : Chaque commande requiert un niveau de privilège différent, comme indiqué ci-dessous.

Code	Commandes Netfn 0x2E	Privilège
0xCC	Réinitialiser XCC aux valeurs par défaut	PRIV_USR

Code	Commandes Netfn 0x3A	Privilège
0x00	Interroger la version du microprogramme	PRIV_USR
0x0D	Informations relatives à la carte	PRIV_USR
0x1E	Options de délai de restauration de l'alimentation du châssis	PRIV_USR
0x38	NMI et réinitialiser	PRIV_USR
0x49	Lancer la collecte de données	PRIV_USR
0x4A	Envoyer fichier	PRIV_USR
0x4D	État de la collecte de données	PRIV_USR
0x50	Obtenir les informations du build	PRIV_USR
0x55	Obtenir/définir le nom d'hôte	PRIV_USR

Code	Commandes Netfn 0x3A	Privilège
0x6B	Interroger le niveau de révision du microprogramme de module FPGA	PRIV_USR
0x6C	Interroger le niveau de révision du matériel intégré	PRIV_USR
0x6D	Interroger le niveau de révision du microprogramme de PSoC	PRIV_USR
0x98	Contrôle du port USB FP	PRIV_USR
0xC7	Commutateur NM IPMI natif	PRIV_ADM

Commande Réinitialiser XCC aux valeurs par défaut

Cette commande réinitialise le paramètre de configuration XCC aux valeurs par défaut.

Fonction Net = 0x2E			
Code	**Commande**	**Demande, données de réponse**	**Description**
0xCC	Réinitialiser XCC aux valeurs par défaut	**Demande :** Octet 1 – 0x5E Octet 2 – 0x2B Octet 3 - 0x00 Octet 4 – 0x0A Octet 5 – 0x01 Octet 6 - 0xFF Octet 7 – 0x00 Octet 8 – 0x00 Octet 9 - 0x00 **Réponse :** Octet 1 – Code achèvement Octet 2 – 0x5E Octet 3 – 0x2B Octet 4 - 0x00 Octet 5 – 0x0A Octet 6 – 0x01 Octet 7 – Données de réponse 0 = Réussite non-nul = Échec	Cette commande réinitialise les paramètres de configuration XCC aux valeurs par défaut.

Commandes d'informations de carte/microprogramme

Cette section répertorie les commandes permettant d'interroger les informations sur la carte et le microprogramme.

Net Function = 0x3A			
Code	**Commande**	**Demande, données de réponse**	**Description**
0x00	Interroger la version du micropro-gramme	**Demande** : Aucune donnée sur la demande **Réponse** : Octet 1 – Code achèvement Octet 2 – Version majeure Octet 3 – Version mineure	Cette commande renvoie les numéros de version majeure et mineure du microprogramme. Si la commande est effectuée avec les données de demande de 1 octet en option, la réponse XCC renvoie également la troisième zone (révision) de la version. (Majeur. mineur. Révision)
0x0D	Interroger les informations de la carte	**Demande** : S/O **Réponse** : Octet 1 - ID du système Octet 2 – Révision de la carte	Cette commande renvoie l'ID de la carte et la révision de la carte.
0x50	Interroger les informations du build	**Demande** : S/O **Réponse** : Octet 1 – Code achèvement. Octets 2:10 – Nom ASCIIZ du build Octets 11:23 – Date de génération ASCIIZ Octets 24:31 – Heure de génération ASCII	Cette commande renvoie le nom du build, la date de génération et l'heure de génération. Le nom du build et les chaînes de date de génération ont une terminaison zéro. Le format de la date de génération est YYYY-MM-DD Par exemple : « ZUBT99A » “2005-03-07” “23:59:59”

