Lenovo

XClarity Controller 2
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 237.

Première édition (Mai 2021)

Table des matières

Table des matières i

Chapitre 1. Introduction 1

Fonctionnalités de niveau standard et Platinum de XClarity Controller 2

Fonctionnalités de niveau standard de XClarity Controller 2

Fonctionnalités de niveau Platinum de XClarity Controller 5

Mise à niveau de XClarity Controller 6

Exigences relatives au navigateur Web et au système d'exploitation 6

Support multilingue 7

Introduction aux MIB 8

Consignes utilisées dans ce document 8

Chapitre 2. Ouverture et utilisation de l'interface Web de XClarity Controller 9

Accès à l'interface Web de XClarity Controller 9

Configuration de la connexion réseau de XClarity Controller via XClarity Provisioning Manager 10

Connexion à XClarity Controller 12

Description des fonctions de XClarity Controller dans l'interface Web 13

Chapitre 3. Configuration de XClarity Controller 17

Configuration des comptes utilisateur/LDAP . . . 17

Méthode d'authentification utilisateur 17

Création d'un rôle 18

Création d'un compte utilisateur 19

Suppression d'un compte utilisateur 21

Utilisation de mots de passe cryptés pour l'authentification 21

Configuration des paramètres de connexion globale 23

Configuration LDAP 25

Configuration des protocoles réseau 31

Configuration des paramètres Ethernet 31

Configuration DNS 33

Configuration DDNS 33

Configuration d'Ethernet sur USB 34

Configuration SNMP 35

Activation ou désactivation de l'accès réseau IPMI 35

Configuration des paramètres réseau à l'aide de commandes IPMI 35

Activation du service et affectation de port . . 36

Configuration de la restriction d'accès 37

Configuration du port USB du panneau frontal pour la gestion 38

Configuration des paramètres de sécurité 39

Tableau de bord de sécurité 39

Mode de sécurité 39

Passage au mode de sécurité 42

Présentation de SSL 42

Traitement des certificats SSL 42

Gestion des certificats SSL 43

Configuration du serveur Secure Shell 44

IMPI sur accès KCS à XClarity Controller . . . 44

Enveloppement du journal IPMI SEL 45

Comment éviter de revenir au niveau antérieur du microprogramme du système - 45

Configuration du serveur de gestion de clé de sécurité (SKM) 45

Security password manager 50

Journal d'audit étendu 50

Limite de connexions simultanées par compte utilisateur 50

Protection du système 51

Paramètres cryptographiques 51

Configuration de l'appel vers Lenovo 53

Sauvegarde et restauration de la configuration BMC 55

Sauvegarde de la configuration BMC 56

Restauration de la configuration BMC 56

Réinitialisation de BMC aux paramètres d'usine par défaut 56

Redémarrage de XClarity Controller 57

Chapitre 4. Surveillance de l'état du serveur 59

Affichage de l'état d'intégrité/des événements système actifs 59

Affichage des informations système 60

Affichage de l'utilisation du système 62

Affichage des journaux des événements 63

Affichage des journaux d'audit 64

Affichage de l'historique de maintenance 65

Configuration des destinataires de l'alerte 65

Capture des données d'écran du dernier échec du système d'exploitation 67

Chapitre 5. Configuration du serveur 69

Affichage des informations et des paramètres de configuration de l'adaptateur 69
Configuration du mode d'amorçage système et de l'ordre d'amorçage 69
Configuration d'amorçage unique 70
Gestion de l'alimentation du serveur 71
Configuration de la redondance d'alimentation 71
Configuration de la stratégie de plafonnement énergétique 72
Configuration de la stratégie de restauration de l'alimentation 72
Actions d'alimentation 73
Gestion et surveillance de la consommation électrique à l'aide de commandes IPMI 74
Fonctionnalité de console distante 76
Activation de la fonction de console distante 77
Contrôle à distance de l'alimentation 77
Écran de capture de console distante 78
Prise en charge du clavier de la console distante 78
Prise en charge de la souris de la console distante 79
Enregistrement/relecture de vidéo à l'écran . . 79
Modes d'écran de console distante 80
Méthodes de montage de support 80
Disque distant utilisant le client Java 85
Problèmes liés aux erreurs de montage de support 89
Sortie de la session de console distante . . . 91
Téléchargement du journal des données de maintenance 91
Propriétés du serveur 91
Définition de l'emplacement et du contact . . . 91
Configuration des délais d'attente du serveur 92
Message Trespass 93
Définition des date et heure XClarity Controller . . . 93

Chapitre 6. Configuration du stockage 95
Détails RAID 95
Configuration RAID 95
Affichage et configuration des unités virtuelles 95
Affichage et configuration de l'inventaire de stockage 96

Chapitre 7. Mise à jour du microprogramme de serveur 99
Présentation 99
Mise à jour du microprogramme du système, de l'adaptateur et du bloc d'alimentation 100
Mise à jour à partir du référentiel 100

Chapitre 8. Gestion des licences . . . 105
Installation d'une clé d'activation 105
Retrait d'une clé d'activation 106
Exportation d'une clé d'activation 106

Chapitre 9. Gestion de groupe voisin 107
Fonctionnalités prises en charge 107
Détection de nœuds voisins 108
Configuration de groupe voisin 108
Approvisionnement de groupe voisin 108

Chapitre 10. API REST REDFISH de Lenovo XClarity Controller. 111

Chapitre 11. Interface de ligne de commande 113
Accès à l'interface de ligne de commande 113
Connexion à la session de ligne de commande . . 113
Configuration de la redirection série à SSH 113
Syntaxe de commande 114
Fonctionnalités et limitations 114
Liste des commandes par ordre alphabétique . . . 115
Commandes d'utilitaire 117
Commande exit 117
Commande help 117
Commande history 118
Commandes de surveillance 118
Commande clearlog 118
Commande fans 119
Commande ffdc 119
Commande hreport 121
Commande mhlog 121
Commande led 122
Commande readlog 124
Commande syshealth 125
Commande temps 125
Commande volts 126
Commande vpd 127
Commande de contrôle de l'alimentation et du redémarrage du serveur 127
Commande power 127
Commande reset 129
Commande fuelg 130
Commande pxeboot 131
Commande Serial redirect 132
Commande console 132
Commandes de configuration 132
Commande accseccfg 132

Commande alertcfg 134
Commande asu 134
Commande backup 137
Commande dhcpinfo 138
Commande dns 139
Commande encaps 141
Commande ethtousb 141
Commande firewall 142
Commande gprofile 143
Commande hashpw 144
Commande ifconfig 145
Commande keycfg 148
Commande ldap 149
Commande ntp 151
Commande portcfg 152
Commande portcontrol 153
Commande ports 154
Commande rdmount 155
Commande restore 155
Commande restoredefaults 156
Commande roles 157
Commande seccfg 158
Commande set 158
Commande smtp 158
Commande snmp 159
Commande snmpalerts 161
Commande srcfg 163
Commande sshcfg 164
Commande ssl 165
Commande sslcfg 166
Commande storekeycfg 170
Commande syncrep 171
Commande thermal 172
Commande timeouts 173
Commande tls 173
Commande trespass 174
commande trespass 175
Commande usbeth 176
Commande usbfp 176
Commande users 176
Commandes de contrôle de IMM 181
Commande alertentries 181
Commande batch 184
Commande clearcfg 184
Commande clock 185
Commande identify 185
Commande info 186
Commande spreset 186
Commandes de Service Advisor 186
Commande chconfig 187
Commande chmanual 189
Commande chlog 189
Commandes sans agent 190
Commande storage 190
Commande adapter 200
Commande mvstor 202
Commandes Support 203
Commande dbgshimm 203

Chapitre 12. Interface IPMI 205
Gestion de XClarity Controller à l'aide d'IPMI . . . 205
Utilisation d'ipmitool 205
Commandes IPMI avec paramètres OEM 206
Obtention/définition des paramètres de configuration LAN 206
Commandes IPMI OEM 218

Chapitre 13. Serveurs Edge 229
Mode de verrouillage du système 229
Gestionnaire de clé d'authentification (AK) SED . . 230
Réseaux Edge 230

Annexe A. Service d'aide et d'assistance 233
Avant d'appeler 233
Collecte des données de maintenance 234
Contact du support 235

Annexe B. Consignes 237
Marques 238
Remarques importantes 238
Contamination particulaire 239
Déclaration réglementaire relative aux télécommunications 239
Déclarations de compatibilité électromagnétique 240
Déclaration BSMI RoHS pour Taïwan 241
Informations de contact pour l'importation et l'exportation de Taïwan 241

Index 243

Chapitre 1. Introduction

Lenovo XClarity Controller 2 (XCC2) est un contrôleur de gestion nouvelle génération qui remplace le contrôleur de gestion de la carte mère (BMC) pour les serveurs Lenovo ThinkSystem.

Il s'agit de la troisième génération de processeur de maintenance Integrated Management Module II (IMM2) qui regroupe la fonctionnalité de processeur de maintenance, ainsi que les fonctionnalité de contrôleur Super I/O, de contrôleur vidéo et de présence à distance dans une seule puce située 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.

  Remarque : XClarity Controller prend en charge actuellement la spécification d'API Redfish Scalable Platforms Management 1.0.2 et le schéma 2016.2.

Remarques :

- 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.
- Pour les serveurs Flex, le module Chassis Management Module (CMM) constitue le module de gestion principal pour les fonctions de gestion des systèmes. XClarity Controller est accessible via le port réseau sur le module CMM.

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 à Support Portal, 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 **Manage my product lists**. 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 chargée, 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 Platinum de XClarity Controller

XClarity Controller se décline dans plusieurs niveaux de fonctionnalités : standard et Platinum. 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

Remarque : Certaine fonctions peuvent ne pas s'appliquer aux serveurs Flex System.

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

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
- Interface de ligne de commande existante
- 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
- E-mail
- Événements 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
- 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

- Détection de groupes voisins
- 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 Platinum de XClarity Controller

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

Toutes les fonctionnalités de niveau standard de XClarity Controller, plus :

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 IO/IMG de client local
- Contrôle qualité/bande passante
- Collaboration de console virtuelle (6 utilisateurs)
- Dialogue de console virtuelle
- Enregistrement/relecture de vidéo
- Montage de supports virtuels de fichiers ISO/IMG distants HTTP, Samba et NFS
- Client Java de console distante

Redirection série

- Redirection série via Telnet/SSH

Sécurité

- Authentification unique
- Security Key Lifecycle Manager (SKLM)
- 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
- Compteurs d'alimentation historiques
- Graphiques de température

Déploiement et configuration

- Déploiement du SE distant

Mises à jour du microprogramme

- Synchronisation avec le référentiel
- Mise à jour automatique
- Mise à jour de lot du microprogramme
- Restauration du microprogramme depuis le référentiel local dans une carte MicroSD

Autres fonctions de gestion

- Gestion de groupe voisin

Mise à niveau de XClarity Controller

Si votre serveur a été fourni avec le niveau de base ou 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 8 « Gestion des licences » à la page 105.

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 48.0 ou supérieur (55.0 ou supérieur pour console distante)
- Firefox ESR 38.6.0 ou supérieur
- Microsoft Edge
- Safari 9.0.2 ou supérieur (iOS 7 ou supérieur et système d'exploitation X)

Remarque : La prise en charge de la fonction de 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 :

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-ECDSA-AES256-SHA
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES128-SHA
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256

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 interruptions 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. Pour accéder à XClarity Controller à distance à l'aide de l'interface Web de XClarity Controller, vous devez d'abord vous connecter. 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.

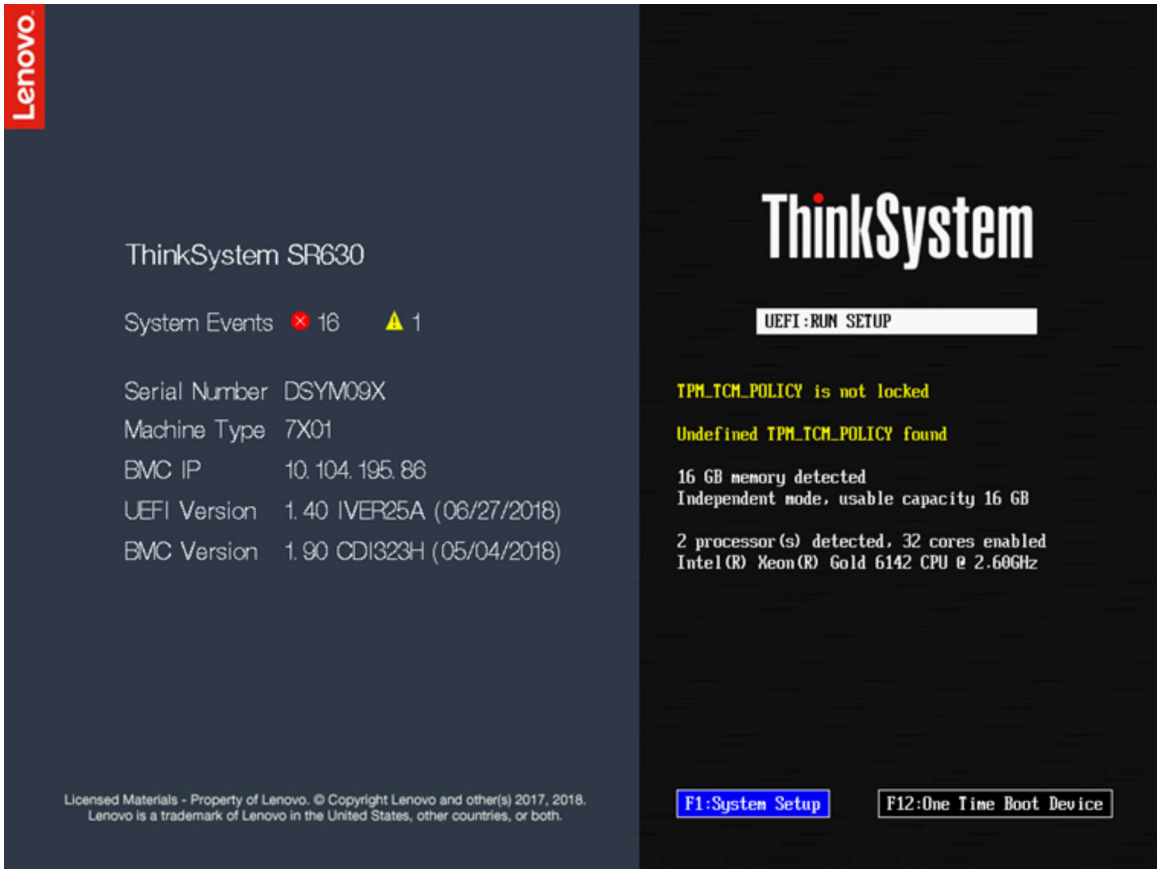
Configuration de la connexion réseau de XClarity Controller via XClarity Provisioning Manager

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.



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.

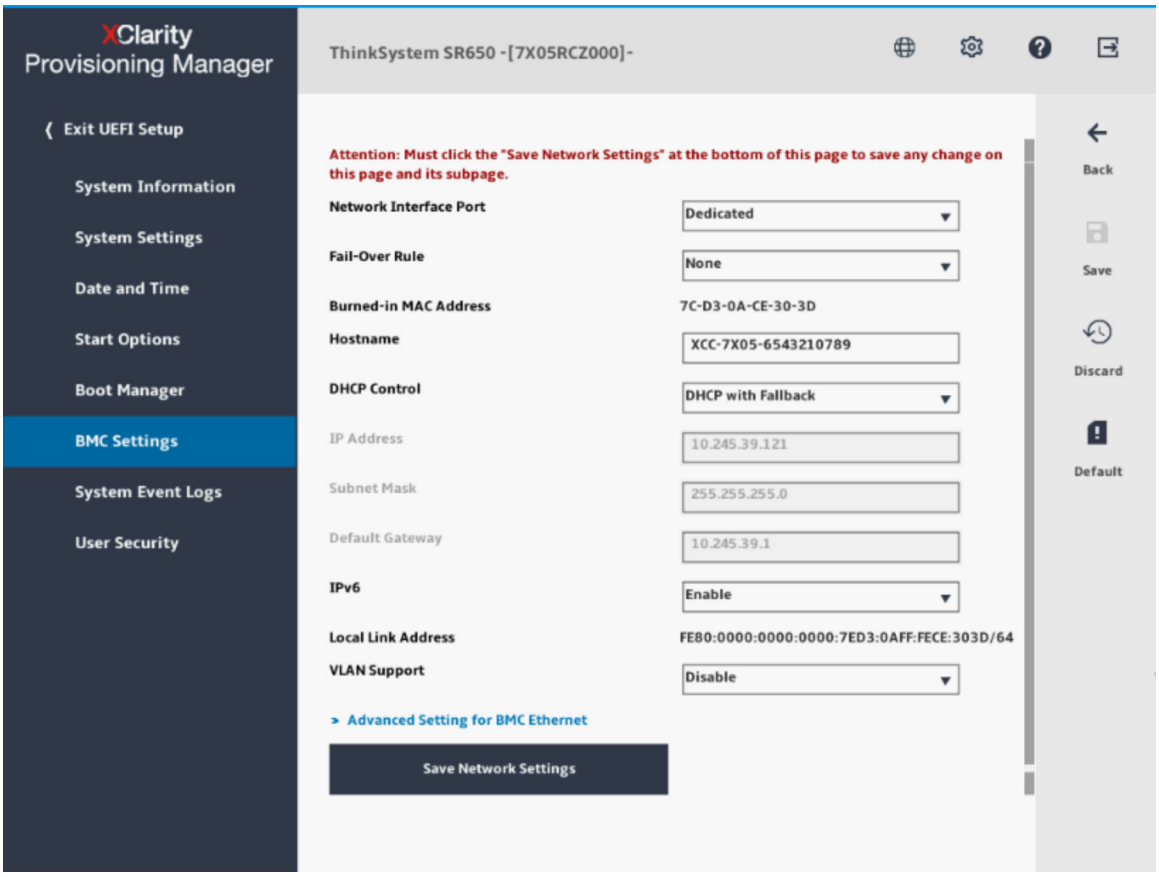
Etape 3. Depuis le menu principal de XClarity Provisioning Manager, sélectionnez **UEFI Setup**.

Etape 4. À l'écran suivant, sélectionnez **BMC Settings**, puis cliquez sur **Network Settings**.

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

- Static IP
- DHCP Enabled

- DHCP with Fallback



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 *shared* est la seule option XClarity Controller disponible. Depuis l'écran **Network Configuration**, sélectionnez **Dedicated**, le cas échéant, ou **Shared** dans la zone **Network Interface Port**.
- 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, en puis 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.