Net Function = 0x3A			
Code	**Commande**	**Demande, données de réponse**	**Description**
0x6B	Interroger le niveau de révision du micropro-gramme de module FPGA	**Demande** : Octet 1 - Type de dispositif FPGA* Type de dispositif FPGA 0 = Local (niveau actif) 1 = Carte d'UC 1 (niveau actif) 2 = Carte d'UC 2 (niveau actif) 3 = Carte d'UC 3 (niveau actif) 4 = Carte d'UC 4 (niveau actif) 5 = ROM principale locale 6 = ROM de récupération locale **Réponse** : Octet 1 – Code achèvement Octet 2 – Niveau de révision majeur Octet 3 – Niveau de révision mineur Octet 4 – Niveau de révision sous-mineur (Octet de test sur les plateformes XCC)	Cette commande renvoie le niveau de révision du microprogramme FPGA. Si l'octet 1 est omis, alors le paramètre local (niveau actif) est sélectionné
0x6C	Interroger le niveau de révision du matériel intégré	**Demande** : Aucune donnée. **Réponse** : Octet 1 – Code achèvement Octet 2 – Niveau de révision	Cette commande renvoie le niveau de révision du matériel intégré sur lequel se trouve le FPGA.
0x6D	Interroger le niveau de révision du micropro-gramme de PSoC	**Demande** : Aucun **Réponse** : Octet 1 – Code achèvement Octet 2 – bin# Octet 3 – APID	Cette commande renvoie le niveau de révision de tous les périphériques PSoC détectés. Remarque : bin# représente un emplacement physique. Pour plus de détails, consultez la spécification du système.

Net Function = 0x3A			
Code	**Commande**	**Demande, données de réponse**	**Description**
		Octet 4 – Rév. Octet 5-6 – ID de FRU Octets 6 : N – Répétition des octets 2-6 pour chaque PSoC détecté	

Commandes de contrôle du système

La spécification IPMI fournit le contrôle d'alimentation et de réinitialisation de base. Lenovo ajoute des fonctions de contrôle supplémentaires.

<table>
<tr><th colspan="4">Fonction Net = 0x2E</th></tr>
<tr><th>Code</th><th>Commande</th><th>Demande, données de réponse</th><th>Description</th></tr>
<tr><td>0x1E</td><td>Options de délai de restauration de l'alimentation du châssis</td><td>Demande :<table><tr><td>Octet 1</td><td>Type de demande :

0x00 = Définir les options de délai

0x01 = Interroger les options de délai</td></tr><tr><td>Octet 2</td><td>(si octet 1 = 0x00)

0x00= Désactivé (par défaut)

0x01 = Aléatoire

0x02-0xFF réservé</td></tr></table>Réponse :

Octet 1 – Code achèvement

Octet 2 – Options de délai (pour la demande de requête uniquement)</td><td>Ce paramètre est utilisé lorsque la politique de restauration de l'alimentation électrique du châssis est définie sur toujours mettre sous tension ou restaurer pour mettre sous tension (si précédemment mis sous tension), une fois l'alimentation en courant alternatif appliquée/rétablie. Vous avez 2 choix : Désactivé (paramètre par défaut, aucun délai lors de la mise sous tension) et aléatoire. Le paramètre de délai aléatoire fournit un délai aléatoire, défini entre 1 et 15 secondes, à partir de l'heure à laquelle l'alimentation en courant alternatif est appliquée/rétablie et lorsque le serveur est automatiquement mis sous tension.

La commande est prise en charge par XCC uniquement sur les serveurs rack.</td></tr>
<tr><td>0x38</td><td>NMI et réinitialiser</td><td>Demande :

Octet 1 – Nombre de secondes
0 = NMI uniquement

Octet 2 – Type de réinitialisation
0 = réinitialisation logicielle
1 = cycle d'alimentation

Réponse :

Octet 1 – Code achèvement</td><td>Cette commande permet d'exécuter un système NMI. Le système peut également être réinitialisé (réamorcé) ou mis hors tension après l'interruption non masquable (NMI).

Si la zone « nombre de secondes » n'est pas définie sur 0, le système est réinitialisé ou mis hors tension après le nombre de secondes indiqué.

L'octet 2 de la demande est facultatif. Si l'octet 2 n'est pas fourni, ou s'il comporte une valeur 0x00, une réinitialisation logicielle est effectuée. Si l'octet 2 est 0x01, le système est mis hors tension.</td></tr>
</table>

Commandes diverses

Cette section décrit les commandes qui ne rentrent dans aucune autre section.