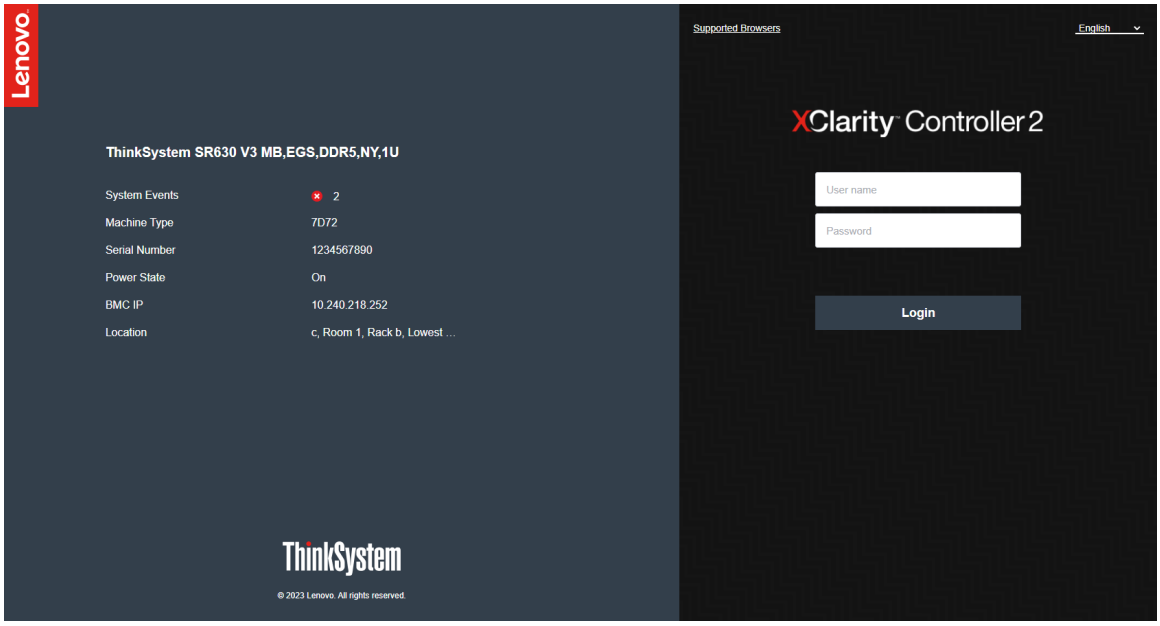
Remarque : Dans Flex System, les comptes utilisateur XClarity Controller peuvent être gérés par un module Chassis Management Module (CMM) Flex System et ils peuvent différer de la combinaison USERID/ PASSW0RD décrite ci-dessus.

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

Etape 1. Ouvrez un navigateur Web. Dans la zone d'adresse ou d'URL, entrez l'adresse IP ou le nom d'hôte de XClarity Controller auquel vous souhaitez vous connecter.

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

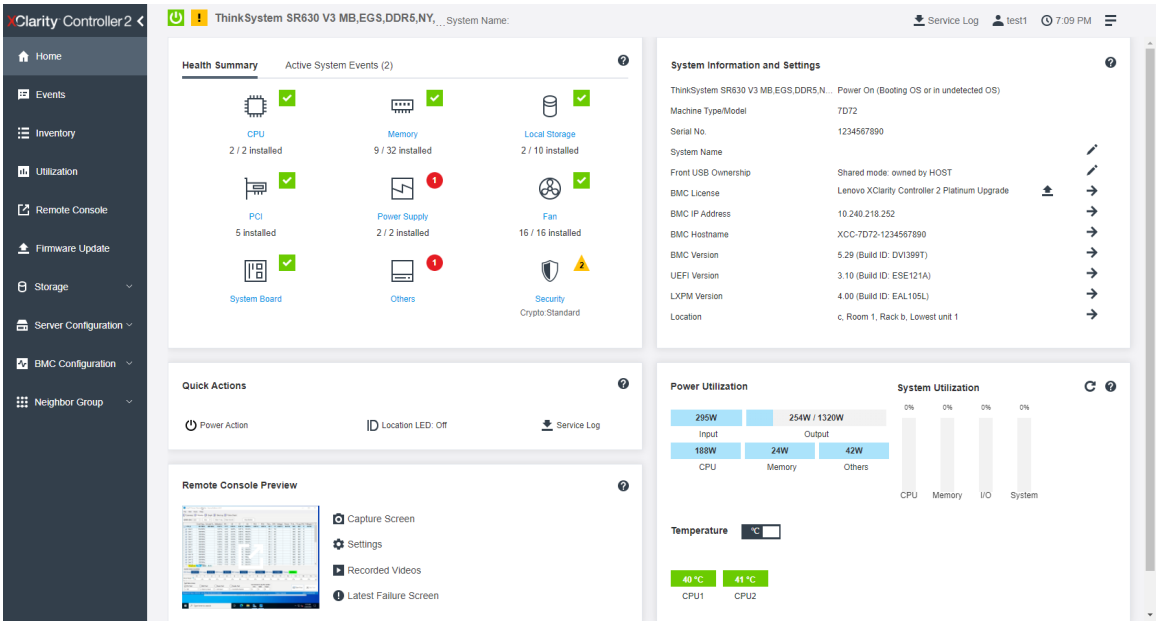
L'image suivante représente la fenêtre de connexion.



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 et le nombre d'avertissements actuellement présents sur le système.



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

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.

Tableau 1. Fonctions de XClarity Controller

Tableau de trois colonnes contant les descriptions des actions pouvant être réalisées depuis l'interface Web de XClarity Controller.

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.

Tableau 1. Fonctions de XClarity Controller (suite)

Tab	Sélection	Description
	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/ Utilisation du système/ Température	Fournit une présentation rapide de l'utilisation électrique actuelle, de l'utilisation du système et de la température globale du serveur.
	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. La barre d'outils de droite inclut les actions rapides suivantes : • Capture d'écran • Paramètres • Vidéos enregistrées • Dernier écran de défaillance en date
Événements	Journal des événements	Fournit une liste historique de l'ensemble des événements de gestion et concernant le matériel.
	Journal d'audit	Fournit un enregistrement historique des actions utilisateur, comme la connexion à Lenovo 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 et les contrôles dans les systèmes informatiques.
	Historique de maintenance	Affiche l'historique relatif aux mises à jour de microprogramme, à la configuration et au remplacement du matériel.
	Destinataires d'alertes	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 SMM2 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, l'utilisation du sous-système de système et les informations relatives à la vitesse du ventilateur du serveur et ses composants, sous forme graphique ou tabulaire.
Stockage	Détails	Affiche la structure physique et la configuration de stockage des périphériques de stockage
	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.

Tableau 1. Fonctions de XClarity Controller (suite)

Tab	Sélection	Description
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 apparaît comme une unité de disque USB reliée 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.
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 SMM2 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. • Permet de gérer les dépassements de délai de démarrage afin de détecter et de récupérer à la suite d'un blocage. • 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.
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.

Tableau 1. Fonctions de XClarity Controller (suite)

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	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 **Autoriser les connexions de** pour définir la façon dont les tentatives de connexion utilisateur sont authentifiées. 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, 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

Pour créer un nouveau compte utilisateur, cliquez sur **Créer**.

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, 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, sélectionnez la case à cocher en regard de **Paramètres SNMPv3**. 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.

Adresse pour les interruptions
Spécifiez la destination des interruptions pour l'utilisateur. Il peut s'agir d'une adresse IP ou d'un nom d'hôte. En utilisant des interruptions, l'agent SNMP avertit la station de gestion des événements survenus (par exemple, lorsque la température d'un processeur dépasse la limite prescrite).

Protocole d'authentication
Seul le protocole d'authentification **HMAC-SHA** est pris en charge. Cet algorithme est utilisé par le modèle de sécurité SNMPv3 pour l'authentification.

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 prises en charge sont **CBC-DES** et **AES**.

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

- Si le mot de passe est défini sur « *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 comme suit : « *111111111* » (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 suit : « *bertbertbert* ». Les deux mots de passe sont considérés comme ayant la même clé.

Pour plus de détails, reportez-vous à la page 72 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, sélectionnez la case à cocher en regard de **Clé SSH**. 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 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.

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 **Security Password Manager** pour activer ou désactiver la fonction de mot de passe 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 tiers* 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 tiers*, cliquez sur **Utilisateur/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 tiers et les zones **Mot de passe** et **Confirmer mot de passe** ont été grisées.
- Si le mot de passe 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 fonction

```
$ 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 fonction

  ```
  > 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 le mot de passe crypté a été configuré, rappelez-vous de pas utiliser ce dernier pour vous connecter au 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.

Remarques : Sur un système Flex, les paramètres de la stratégie de sécurité de compte sont gérés par le Flex System Chassis Management Module (CMM) et ne peuvent pas être modifiés via XCC. Lorsque le CMM est utilisé pour configurer la stratégie de sécurité du compte, veuillez noter les éléments suivants :

- Contrairement au XCC, le module CMM ne dispose pas du paramètre *période d'avertissement d'expiration du mot de passe (en jours)*. Lorsque la *période d'expiration du mot de passe* est configurée pour plus de 5 jours dans le module CMM, le XCC définit la période d'avertissement d'expiration du mot de passe comme étant 5 jours. En revanche, si le paramètre est inférieur à 5 jours, la période d'avertissement d'expiration du mot de passe sera la même que la valeur entrée dans la *période d'expiration du mot de passe*.
- Pour le paramètre du *nombre maximal d'échecs de connexion (en heures)*, la plage définie dans le module CMM est de 0-100 fois. Toutefois, la plage définie dans le XCC est de 0-10 fois. Ainsi, lorsque l'utilisateur active une valeur supérieure à 10 fois dans le module CMM, le XCC définira toujours le nombre maximal d'échecs de connexion comme 10 fois.
- Pour le paramètre d'*intervalle de modification du mot de passe minimal (en heures)*, la plage définie dans le module CMM est de 0-1440 heures. Toutefois, la plage définie dans le XCC est de 0-240 heures. Ainsi, lorsque l'utilisateur sélectionne une valeur supérieure à 240 heures dans le module CMM, le XCC définira toujours l'intervalle de modification du mot de passe minimal à 240 heures.

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 32 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 32 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 de mot de passe minimum
Cette zone contient la longueur minimale du mot de passe.

Cycle de réutilisation du mot de passe minimum
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 Server)
- Microsoft Lightweight Directory Service (Windows 2008, Windows 2012)
- Serveur Novell eDirectory, version 8.7, 8.8 et 9.4
- Serveur OpenLDAP 2.1, 2.2, 2.3 et 2.4

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 utilisateur à l'aide de la chaîne IBMRBSPermissions. 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 de groupe et les privilèges peuvent être configurés dans la section Paramètres d'Active Directory.
   - **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 quatre serveurs LDAP en entrant l'adresse IP ou le nom d'hôte de chaque serveur IP si 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, cliquez sur la case à cocher **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 42.
2. Renseignez les information sous **Paramètres supplémentaires**. Les paramètres sont décrits ci-dessous.

   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 :

   - **Aucunes données d'identification requises**

     Utilisez cette méthode pour effectuer une liaison sans nom distinctif ou mot de passe. Cette méthode est fortement déconseillée car la plupart des serveurs sont configurés de sorte à ne pas autoriser les demandes de recherche sur des enregistrements d'utilisateurs spécifiques.
   - **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 n'est effectuée que lorsque les méthodes de liaison **Aucune donnée d'identification requise** ou **Utiliser des données d'identification configurées** sont utilisées.

Nom distinctif 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 UID

Lorsque la méthode de liaison est définie sur **Aucune donnée d'identification requise** ou **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 d'attribut est normalement **sAMAccountName**. Sur les serveurs Novell eDirectory et OpenLDAP, le nom d'attribut est **uid**. Si cette zone est laissée vide, la valeur par défaut est **uid**.

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.

L'appartenance à un groupe imbriqué est prise en charge uniquement dans les environnements Active Directory. Par exemple, si un utilisateur est membre de GroupA et GroupB, et que GroupA est également membre de GroupC, l'utilisateur est considéré comme étant également membre de GroupC. Les recherches imbriquées s'arrêtent lorsque 128 groupes ont été recherchés. Les groupes d'un niveau sont recherchés avant les groupes appartenant à un niveau inférieur. Les boucles ne sont pas détectées.

Attribut de recherche de groupe

Dans un environnement Active Directory ou Novell eDirectory, la zone **Attribut de recherche de groupe** spécifie le nom d'attribut utilisé pour identifier les groupes auxquels un utilisateur appartient. Dans un environnement Active Directory, le nom d'attribut est **memberOf**. Dans un environnement eDirectory, le nom d'attribut est **groupMembership**. Dans un environnement de serveur OpenLDAP, les utilisateurs sont généralement affectés aux groupes pour lesquels objectClass correspond 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. La zone **Attribut d'autorisation de connexion** indique le nom de l'attribut. Si cette zone est laissée vide, l'utilisateur obtient les droits de lecture seule par défaut, dans la mesure où l'authentification de groupe et d'utilisateur a réussi.

La valeur d'attribut renvoyée par le serveur LDAP recherche la chaîne de mot clé IBMRBSPermissions=. Cette chaîne de mot clé doit être immédiatement suivie d'une chaîne de bits correspondant à 12 occurrences consécutives du chiffre 0 ou du chiffre 1. Chaque bit représente un ensemble de fonctions. Les bits sont numérotés selon leur position. Le bit le plus à gauche correspond à la position de bit 0 et le bit le plus à droite à la position de bit 11. La valeur 1 placé à une position de bit particulière active la fonction qui est 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 IBMRBSPermissions=010000000000 est un exemple valide. Le mot clé IBMRBSPermissions= est utilisé pour être placé à n'importe quel endroit dans cette zone. Ceci permet à l'administrateur LDAP de réutiliser un attribut existant, évitant ainsi une extension du schéma LDAP. Cela permet également d'utiliser l'attribut pour sa fonction initiale. Vous pouvez ajouter la chaîne de mot clé n'importe où dans cette zone. 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 2. Bits d'autorisation

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

Tableau 2. Bits d'autorisation (suite)

Position de bit	Fonction	Explication
0	Refuser toujours	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	Réseaux et sécurité	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 de l'adaptateur	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.

Tableau 2. Bits d'autorisation (suite)

Position de bit	Fonction	Explication
10	Configuration avancée de l'adaptateur	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 XClarity Controller, modification et restauration de la configuration de l'adaptateur depuis un fichier de configuration et redémarrage/réinitialisation de XClarity Controller.
11	Réservé	Cette position de bit est réservée pour un usage ultérieur. Si aucun bit n'est défini, l'utilisateur obtient les droits de lecture seule. Le système donne la priorité aux droits de connexion récupérés directement de l'enregistrement utilisateur. Si l'attribut d'autorisation de connexion ne figure pas dans l'enregistrement utilisateur, le système tente de récupérer les droits des groupes auxquels l'utilisateur appartient. Ceci fait partie de la phase d'authentification de groupe. L'utilisateur reçoit l'opérateur inclusif OR de tous les bits pour tous les groupes. Le bit Accès en lecture seule (position 2) est uniquement défini si tous les autres bits sont définis sur zéro. Si le bit Refuser toujours (position 0) est défini pour l'un des groupes, l'accès est refusé à l'utilisateur. Le bit Refuser toujours (position 0) prévaut toujours sur les autres.

Si aucun des bits n'est défini, la valeur par défaut est définie sur **Lecture seule** pour l'utilisateur.

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 **Refuser toujours** est défini pour l'un des groupes, l'accès sera refusé à l'utilisateur. Le bit **Refuser toujours** a toujours priorité sur les autres bits.

Remarque : 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. Indiquez s'il est nécessaire ou non d'**Activer la sécurité étendue basée sur les rôles pour les utilisateurs Active Directory** sous **Paramètres d'Active Directory** (si le mode **Utiliser le serveur LDAP pour l'authentification et l'autorisation** est utilisé), ou configurez les **Groupes pour autorisation locale :** (si le mode **Utiliser le serveur LDAP pour l'authentification uniquement** (**avec autorisation locale**) est utilisé).
   - **Activer la sécurité étendue basée sur les rôles pour les utilisateurs Active Directory :**

     Si le paramètre de sécurité étendue basée sur les rôles est activé, un nom de serveur au format libre doit être configuré pour agir en tant que nom cible pour ce XClarity Controller en particulier. Le nom cible peut être associé à un ou plusieurs rôles sur le serveur Active Directory via un composant logiciel enfichable RBS (Role Based Security). Cette opération peut être effectuée en créant des cibles gérées et en leur attribuant des noms spécifiques, puis en les associant aux rôles appropriés.

Si un nom est configuré dans ce champ, il octroie l'autorisation de définir des rôles spécifiques pour les utilisateurs et contrôleurs XClarity Controller (cibles) membres du même rôle. Lorsqu'un utilisateur se connecte à XClarity Controller et est authentifié via Active Directory, les rôles dont l'utilisateur est membre sont extraits de l'annuaire. Les autorisations qui sont attribuées à l'utilisateur sont extraites des rôles ayant également en tant que membre une cible dont le nom de serveur correspond à celui configuré ici, ou à une cible correspondant à XClarity Controller. Plusieurs XClarity Controller peuvent avoir le même nom cible. Ceci peut être utilisé, par exemple, pour regrouper plusieurs XClarity Controller et les affecter au(x) même(s) rôle(s) en utilisant une cible gérée unique (identifiée via un nom de cible unique). Inversement, chaque XClarity Controller peut avoir un nom unique.

- **Groupes pour autorisation locale**

  Les noms de groupe sont configurés afin de fournir des spécifications d'autorisation locale pour des groupes d'utilisateurs. Des droits (rôles) peuvent être affectés à chaque nom de groupe, qui sont identiques à ceux décrits dans le tableau ci-dessous. Le serveur LDAP associe les utilisateurs avec un nom de groupe. Lorsque l'utilisateur se connecte, les droits qui lui sont affectés sont associés au groupe auquel appartient l'utilisateur. Des groupes supplémentaires peuvent être configurés en cliquant sur l'icône « + » ou supprimés en cliquant sur l'icône « x ».

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 **désactivé**, 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 USBLAN ou 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**, entrez 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.

Remarque : Sur un système Flex System, les paramètres VLAN sont gérés par un module CMM Flex System et ne peuvent pas être modifiés dans XClarity Controller.

Pour activer le marquage VLAN (LAN virtuel), sélectionnez la case à cocher **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 **Sélection MAC**, sélectionnez l'une des options 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 `000000000000` 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 **Unité de transmission maximale**, spécifiez l'unité de transmission maximale d'un paquet (en octets) pour votre interface réseau. La plage des unités de transmission maximale va de 60 à 1500. La valeur par défaut de cette zone est 1500.

Pour utiliser une connexion Ethernet IPv6, procédez comme suit :

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 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.

Remarque : Sur un système Flex System, les paramètres DNS ne peuvent pas être modifiés sur XClarity Controller. Les paramètres DNS sont gérés par le module CMM.

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

Si vous cliquez sur la case à cocher **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.

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.

Cliquez sur la case à cocher **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. Cliquez sur la case à cocher 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 flashage de Linux ou Windows.

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*
- **Utiliser l'adresse IPv4 de type lien local pour Ethernet via USB** : Une adresse IP de la plage 169.254.0.0/16 est affectée à XClarity Controller et côté serveur du réseau.
- **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 :

1. 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.
2. 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.

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 **Interruption SNMPv1**, **Interruption SNMPv2** et/ou **Interruption SNMPv3**.
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 **Interruption SNMPv3** est activé, 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.