<table>
<tr><th colspan="4">Net Function = 0x3A</th></tr>
<tr><th>Code</th><th>Commande</th><th>Demande, données de réponse</th><th>Description</th></tr>
<tr><td>0x55</td><td>Obtenir/ définir le nom d'hôte</td><td>Longueur de demande = 0 :

Données de demande vides

Réponse :

<table><tr><td>Octet 1</td><td>Code achèvement</td></tr><tr><td>Octets 2-65</td><td>Nom d'hôte actuel.

ASCIIZ, chaîne terminée par une valeur null.</td></tr></table>
Longueur de demande 1-64 :

<table><tr><td>Octets 1-64</td><td>Nom d'hôte DHCP

ASCIIZ se termine par 00h</td></tr></table></td><td>Utilisez cette commande pour obtenir/définir le nom d'hôte.

Lors de la définition du nom d'hôte, la valeur souhaitée doit se terminer par 00h. Le nom d'hôte est limité à 63 caractères, plus la valeur null.</td></tr>
<tr><td>0x98</td><td>Contrôle du port USB FP</td><td>Demande :

Octet 1

<table><tr><td>01h :</td><td>Obtenir le propriétaire actuel du port USB du panneau frontal</td></tr></table>
Réponse :

Octet 1 – Code achèvement

Octet 2

<table><tr><td>00h :</td><td>Appartenant à l'hôte</td></tr><tr><td>01h :</td><td>Appartenant à BMC</td></tr></table>
Demande :

Octet 1

<table><tr><td>02h :</td><td>Obtenir la configuration du port USB</td></tr></table></td><td>Cette commande est utilisée pour interroger l'état/la configuration du port USB FP, configurer le mode/le délai d'attente du port USB FP et commuter le propriétaire du port USB entre l'hôte et le BMC.

Dans la configuration, le port USB FP peut disposer de 3 modes : dédié à l'hôte, appartement uniquement au module BMC ou partagé, ce qui permet le basculement entre l'hôte et le module BMC.

Si le mode partagé est activé, le port USB est connecté au module BMC lorsque le serveur est mis hors tension et connecté au serveur lorsque le serveur est sous tension.

Lorsque le mode partagé est activé et que le serveur est sous tension, le module BMC renvoie le port USB au serveur après un dépassement du délai d'inactivité dans la configuration.

Si le serveur est doté d'un bouton d'identification, les utilisateurs peuvent activer/désactiver le</td></tr>
</table>

<table>
<tr><th colspan="4">Net Function = 0x3A</th></tr>
<tr><th>Code</th><th>Commande</th><th>Demande, données de réponse</th><th>Description</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td></td><td>du panneau frontal</td></tr>
</table>
Réponse :

Octet 1 – Code achèvement

Octet 2

<table>
<tr><td>00h :</td><td>Dédié à l'hôte</td></tr>
<tr><td>01h :</td><td>Dédié à BMC</td></tr>
<tr><td>02h :</td><td>Mode partagé</td></tr>
</table>
Octet 3:4 – Délai d'inactivité en minutes (MSB en premier)

Octet 5 – Activer le bouton ID

<table>
<tr><td>00h :</td><td>Désactivé</td></tr>
<tr><td>01h :</td><td>Activée</td></tr>
</table>
Octet 6 – Hystérésis (facultatif) en secondes

Demande :

Octet 1

03h : définir la configuration du port USB du panneau frontal

Octet 2

<table>
<tr><td>00h :</td><td>Dédié à l'hôte</td></tr>
<tr><td>01h :</td><td>Dédié à BMC</td></tr>
<tr><td>02h :</td><td>Mode partagé</td></tr>
</table>
Octet 3:4 – Délai d'inactivité en minutes (MSB en premier)

Octet 5 – Activer le bouton ID

<table>
<tr><td>00h :</td><td>Désactivé</td></tr>
<tr><td>01h :</td><td>Activée</td></tr>
</table>
Octet 6 – Hystérésis (facultatif) en secondes

Réponse :
</td><td>bouton ID pour changer le propriétaire du port USB FP en maintenant le bouton ID enfoncé pendant plus de 3 secondes.

L'hystérésis en secondes est définie lors du basculement automatique du port pendant le cycle d'alimentation. Ce paramètre est facultatif.

Serveurs SD530

Sur la plateforme SD530, le port est facultatif et, s'il est présent, connecté directement au XCC, et uniquement au XCC. Basculement du port à l'hôte non disponible.