Activation ou désactivation de l'accès réseau IPMI

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

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

IMPI sur accès LAN
Cliquez sur le commutateur pour activer ou désactiver l'accès réseau IPMI à XClarity Controller.

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 :

Web
Le numéro de port est 80. Cette zone n'est pas configurable par l'utilisateur.

Web via HTTPS
Dans cette zone, spécifiez le numéro de port pour Web via HTTPS. La valeur par défaut est 443.

REST via HTTPS
Le numéro de port change automatiquement en celui indiqué dans la zone Web via HTTPS. Cette zone n'est pas configurable par l'utilisateur.

Présence à distance
Dans cette zone, spécifiez le numéro de port pour Présence à distance. La valeur par défaut est 3900.

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

Remarque : IPMI est désactivé par défaut.

SFTP
Dans cette zone, spécifiez le numéro de port utilisé pour le protocole SFTP (SSH File Transfer Protocol). Le numéro de port est 115. Cette zone n’est pas configurable par l’utilisateur.

Remarque : IMM.SFTPPortControl=open est requis pour les mises à jour OneCLI internes.

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.

Interruptions SNMP
Dans cette zone, spécifiez le numéro de port utilisé pour les interruptions SNMP. La valeur par défaut est 162. Les valeurs de numéro de port valides sont comprises entre 1 et 65535.

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.

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

Cliquez sur **Réseau** sous **Configuration BMC** pour afficher ou modifier les paramètres du gestion du port USB de panneau frontal XClarity Controller.

Vous avez le choix entre quatre types de paramètres :

Mode hôte uniquement
Le port USB du panneau frontal est toujours connecté uniquement au serveur.

Mode BMC uniquement
Le port USB du panneau frontal est toujours connecté uniquement à XClarity Controller.

Mode partagé : appartenant à BMC
Le port USB du panneau frontal est partagé par le serveur et XClarity Controller, mais le port est commuté sur XClarity Controller.

Mode partagé : appartenant à l'hôte
Le port USB du panneau frontal est partagé par le serveur et XClarity Controller, mais le port est commuté sur l'hôte.

Pour plus d'informations sur l'application mobile, consultez le site suivant :

http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/lxca_usemobileapp.html

Remarques :

- Si le port USB du panneau frontal est configuré pour le mode partagé, le port est connecté à XClarity Controller lorsqu'il n'existe pas d'alimentation, et il est connecté au serveur s'il existe une alimentation. S'il y a une alimentation, le contrôle du port USB du panneau frontal peut être commuté dans les deux sens entre le serveur et XClarity Controller. En mode partagé, le port peut également être commuté entre le serveur et XClarity Controller en maintenant le bouton d'identification du panneau frontal enfoncé (pour les nœuds de traitement, il peut s'agir du bouton de gestion USB) pendant plus de 3 secondes.
- Lorsqu'il est configuré en mode partagé et que le port USB est actuellement connecté au serveur, XClarity Controller peut prendre en charge une demande de basculer le port USB du panneau frontal sur XClarity Controller. Lorsque cette demande est exécutée, le port USB du panneau frontal reste connecté à XClarity Controller jusqu'à ce qu'il n'existe aucune activité USB au niveau de XClarity Controller pendant la période indiquée par le délai d'inactivité.

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 173.

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, l'intrusion du 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 Détail 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 V3.

La licence XCC Platinum est dotée d'un troisième mode de sécurité : le mode Enterprise Strict. Ce mode convient plus particulièrement aux exigences de sécurité de haut niveau.

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 Enterprise Strict.
- Le BMC fonctionne en mode standard validé.
- Nécessite des certificats de niveau Enterprise Strict.
- Seuls les services qui prennent en charge le chiffrement de niveau Enterprise Strict sont autorisés.
- 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 chiffrement utilisés par BMC sont compatibles avec la norme standard.
- Le BMC fonctionne en mode standard validé.
- Nécessite des certificats de niveau standard.
- Les services nécessitant un chiffrement ne prennent pas en charge le chiffrement de niveau Enterprise Strict, lequel est désactivé par défaut.

Mode de sécurité 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 cryptographie est prise en charge.
- Lorsque ce mode est activé, BMC ne FONCTIONNE PAS en mode standard validé.
- Permet d'activer tous les services.

Matrice de service dans les trois modes de sécurité :

Fonctionnalité/service	**Utilise le chiffrement**	**État par défaut** **Préconfiguration**	**Prise en charge** **Mode strict**	**Prise en charge** **Mode standard**	**Prise en charge** **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 configuré	Non	Oui Si activé, il permet 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

Fonctionnalité/service	Utilise le chiffrement	État par défaut Préconfiguration	Prise en charge Mode strict	Prise en charge Mode standard	Prise en charge Mode compatibilité
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 configurée	Oui	Oui	Oui
Console distante	Oui	Activée	Oui	Oui	Oui
Support virtuel - CIFS	Oui	Non configuré	Non	Oui	Oui
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 configurée	Non	Oui	Oui

Fonctionnalité/service	Utilise le chiffrement	État par défaut Préconfiguration	Prise en charge Mode strict	Prise en charge Mode standard	Prise en charge Mode compatibilité
Mise à jour à partir du référentiel - NFS	Non	Non configurée	Non	Oui	Oui
Mise à jour à partir du référentiel - HTTP	Non	Non configurée	Non	Oui	Oui
Mise à jour à partir du référentiel - HTTPS	Oui	Non configurée	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.

Vous pouvez utiliser SSL avec un certificat autosigné ou un certificat signé par une autorité de certification tierce. Le certificat d'auto-signature représente la méthode la plus simple pour utiliser SSL mais il soulève un risque de sécurité mineur. Car le client SSL n'a aucun moyen de valider l'identité du serveur SSL lors de la première tentative de connexion entre le client et le serveur. En effet, un tiers peut usurper l'identité du serveur Web de XClarity Controller pour intercepter les données échangées entre le serveur Web de XClarity Controller actuel et le navigateur Web de l'utilisateur. 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).

Pour une sécurité accrue, vous pouvez utiliser un certificat signé par une autorité de certification (CA). Pour obtenir un certificat signé, vous devez sélectionner **Générer une demande de signature de certificat (CSR)**. Sélectionnez **Télécharger une demande de signature de certificat (CSR)** et envoyez une demande de signature de certificat à une autorité de certification afin d'obtenir un certificat signé. Une fois le certificat signé reçu, sélectionnez **Importer un certificat signé** pour l'importer dans XClarity Controller.

La fonction de l'autorité de certification est de vérifier l'identité de XClarity Controller. Le certificat contient les signatures numériques de l'autorité de certification et de XClarity Controller. Si une autorité de certification connue émet le certificat ou si le certificat de l'autorité de certification a déjà été importé dans le navigateur Web, le navigateur peut valider le certificat et identifier de manière catégorique le serveur Web de XClarity Controller.

XClarity Controller requiert un certificat pour son utilisation avec le serveur HTTPS, CIM via HTTPS et le client LDAP sécurisé. De même, le client LDAP sécurisé a besoin d'importer un ou plusieurs certificats sécurisés. Le certificat sécurisé est utilisé par le client LDAP sécurisé pour identifier de manière catégorique le serveur LDAP. Le certificat sécurisé est le certificat de l'autorité de certification qui a signé le certificat du serveur LDAP. Si le serveur LDAP utilise des certificats autosignés, le certificat sécurisé peut être le certificat du serveur LDAP lui-même. Des certificats sécurisés supplémentaires doivent être importés si vous utilisez plusieurs serveurs LDAP dans votre configuration.

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 visualisé avec un outil tiers comme OpenSSL (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 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 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 de nouveau une clé**.
- Une fois l'action terminée, redémarrez XClarity Controller pour que vos modifications prennent effet.

IMPI sur accès KCS à XClarity Controller

Les informations de cette rubrique vous indiquent comment contrôler IMPI sur accès KCS à XClarity Controller.

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

Cliquez **Security** sous **BMC Configuration** pour activer ou désactiver IMPI sur accès KCS.

Remarque : Une fois les paramètres modifiés, vous devez redémarrer XClarity Controller pour que vos modifications prennent effet.

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 IMPI sur accès KCS pour une sécurité accrue. XClarity Essentials utilise l'interface IPMI via KCS avec XClarity Controller. Si vous avez désactivé l'interface IPMI via KCS, réactivez-la avant d'exécuter XClarity Essentials sur le serveur. Ensuite, désactivez l'interface lorsque vous avez terminé.

Enveloppement du journal IPMI SEL

Les informations de cette rubrique vous permettent de configurer le journal IPMI SEL.

XClarity Controller propose une option d'enveloppement de journal IPMI SEL.

Cliquez sur le commutateur du coin supérieur droit pour activer ou désactiver l'enveloppement du journal IPMI SEL.

Cette fonctionnalité rend possible l'enregistrement circulaire du journal IPMI SEL. Le nouvel enregistrement SEL est toujours annexé, tandis que le plus ancien est abandonné dès lors que le journal IPMI SEL est complet.

Remarque : L'application de ce paramètre entraîne le réamorçage du BMC.

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 éviter le passage du microprogramme du système à un niveau plus ancien.

Pour activer ou désactiver cette fonction, cliquez sur **Réseau** sous **Configuration BMC**. 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).

XClarity Controller utilise le réseau pour récupérer les clés de chiffrement du serveur de gestion de clé ; le serveur de gestion de clé doit être accessible à XClarity Controller. XClarity Controller fournit le canal de communication entre le serveur de gestion de clé et le serveur ThinkSystem qui présente la demande. Le microprogramme XClarity Controller essaie de se connecter avec chaque serveur de gestion de clé configuré, et il s'arrête lorsqu'une connexion est établie.

XClarity Controller établit la communication avec le serveur de gestion de clé si les conditions suivantes sont remplies :

- Un ou plusieurs noms d'hôte/adresses IP de serveur de gestion de clé sont configurés dans XClarity Controller.
- Deux certificats (client et serveur) pour communiquer avec le serveur de gestion de clé sont installés dans XClarity Controller.

Remarque : Configurez au moins deux serveurs de gestion de clé (primaire et secondaire) avec le même protocole pour votre appareil. Si le serveur de gestion de clé ne réagit pas à la tentative connexion de

XClarity Controller, des tentatives de connexion sont initiées avec les serveurs de gestion de clé supplémentaires jusqu'à ce qu'une connexion soit établie.

Une connexion TLS (Transport Layer Security) doit être établie entre XClarity Controller et le serveur de gestion de clé. XClarity Controller authentifie le serveur de gestion de clé en comparant le certificat serveur soumis par le serveur de gestion de clé au certificat serveur de gestion de clé préalablement importé dans le fichier de clés certifiées XClarity Controller. Le serveur de gestion de clé authentifie chaque XClarity Controller qui communique avec lui et vérifie que XClarity Controller est autorisé à accéder au serveur de gestion de clé. Cette authentification est effectuée en comparant le certificat client soumis par XClarity Controller à la liste des certificats sécurisés qui sont stockés sur le serveur de gestion de clé.

Au moins un serveur de gestion de clé (serveur référentiel principal) est connecté, et le groupe d'appareils est considéré comme étant facultatif. Le certificat du serveur de gestion de clé doit être importé, tandis que le certificat client doit être spécifié. Par défaut, le certificat HTTPS est utilisé. Si vous souhaitez le remplacez, vous pouvez en générer un nouveau.

Remarque : Pour connecter le serveur KMIP (KeySecure et CipherTrust), il doit générer une demande de signature de certificat (CSR), et son nom commun doit être mis en correspondance avec le nom d'utilisateur défini sur le serveur, puis importer un certificat qui a été signé par l'autorité de certification (CA) digne de confiance par le serveur KMIP pour le CSR.

Configuration des serveurs de gestion de clé

Les informations de cette rubrique vous permettent de créer le nom d'hôte ou l'adresse IP ainsi que les informations de port associées pour le serveur de gestion de clé.

La section configuration du/des serveur(s) de gestion de clé se compose des zones suivantes :

Nom d'hôte ou adresse IP
Entrez le nom d'hôte (si DNS est activé et configuré) ou l'adresse IP du serveur de gestion de clé dans cette zone. Jusqu'à quatre serveurs peuvent être ajoutés.

Port
Entrez le numéro de port du serveur de gestion de clé dans cette zone. Si cette zone est laissée vide, la valeur par défaut 5696 est utilisée. Les valeurs valides pour le numéro de port sont comprises entre 1 et 65535.

Configuration du groupe d'appareils

Les informations de cette rubrique vous permettent de configurer le groupe de périphériques utilisé sur le serveur SKLM.

Dans le serveur SKLM, un groupe d'appareils permet aux utilisateurs de gérer les clés (SED) sur plusieurs serveurs en tant que groupe. Un groupe d'appareils avec le même nom doit également être créé sur le serveur SKLM.

La section Groupe d'appareils contient la zone suivante :

Groupe d'appareils
Un groupe d'appareils permet aux utilisateurs de gérer les clés pour les unités SED sur plusieurs serveurs en tant que groupe. Un groupe d'appareils avec le même nom doit également être créé sur le serveur SKLM. La valeur par défaut de cette zone est IBM_SYSTEM_X_SED.

Établissement de la gestion des certificats

Cette rubrique fournit des informations sur la gestion du certificat du client et du serveur.

Les certificats du client et du serveur sont utilisés pour authentifier la communication entre le serveur SKLM et le serveur XClarity Controller situés sur le serveur ThinkSystem. La gestion du certificat du serveur et du client est décrite dans cette section.

Gestion des certificats du client

Cette rubrique fournit des informations sur la gestion des certificats du client.

La classification des certificats du client s'effectue comme suit :

- Certificat affecté automatiquement par XClarity Controller.
- Certificat généré à partir d'une demande de signature de certificat XClarity Controller et signé (en externe) par une autorité de certification tierce.

Un certificat client est requis pour communiquer avec le serveur SKLM. Le certificat client contient les signatures numériques de l'autorité de certification et de XClarity Controller.

Remarques :

- Les certificats sont conservés dans les mises à jour du microprogramme.
- Si un certificat client n'est pas créé pour communiquer avec le serveur SKLM, le certificat du serveur HTTPS de XClarity Controller est utilisé.
- La fonction de l'autorité de certification est de vérifier l'identité de XClarity Controller.

Pour créer un certificat client, cliquez sur l'icône plus ( ) et sélectionnez l'un des éléments suivants :

- Générer une nouvelle clé et un certificat auto-signé
- Générer une nouvelle clé et une demande de signature de certificat (CSR)

L'élément d'action **Générer une nouvelle clé et un certificat auto-signé** génère une nouvelle clé de chiffrement et un certificat autosigné. Dans la fenêtre Générer une nouvelle clé et un certificat auto-signé, entrez ou sélectionnez les informations dans les zones requises et les zones facultatives qui s'appliquent à votre configuration (voir le tableau ci-après). Cliquez sur **OK** pour générer votre clé de chiffrement et le certificat. Une fenêtre de progression s'affiche pendant la génération du certificat autosigné. Une fenêtre de confirmation s'affiche une fois le certificat correctement installé.

Remarque : La nouvelle clé de chiffrement et le certificat remplacent la clé et le certificat existants.

Tableau 3. Générer une nouvelle clé et un certificat auto-signé

Tableau, à deux colonnes et des en-têtes, qui décrit les zones obligatoires et facultatives pour l'action Générer une nouvelle clé et un certificat auto-signé. La ligne du bas s'étend sur les deux colonnes.

Zone	Description
Pays[1]	Dans l'élément de liste, sélectionnez le pays de résidence physique du contrôleur BMC.
État ou province[1]	Entrez l'état ou la province de résidence du contrôleur BMC.
Ville ou localité[1]	Entrez la ville ou la localité de résidence du contrôleur BMC.
Nom de société[1]	Entrez le nom de la société ou de l'organisation propriétaire du contrôleur BMC.
Nom d'hôte du BMC[1]	Entrez le nom d'hôte BMC qui apparaît dans la barre d'adresse Web.
Personne de contact	Entrez le nom de la personne à contacter responsable du contrôleur BMC.
Adresse e-mail	Entrez l'adresse e-mail de la personne à contacter responsable du contrôleur BMC.

Tableau 3. Générer une nouvelle clé et un certificat auto-signé (suite)

Zone	Description
Unité organisationnelle	Saisissez l'unité au sein de la société propriétaire du contrôleur BMC.
Nom de famille	Entrez le nom de la personne à contacter responsable du contrôleur BMC. Vous devez indiquer un nom de 60 caractères maximum.
Prénom	Entrez le prénom de la personne à contacter responsable du contrôleur BMC. Vous devez indiquer un nom de 60 caractères maximum.
Initiales	Entrez les initiales de la personne à contacter responsable du contrôleur BMC. Cette zone peut contenir au maximum 20 caractères.
Qualificatif DN	Entrez le nom distinctif du contrôleur BMC. Vous devez indiquer un nom de 60 caractères maximum.
1. Cette zone est obligatoire.	

Une fois le certificat du client généré, vous pouvez le télécharger dans l'espace de stockage de votre XClarity Controller en sélectionnant l'élément d'action **Télécharger le certificat**.

L'élément d'action **Générer une nouvelle clé et une demande de signature de certificat (CSR)** génère une nouvelle clé de chiffrement et une demande de signature de certificat. Dans la fenêtre Générer une nouvelle clé et une demande de signature de certificat (CSR), entrez ou sélectionnez les informations dans les zones requises et les zones facultatives qui s'appliquent à votre configuration (voir le tableau ci-après). Cliquez sur **OK** pour générer votre nouvelle clé de chiffrement et demande de signature de certificat.

Une fenêtre de progression s'affiche pendant la génération de la demande de signature de certificat et une fenêtre de confirmation s'affiche une fois l'opération terminée. Après génération de la demande de signature de certificat, vous devez envoyer cette demande à une autorité de certification pour signature numérique. Sélectionnez l'élément d'action **Télécharger une demande de signature de certificat (CSR)** et cliquez sur **OK** pour sauvegarder la demande de signature de certificat sur votre serveur. Vous pouvez ensuite soumettre la demande de signature de certificat à votre autorité de certification en vue de sa signature.

Tableau 4. Générer une nouvelle clé et une demande de signature de certificat

Tableau, comportant deux colonnes et des en-têtes, qui décrit les zones obligatoires et facultatives pour l'action Générer une nouvelle clé et une demande de signature de certificat. La ligne du bas s'étend sur les deux colonnes.

Zone	Description
Pays[1]	Dans l'élément de liste, sélectionnez le pays de résidence physique du contrôleur BMC.
État ou province[1]	Entrez l'état ou la province de résidence du contrôleur BMC.
Ville ou localité[1]	Entrez la ville ou la localité de résidence du contrôleur BMC.
Nom de société[1]	Entrez le nom de la société ou de l'organisation propriétaire du contrôleur BMC.
Nom d’hôte du BMC[1]	Entrez le nom d'hôte BMC qui apparaît dans la barre d'adresse Web.
Personne de contact	Entrez le nom de la personne à contacter responsable du contrôleur BMC.