• Lorsque la commande est émise avec l'octet 1 = 1, le XCC répond toujours que le port appartient au module BMC.
• Lorsque la commande est émise avec l'octet 1 = 2, le XCC répond toujours que le port est dédié au module BMC.
• Lorsque la commande est émise avec l'octet 1 = 3 ou l'octet 1 = 4, le XCC répond avec le code achèvement D6h.

Serveurs non SD530

Sur la plateforme non SD530, l'utilisation du port USB du panneau frontal par XCC peut être désactivée en basculant en mode « hôte uniquement »

Lorsque la commande est émise avec l'octet 1 = 5 ou l'octet 1 = 6, le XCC répond avec le code achèvement D6h.</td></tr>
</table>

<table>
<tr><th colspan="4">Net Function = 0x3A</th></tr>
<tr><th>Code</th><th>Commande</th><th>Demande, données de réponse</th><th>Description</th></tr>
<tr><td></td><td></td><td>Octet 1 – code achèvement
Octet 2
<table><tr><td>00h :</td><td>Basculer vers l'hôte</td></tr><tr><td>01h :</td><td>Basculer vers BMC</td></tr></table>
Réponse :
Octet 1 – Code achèvement
Octet 1
<table><tr><td>05h :</td><td>Activer/ désactiver le port USB du panneau frontal</td></tr></table>
Octet 2
<table><tr><td>00h :</td><td>Désactiver</td></tr><tr><td>01h :</td><td>Activation</td></tr></table>
Réponse :
Octet 1 – Code achèvement
Demande :
Octet 1
<table><tr><td>06h :</td><td>Lire l'état d'activation/ désactivation du port USB du panneau frontal</td></tr></table>
Réponse :
Octet 1 - Code achèvement
Octet 2</td><td></td></tr>
<tr><td>0xC7</td><td>Commutateur NM IPMI natif</td><td>Longueur de demande = 0 :
Données de demande vides
Réponse :
<table><tr><td>Octet 1</td><td>Code achèvement</td></tr></table></td><td>Cette commande permet d'activer/ désactiver la fonction de passerelle de XCC pour les commandes IPMI Native Intel.</td></tr>
</table>

<table>
<tr><th colspan="4">Net Function = 0x3A</th></tr>
<tr><th>Code</th><th>Commande</th><th>Demande, données de réponse</th><th>Description</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>Octets 2</td><td>État d'activation/ désactivation actuel</td></tr>
</table>
Longueur de demande = 1 :
<table>
<tr><td>Octet 1</td><td>Attribut Activer/ Désactiver de l'interface IPMI Native NM

00h – Désactiver

01h – Activer</td></tr>
</table>
Réponse :
<table>
<tr><td>Octet 1</td><td>Code achèvement</td></tr>
</table>
</td><td></td></tr>
</table>

Annexe A. Service d’aide et d’assistance

Lenovo met à votre disposition un grand nombre de services que vous pouvez contacter pour obtenir de l’aide, une assistance technique ou tout simplement pour en savoir plus sur les produits Lenovo.

Sur le Web, vous trouverez des informations à jour relatives aux systèmes, aux dispositifs en option, à Lenovo Services et support Lenovo sur :

http://datacentersupport.lenovo.com

Remarque : Cette section contient des références à des sites Web IBM et des informations relatives à l’assistance technique. IBM est le prestataire de services préféré de Lenovo pour ThinkSystem.

Avant d'appeler

Avant d’appeler, vous pouvez exécuter plusieurs étapes pour essayer de résoudre vous-même le problème. Si vous devez contacter le service, rassemblez les informations dont le technicien de maintenance aura besoin pour résoudre plus rapidement le problème.

Tentative de résolution du problème par vous-même

Bon nombre de problèmes peuvent être résolus sans aide extérieure. Pour cela, suivez les procédures indiquées par Lenovo dans l’aide en ligne ou dans la documentation de votre produit Lenovo. La documentation produit Lenovo décrit également les tests de diagnostic que vous pouvez exécuter. La documentation de la plupart des systèmes, des systèmes d’exploitation et des programmes contient des procédures de dépannage, ainsi que des explications sur les messages et les codes d’erreur. Si vous pensez que le problème est d’origine logicielle, consultez la documentation qui accompagne le système d’exploitation ou le programme.