Tableau 4. Générer une nouvelle clé et une demande de signature de certificat (suite)

Zone	Description
Adresse e-mail	Entrez l'adresse e-mail de la personne à contacter responsable du contrôleur BMC.
Unité organisationnelle	Saisissez l'unité au sein de la société propriétaire du contrôleur BMC.
Nom de famille	Entrez le nom de la personne à contacter responsable du contrôleur BMC. Vous devez indiquer un nom de 60 caractères maximum.
Prénom	Entrez le prénom de la personne à contacter responsable du contrôleur BMC. Vous devez indiquer un nom de 60 caractères maximum.
Initiales	Entrez les initiales de la personne à contacter responsable du contrôleur BMC. Cette zone peut contenir au maximum 20 caractères.
Qualificatif DN	Entrez le nom distinctif du contrôleur BMC. Vous devez indiquer un nom de 60 caractères maximum.
Mot de passe de demande d'authentification	Entrez le mot de passe de la demande de signature de certificat. Cette zone peut contenir au maximum 30 caractères.
Nom non structuré	Entrez des informations complémentaires, comme le nom non structuré affecté au module BMC. Vous devez indiquer un nom de 60 caractères maximum.
1. Cette zone est obligatoire.	

La demande de signature de certificat est signée par l'autorité de certification à l'aide de l'outil de traitement de certificat de l'utilisateur, comme l'outil de ligne de commande *OpenSSL* ou *Certutil*. Tous les certificats du client qui sont signés à l'aide de l'outil de traitement de certificat de l'utilisateur ont le même certificat de *base*. Ce certificat de *base* doit également être importé sur le serveur SKLM de sorte que tous les serveurs signés numériquement par l'utilisateur soient acceptés par le serveur SKLM.

Une fois que le certificat signé par l'autorité de certification, vous devez l'importer sur le contrôleur BMC. Sélectionnez l'élément d'action **Importer un certificat signé** et sélectionnez le fichier à télécharger sous la forme d'un certificat client ; ensuite, cliquez sur le bouton **OK**. Une fenêtre de progression s'affiche pendant le téléchargement du certificat signé par l'autorité de certification. Une fenêtre Téléchargement de certificat s'affiche si le processus de téléchargement aboutit. Une fenêtre d'erreur Téléchargement de certificat s'affiche si le processus de téléchargement échoue.

Remarques :

- Pour une sécurité accrue, utilisez un certificat qui est signé numériquement par une autorité de certification.
- Le certificat qui est importé dans XClarity Controller doit correspondre à la demande de signature de certificat préalablement générée.

Une fois qu'un certificat signé par une autorité de certification est importé sur le contrôleur BMC, sélectionnez l'élément d'action **Télécharger le certificat**. Lorsque vous sélectionnez cet élément d'action, le certificat signé par une autorité de certification est téléchargé depuis XClarity Controller pour être stocké sur votre système.

Gestion des certificats du serveur
Cette rubrique fournit des informations sur la gestion des certificats du serveur.

Le certificat de serveur est généré sur le serveur SKLM et doit être importé dans XClarity Controller pour que la fonction d'accès à l'unité sécurisé fonctionne. Pour importer le certificat qui authentifie le serveur SKLM auprès du contrôleur BMC, cliquez sur **Importation d'un certificat** dans la section Statut de certificat du serveur depuis la page d'accès de l'unité. Un indicateur de déroulement s'affiche lors du transfert du fichier dans la mémoire de XClarity Controller.

Une fois le certificat du serveur transféré vers XClarity Controller, la zone d'état de certificat du serveur affiche le contenu suivant : `A server certificate is installed.`

Pour supprimer un certificat sécurisé, cliquez sur le bouton **Retirer** correspondant.

Security password manager

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.

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 configuration matérielle différente**. 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.

Paramètres cryptographiques

Les informations de cette rubrique vous permettent de comprendre différents paramètres cryptographiques.

Mode de sécurité avancée

- Ne prend en charge que des chiffrements modernes et puissants.
- Compatible avec NIST.
- Compatible avec PFS (confidentialité persistante parfaite).

Mode compatibilité.

- Prend en charge un grand nombre de chiffrements pour une compatibilité maximale.
- Non compatible avec PFS et NIST.

Mode compatibilité NIST

- Prend en charge un grand nombre de chiffrements pour une compatibilité maximale.
- Compatible avec NIST.
- Compatible avec PFS.

Prise en charge de la version TLS

- TLS 1.0 et ultérieure
- TLS 1.1 et ultérieure
- TLS 1.2 et ultérieure
- TLS 1.3

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

Consultez le tableau suivant pour savoir si les différents paramètres d'algorithmes de cryptographie TLS sont pris en charge

Mode de sécurité	**Version TLS**	**Algorithmes de cryptographie TLS**
Mode de sécurité avancée	TLS 1.3	• TLS_AES_256_GCM_SHA384
Mode de sécurité avancée	TLS 1.2	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
Mode compatibilité NIST	TLS 1.3	• TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256

Mode de sécurité	Version TLS	Algorithmes de cryptographie TLS
Mode compatibilité NIST	TLS 1.2	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • 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 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256
Mode compatibilité	TLS 1.3	• TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256
Mode compatibilité	TLS 1.2	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • 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 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256
Mode compatibilité	TLS 1.1 TLS 1.0	• TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256

Configuration de l’appel vers Lenovo

Les informations de cette rubrique vous permettent de configurer l’appel vers Lenovo.

Vous pouvez créer un réexpéditeur de service qui envoie automatiquement les données de maintenance d'un appareil géré à Support Lenovo à l'aide de la fonction d'appel vers Lenovo.

La sécurité est extrêmement importante pour Lenovo. Lorsque cette option est activée, l'appel vers Lenovo contacte automatiquement Lenovo pour ouvrir un ticket de maintenance et envoie les données de maintenance collectées à partir d'un appareil géré chaque fois que cet appareil signale une panne matérielle. Les données de maintenance, habituellement envoyées manuellement à Support Lenovo, sont automatiquement envoyées au Centre de Support Lenovo via HTTPS à l'aide de TLS 1.2 ou d'une version ultérieure. Vos données commerciales ne sont jamais transmises. L'accès aux données de maintenance dans le Centre de Support Lenovo est limité au personnel de maintenance autorisé.

Utilisation de la page Appel vers Lenovo pour la première fois

Lorsque vous accédez la page d'appel vers Lenovo pour la première fois, une fenêtre d'avertissement s'affiche. Cliquez sur « Afficher les conditions générales » pour continuer.

Attention : vous devez accepter la **déclaration de confidentialité Lenovo** avant de pouvoir transférer des données à Support Lenovo. Cette action ne doit être effectuée qu'une seule fois : lors de votre premier accès à la page.

Remarque : Vous pouvez accéder à la section « Afficher les conditions générales » et la **déclaration de confidentialité Lenovo** en haut de la page pour les consulter à tout moment.

Configuration de l'appel vers Lenovo

Neuf champs doivent obligatoirement être remplis :

- Pays
- Nom de contact
- Téléphone
- E-mail
- Code postal
- Nom de la société
- Adresse
- Ville
- État/province

Attention : tous les champs requis doivent être remplis. Sinon, vous ne pourrez pas appliquer les modifications et activer le **service de signalement à Lenovo**.

État de ticket

Chaque ticket peut présenter l'un des cinq états suivants :

- **En attente :** les informations de maintenance sont envoyées ou en attente de réponse.
- **Actif :** les informations de maintenance ont été envoyées avec succès et le problème est en cours de traitement.
- **Échec :** échec de l'envoi des informations de maintenance.
- **Fermé :** le problème a été traité et fermé.
- **Annulé :** le problème a été traité et annulé.

Appel vers Lenovo test

Vous pouvez tester la fonction d'appel vers Lenovo en cliquant sur « Appel vers Lenovo test ». Un message s'affiche en haut de la page pour vous indiquer si l'opération s'est terminée avec succès. Vous pouvez également consulter le journal des événements ci-dessous pour obtenir le résultat du test.

- **Action — Annuler :** Lorsque l'état d'un ticket est « Actif », vous pouvez cliquer sur l'icône « Annuler » dans la colonne « Action » pour annuler le ticket.
- **Action — Remarque :** lorsque vous cliquez sur l'icône « Remarque » dans la colonne « Action », vous êtes invité(e) à laisser des remarques relatives à l'événement correspondant.

  Remarque : Les sections Titre et Corps du message doivent être remplies afin de finaliser l'envoi. Cette fonction envoie **UNIQUEMENT des informations au serveur**. Elle n'est pas destinée à l'enregistrement ou à l'affichage d'informations. Si vous cliquez de nouveau sur Remarque, une nouvelle fenêtre s'affiche ; vous pouvez alors laisser un autre message.

Attention : pour réussir l'appel vers Lenovo, assurez-vous que les paramètres DNS sont valides et qu'une connexion à l'adresse Internet requise a bien été établie. Si XClarity Controller accède à Internet via un proxy HTTP, assurez-vous que le serveur proxy est configuré pour utiliser l'authentification de base et qu'il est configuré en tant que proxy sans terminaison.

Proxy HTTP

Le **proxy HTTP** occupe deux rôles intermédiaires, sous la forme d'un client HTTP et d'un serveur HTTP pour les fonctions de sécurité, de gestion et de mise en cache. Le proxy HTTP achemine les demandes du client HTTP à partir d'un navigateur Web vers Internet, tout en prenant en charge la mise en cache des données Internet.