La documentation des produits ThinkSystem est disponible à l’adresse suivante :

https://pubs.lenovo.com/

Vous pouvez suivre la procédure ci-dessous pour tenter de résoudre le problème vous-même :

- Vérifiez que tous les câbles sont bien connectés.
- Observez les interrupteurs d’alimentation pour vérifier que le système et les dispositifs en option éventuels sont sous tension.
- Vérifiez si des mises à jour du logiciel, du microprogramme et des pilotes de périphériques du système d’exploitation sont disponibles pour votre produit Lenovo. La Déclaration de garantie Lenovo souligne que le propriétaire du produit Lenovo (autrement dit vous) est responsable de la maintenance et de la mise à jour de tous les logiciels et microprogrammes du produit (sauf si lesdites activités sont couvertes par un autre contrat de maintenance). Votre technicien vous demandera de mettre à niveau vos logiciels et microprogrammes si ladite mise à niveau inclut une solution documentée permettant de résoudre le problème.
- Si vous avez installé un nouveau matériel ou un logiciel dans votre environnement, consultez http://www.lenovo.com/serverproven/ pour vous assurer que le matériel ou le logiciel est pris en charge par votre produit.
- Pour plus d’informations sur la résolution d’un incident, accédez à http://datacentersupport.lenovo.com.
  - Consultez les forums Lenovo à l'adresse suivante : https://forums.lenovo.com/t5/Datacenter-Systems/ct-p/sv_eg pour voir si d'autres personnes ont rencontré un problème identique.

Bon nombre de problèmes peuvent être résolus sans aide extérieure. Pour cela, suivez les procédures indiquées par Lenovo dans l'aide en ligne ou dans la documentation de votre produit Lenovo. La documentation produit Lenovo décrit également les tests de diagnostic que vous pouvez exécuter. La documentation de la plupart des systèmes, des systèmes d'exploitation et des programmes contient des procédures de dépannage, ainsi que des explications sur les messages et les codes d'erreur. Si vous pensez que le problème est d'origine logicielle, consultez la documentation qui accompagne le système d'exploitation ou le programme.

Collecte des informations requises pour appeler le support

Si vous pensez avoir besoin du service prévu par la garantie pour votre produit Lenovo, les techniciens de maintenance peuvent vous aider à préparer plus efficacement votre appel. Pour plus d'informations sur la garantie de votre produit, vous pouvez également consulter http://datacentersupport.lenovo.com/warrantylookup.

Rassemblez les informations suivantes pour les transmettre au technicien de maintenance. Ces données peuvent aider le technicien de maintenance à trouver rapidement une solution à votre problème et garantir que vous receviez le niveau de service attendu du contrat auquel vous avez souscrit.

- Numéros de contrat de maintenance matérielle et logicielle, le cas échéant
- Numéro de type de machine (identificateur de la machine Lenovo à 4 chiffres)
- Numéro de modèle
- Numéro de série
- Niveaux du code UEFI et du microprogramme du système
- Autres informations utiles (par exemple, les messages d'erreur et journaux)

Au lieu d'appeler Support Lenovo, vous pouvez accéder à https://www-947.ibm.com/support/servicerequest/Home.action pour soumettre une demande de service électronique. L'envoi d'une demande de service électronique lance la détermination d'une solution au problème en fournissant les informations pertinentes disponibles aux techniciens de maintenance. Les techniciens de maintenance Lenovo peuvent commencer à travailler sur votre solution dès que vous avez complété et déposé une demande de service électronique.

Collecte des données de maintenance

Pour identifier clairement la cause principale d'un problème de serveur ou à la demande du support Lenovo, vous devrez peut-être collecter les données de maintenance qui peuvent être utilisées pour une analyse plus approfondie. Les données de maintenance contiennent des informations telles que les journaux des événements et l'inventaire matériel.

Les données de maintenance peuvent être collectées avec les outils suivants :

- **Lenovo XClarity Controller**

  Vous pouvez utiliser l'interface Web ou CLI du Lenovo XClarity Controller pour collecter les données de maintenance pour le serveur. Le fichier peut être enregistré et envoyé au support Lenovo.

  - Pour plus d'informations sur l'utilisation de l'interface Web pour collecter les données de maintenance, voir https://pubs.lenovo.com/xcc3/nn1ia_c_servicesandsupport.html.
  - Pour plus d'informations sur l'utilisation de l'interface CLI pour collecter les données de maintenance, voir https://pubs.lenovo.com/xcc3/nn1ia_r_ffdccommand.html.

- **Lenovo XClarity Administrator**

  Lenovo XClarity Administrator peut être configuré pour la collecte et l'envoi automatique de fichiers de diagnostic au support Lenovo lorsque certains événements réparables se produisent dans Lenovo XClarity Administrator et sur les nœuds finaux gérés. Vous pouvez choisir d'envoyer les fichiers de

diagnostic au Support Lenovo à l'aide de la fonction d'Call Home 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 Centre de support Lenovo.

Vous trouverez d'autres informations sur la configuration de la notification automatique de problème au sein de Lenovo XClarity Administrator via https://pubs.lenovo.com/lxca/admin_setupcallhome.html.

- **Lenovo XClarity Provisioning Manager**

  Utilisez la fonction de collecte des données de maintenance de Lenovo XClarity Provisioning Manager pour collecter les données de maintenance du système. Vous pouvez collecter les données du journal système existantes ou exécuter un nouveau diagnostic afin de collecter de nouvelles données.

- **Lenovo XClarity Essentials**

  Lenovo XClarity Essentials peut être exécuté intrabande à partir du système d'exploitation. Outre les données de maintenance du matériel, Lenovo XClarity Essentials peut collecter des informations sur le système d'exploitation, comme le journal des événements du système d'exploitation.

  Pour obtenir les données de maintenance, vous pouvez exécuter la commande `getinfor`. Pour plus d'informations sur l'exécution de `getinfor`, voir https://pubs.lenovo.com/lxce-onecli/onecli_r_getinfor_command.html.

Contact du support

Vous pouvez contacter le support pour vous aider à résoudre un problème.

Vous pouvez bénéficier du service matériel auprès d'un prestataire de services agréé par Lenovo. Pour trouver un prestataire de services autorisé par Lenovo à assurer un service de garantie, accédez à https://datacentersupport.lenovo.com/us/en/serviceprovider et utilisez les filtres pour effectuer une recherche dans différents pays. Pour obtenir les numéros de téléphone du support Lenovo, voir https://datacentersupport.lenovo.com/us/en/supportphonelist pour plus de détails concernant votre région.

Annexe B. Consignes

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services Lenovo non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial Lenovo.

Toute référence à un produit, logiciel ou service Lenovo n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit de Lenovo. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par Lenovo.

Lenovo peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document n'est pas une offre et ne fournit pas de licence sous brevet ou demande de brevet. Vous pouvez en faire la demande par écrit à l'adresse suivante :

Lenovo (United States), Inc.
1009 Think Place
Morrisville, NC 27560
U.S.A.
Attention: Lenovo VP of Intellectual Property

LE PRÉSENT DOCUMENT EST LIVRÉ « EN L'ÉTAT » SANS GARANTIE DE QUELQUE NATURE. LENOVO DÉCLINE TOUTE RESPONSABILITÉ, EXPLICITE OU IMPLICITE, RELATIVE AUX INFORMATIONS QUI Y SONT CONTENUES, Y COMPRIS EN CE QUI CONCERNE LES GARANTIES DE NON-CONTREFAÇON ET D'APTITUDE À L'EXÉCUTION D'UN TRAVAIL DONNÉ. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Il est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Lenovo peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Les produits décrits dans ce document ne sont pas conçus pour être implantés ou utilisés dans un environnement où un dysfonctionnement pourrait entraîner des dommages corporels ou le décès de personnes. Les informations contenues dans ce document n'affectent ni ne modifient les garanties ou les spécifications des produits Lenovo. Rien dans ce document ne doit être considéré comme une licence ou une garantie explicite ou implicite en matière de droits de propriété intellectuelle de Lenovo ou de tiers. Toutes les informations contenues dans ce document ont été obtenues dans des environnements spécifiques et sont présentées en tant qu'illustration. Les résultats peuvent varier selon l'environnement d'exploitation utilisé.

Lenovo pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les références à des sites Web non Lenovo sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit Lenovo et l'utilisation de ces sites relève de votre seule responsabilité.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats

peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Marques

Lenovo, le logo Lenovo, ThinkSystem, Flex System, System x, NeXtScale System et x Architecture sont des marques de Lenovo aux États-Unis et/ou dans certains autres pays.

Intel et Intel Xeon sont des marques d'Intel Corporation aux États-Unis et/ou dans certains autres pays.

Internet Explorer, Microsoft et Windows sont des marques du groupe Microsoft.

Linux est une marque de Linus Torvalds.

Les autres noms de sociétés, de produits et de services peuvent appartenir à des tiers.

Remarques importantes

La vitesse du processeur correspond à la vitesse de l'horloge interne du microprocesseur. D'autres facteurs peuvent également influer sur les performances d'une application.

Les vitesses de l'unité de CD-ROM ou de DVD-ROM recensent les débits de lecture variable. La vitesse réelle varie et est souvent inférieure aux vitesses maximales possibles.

Lorsqu'il est fait référence à la mémoire du processeur, à la mémoire réelle et virtuelle ou au volume des voies de transmission, 1 Ko correspond à 1 024 octets, 1 Mo correspond à 1 048 576 octets et 1 Go correspond à 1 073 741 824 octets.

Lorsqu'il est fait référence à la capacité de l'unité de disque dur ou au volume de communications, 1 Mo correspond à un million d'octets et 1 Go correspond à un milliard d'octets. La capacité totale à laquelle l'utilisateur a accès peut varier en fonction de l'environnement d'exploitation.

La capacité maximale de disques durs internes suppose que toutes les unités de disque dur standard ont été remplacées et que toutes les baies d'unité sont occupées par des unités Lenovo. La capacité de ces unités doit être la plus importante disponible à ce jour.

La mémoire maximale peut nécessiter le remplacement de la mémoire standard par un module de mémoire en option.

Chaque cellule de mémoire à semi-conducteurs a un nombre fini intrinsèque de cycles d'écriture qu'elle peut prendre en charge. Par conséquent, un dispositif SSD peut avoir un nombre de cycles d'écriture maximal exprimé en `total bytes written` (TBW). Un périphérique qui excède cette limite peut ne pas répondre aux commandes générées par le système ou peut ne pas être inscriptible. Lenovo n'est pas responsable du remplacement d'un périphérique ayant dépassé son nombre maximal garanti de cycles de programme/d'effacement, comme stipulé dans les spécifications publiées officielles du périphérique.

Lenovo ne prend aucun engagement et n'accorde aucune garantie concernant les produits non Lenovo. Seuls les tiers sont chargés d'assurer directement le support des produits non Lenovo.

Les applications fournies avec les produits Lenovo peuvent être différentes des versions mises à la vente et ne pas être fournies avec la documentation complète ou toutes les fonctions.

Contamination particulaire

Attention : Les particules aériennes (notamment poussières ou particules métalliques) et les gaz réactifs agissant seuls ou en combinaison avec d'autres facteurs environnementaux tels que l'humidité ou la température peuvent représenter un risque pour l'unité décrite dans le présent document.

En particulier, des concentrations trop élevées de particules ou de gaz dangereux peuvent endommager l'unité et entraîner des dysfonctionnements voire une panne complète. Cette spécification présente les seuils de concentration en particules et en gaz qu'il convient de respecter pour éviter de tels dégâts. Ces seuils ne doivent pas être considérés ou utilisés comme des limites absolues, car d'autres facteurs comme la température ou l'humidité de l'air peuvent modifier l'impact des particules ou de l'atmosphère corrosive et les transferts de contaminants gazeux. En l'absence de seuils spécifiques définis dans le présent document, vous devez mettre en œuvre des pratiques permettant de maintenir des niveaux de particules et de gaz conformes aux réglementations sanitaires et de sécurité. Si Lenovo détermine que les niveaux de particules ou de gaz de votre environnement ont provoqué l'endommagement de l'unité, Lenovo peut, sous certaines conditions, mettre à disposition la réparation ou le remplacement des unités ou des composants lors de la mise en œuvre de mesures correctives appropriées, afin de réduire cette contamination environnementale. La mise en œuvre de ces mesures correctives est de la responsabilité du client.

Tableau 59. Seuils de concentration en particules et en gaz

Contaminant	Seuils
Particules	• L'air de la pièce doit être filtré en continu avec une efficacité contre la poussière atmosphérique de 40 % (MERV 9), conformément à la norme ASHRAE 52.2[1]. • L'air pénétrant dans un centre de données doit être filtré avec une efficacité minimale de 99,97 %, en utilisant des filtres HEPA (filtre à haute efficacité pour les particules de l'air) conformes à la norme MIL-STD-282. • Le taux de déliquescence (absorption de l'humidité relative) lié à la contamination particulaire doit être supérieur à 60 %[2]. • La pièce ne doit présenter aucun risque de contamination par conducteurs, par exemple des filaments de zinc.
Gaz	• Cuivre : Classe G1 selon la norme ANSI/ISA 71.04-1985[3] • Argent : Taux de corrosion inférieur à 300 Å en 30 jours

[1] ASHRAE 52.2-2008 - **Méthode de test de l'air de ventilation général - Nettoyage des unités pour une suppression efficace par taille de particule**. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

[2] L'humidité relative de déliquescence de la contamination particulaire est l'humidité relative à partir de laquelle la poussière absorbe suffisamment d'eau pour devenir humide et favoriser la conduction ionique.

[3] ANSI/ISA-71.04-1985. **Conditions environnementales pour les systèmes de mesure et de contrôle des processus : Contaminants atmosphériques**. Instrument Society of America, Research Triangle Park, Caroline du Nord, États-Unis

Déclaration réglementaire relative aux télécommunications

Ce produit n'est peut-être pas certifié dans votre pays pour la connexion, par quelque moyen que ce soit, aux interfaces des réseaux de télécommunications publics. Des certifications supplémentaires peuvent être requises par la loi avant d'effectuer toute connexion. Contactez un représentant Lenovo ou votre revendeur pour toute question.

Déclarations de compatibilité électromagnétique

Lorsque vous connectez un moniteur à l'équipement, vous devez utiliser les câbles conçus pour le moniteur ainsi que tous les dispositifs antiparasites livrés avec le moniteur.

Vous trouverez d'autres consignes en matière d'émissions électroniques sur :

https://pubs.lenovo.com/

Déclaration BSMI RoHS pour Taïwan

單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛Lead (Pb)	汞Mercury (Hg)	鎘Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr^{+6})	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
機架	○	○	○	○	○	○
外部蓋板	○	○	○	○	○	○
機械組合件	–	○	○	○	○	○
空氣傳動設備	–	○	○	○	○	○
冷卻組合件	–	○	○	○	○	○
內存模塊	–	○	○	○	○	○
處理器模塊	–	○	○	○	○	○
鍵盤	–	○	○	○	○	○
調製解調器	–	○	○	○	○	○
監視器	–	○	○	○	○	○
滑鼠	–	○	○	○	○	○
電纜組合件	–	○	○	○	○	○
電源	–	○	○	○	○	○
儲備設備	–	○	○	○	○	○
電池匣組合件	–	○	○	○	○	○
有mech的電路卡	–	○	○	○	○	○
無mech的電路卡	–	○	○	○	○	○
雷射器	–	○	○	○	○	○

備考1.〝超出0.1 wt %〞及〝超出0.01 wt %〞係指限用物質之百分比含量超出百分比含量基準值。

Note1 : “exceeding 0.1wt%” and “exceeding 0.01 wt%” indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.

備考2.〝○〞係指該項限用物質之百分比含量未超出百分比含量基準值。

Note2 : “○”indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.

備考3.〝-〞係指該項限用物質為排除項目。

Note3 : The “-“ indicates that the restricted substance corresponds to the exemption.

Informations de contact pour l'importation et l'exportation de Taïwan

Des contacts sont disponibles pour les informations d'importation et d'exportation de Taïwan.

委製商/進口商名稱: 台灣聯想環球科技股份有限公司
進口商地址: 台北市南港區三重路 66 號 8 樓
進口商電話: 0800-000-702

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

X