- **Adresse du serveur proxy :** ce champ est requis pour activer le serveur proxy HTTP. Les utilisateurs peuvent spécifier l'adresse IP ou le nom d'hôte en respectant la limite de 63 caractères. Le nom d'hôte doit uniquement être composé de caractères alphanumériques, de traits d'union (« - ») et de traits de soulignement (« _ »).
- **Port :** ce champ est obligatoire pour indiquer le port du serveur proxy HTTP. Seuls des numéros allant de 1 à 65 535 peuvent être saisis dans ce champ.
- **Test du proxy :** pour activer cette fonction, vous devez renseigner l'emplacement du proxy et le port du proxy appropriés afin de vérifier si la fonction du proxy HTTP actuel est disponible.
- **Nom d'utilisateur :** si l'option « **Requiert l'authentification** » est activée, le nom d'utilisateur est requis et sert de données d'identification pour le proxy. Ce champ autorise un nombre maximal de 30 caractères et les espaces ne sont pas valides.
- **Mot de passe :** ce champ est facultatif et s'affiche si l'option « Requiert l'authentification » est activée. Ce champ autorise un nombre maximal de 15 caractères et les espaces ne sont pas valides.

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. Recherchez et sélectionnez le fichier de sauvegarde et entrez le mot de passe lorsque vous y êtes invité.
2. Vérifiez le fichier en cliquant sur **Afficher le contenu** pour 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 utilisateur locaux**
  - **Conserver les paramètres réseau**
- 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 de BMC aux paramètres d'usine par défaut n'affecte pas les paramètres UEFI.

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 73.

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 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.

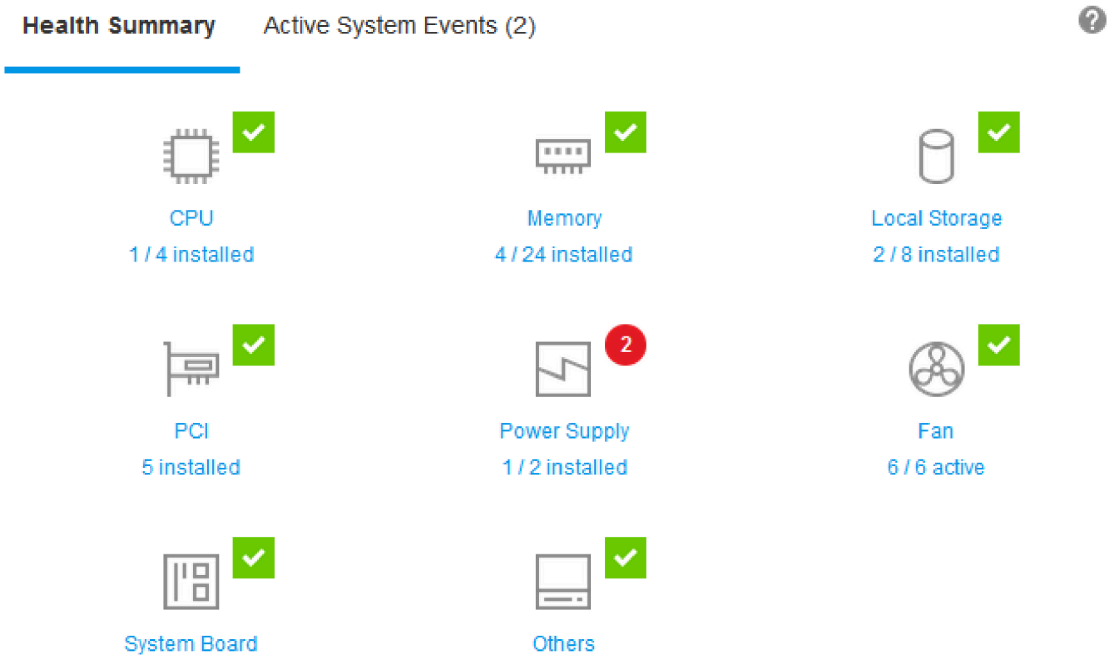
Affichage de l'état d’intégrité/des événements système actifs

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 :

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

Remarque : Stockage local peut afficher l'icône d'état « non disponible » sur les systèmes avec une configuration de fond de plane à remplacement standard.



Si l'un des composants matériels ne fonctionne pas normalement, il est marquée par une icône Critique ou Avertissement. Une condition critique est indiquée par une icône représentant un cercle rouge, tandis qu'une condition d'avertissement est indiqué 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, vous êtes redirigé vers la page **Inventaire**.

Affichage des informations système

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

Le panneau **Informations système et Paramètres** situé à gauche 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
- Propriété USB avant
- Licence BMC
- Adresse IP BMC
- Nom d'hôte du BMC
- Version UEFI
- Version BMC
- Version LXPM
- Emplacement

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

Tableau 5. 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.
System stopped in UEFI	Le serveur est sous tension ; UEFI a détecté un problème et a été arrêté en cours d'exécution.
Amorçage du système d'exploitation ou dans un système d'exploitation non pris en charge	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.
Suspendu vers RAM	Le serveur a été placé en mode de secours ou en mode veille.
Système exécuté en test mémoire	Le serveur est sous tension et exécute des outils de diagnostic de la mémoire.
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. Entrez le nom de système que vous voulez utiliser, puis cliquez sur la coche verte.

Si vous souhaitez modifier la propriété USB avant, cliquez sur l'icône de crayon et sélectionnez le mode **Propriété USB avant** de votre choix dans le menu déroulant. Ensuite, cliquez sur la coche verte.

Si votre serveur dispose d'une licence autre que la licence d'entreprise de XClarity Controller, vous pourrez peut-être acheter une mise à niveau de licence pour activer les fonctions étendues. 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 vers la section **Configuration Ethernet** sous **Réseau**.
- Pour les éléments de version UEFI et BMC, vous être redirigé vers la page **Mise à jour du microprogramme**.
- Pour l'élément d'emplacement, vous être redirigé vers 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 E-S. Les données d’utilisation viennent toutes du côté ME (gestionnaire de nœuds). Elles peuvent être consultées dans la vue Graphique ou la vue Tableau, qui comprend les éléments ci-après :

- **Température**
  - Affichage de 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.

  - L’onglet Historique affiche les températures historiques des dernières 24 heures maximum.
- **Utilisation de l’alimentation**
  - Affichage d’un graphique circulaire sur la consommation d’énergie actuelle, ainsi que d’un graphique historique sur la consommation d’énergie portant sur les dernières 24 heures maximum.
  - 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**
  - Représentation d’un instantané d’utilisation actuelle du système, ainsi que des sous-système du processeur, de la mémoire et d’E-S.
  - L’actualisation du navigateur ou la fonction de rafraîchissement permettent de mettre à jour les données d’utilisation actuelle.
  - L’utilisation du sous-système de l’UC représente le pourcentage de la bande passante totale de l’UC actuellement utilisée, telle que mesurée par les compteurs de performances intégrés dans l’UC. Ces valeurs peuvent légèrement différer des données d’utilisation de l’UC indiquées par le système d’exploitation.
  - L’utilisation du sous-système de mémoire représente le pourcentage de la bande passante totale du contrôleur de canal de mémoire en cours d’utilisation. Ces valeurs ne reflètent pas la quantité de mémoire en cours d’utilisation.
  - L’utilisation du sous-système d’E-S représente le pourcentage de la bande passante totale du trafic PCIe en cours d’utilisation.
  - Bande passante mesurée calculée sous la forme d'un pourcentage de la bande passante de mémoire utilisée et maximale disponible (par seconde).
- **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. Si le ventilateur fonctionne déjà à vitesse maximale, alors aucune modification ne sera apportée

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. Une case bleue autour de l'icône indique que ce 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 63.

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

Les informations de cette rubrique vous indiquent comment ajouter et modifier des destinataires de notifications par courrier électronique et notifications syslog ou des destinataires d'interruption SNMP.

Voici une description des actions qui peuvent être exécutées sous l'onglet **Destinataires de l'alerte**.

Les éléments d'action suivants peuvent être effectués dans la section destinataires **E-mail/Syslog**.

- **Création** : Sélectionnez cet élément d'action pour créer des destinataires e-mail/Syslog supplémentaires. Jusqu'à 12 destinataires e-mail/Syslog uniques peuvent être configurés.
  - **Créer un destinataire des e-mails** : Sélectionnez cette action pour créer un destinataire des e-mails.
    - Entrez le nom et l'adresse e-mail du destinataire.
    - Choisissez d'activer ou de désactiver la notification d'événement. Si vous choisissez la désactivation, le compte reste configuré, mais aucun e-mail n'est envoyé.
    - Sélectionnez les types d'événements dont sera informé le destinataire. Si vous cliquez sur le menu déroulant situé en regard des libellés de catégorie Critique, Attention ou Système, vous pouvez sélectionner ou désélectionner des notifications pour des éléments spécifiques de la catégorie.
    - Vous pouvez indiquer si le contenu du journal des événements doit ou non être inclus dans les alertes e-mail.
    - L'index indique les 12 emplacements de destinataires qui sont affectés.
    - Vous pouvez configurer ici le serveur de messagerie sur lequel seront envoyés les événements ou cliquer sur l'action du serveur SMTP en haut de la section. Pour plus de détails sur la configuration, voir la section Serveur SMTP ci-dessous.
  - **Créer un destinataire Syslog** : Sélectionnez cette action pour créer un destinataire Syslog.
    - Entrez le nom et l'adresse IP ou le nom d'hôte du serveur Syslog.
    - Choisissez d'activer ou de désactiver la notification d'événement. Si vous choisissez la désactivation, le compte reste configuré, mais aucun e-mail n'est envoyé.
    - L'index indique les 12 emplacements de destinataires qui sont affectés.

  - Sélectionnez les types d'événements qui seront envoyés au serveur Syslog. Si vous cliquez sur le menu déroulant situé en regard des libellés de catégorie Critique, Attention ou Système, vous pouvez sélectionner ou désélectionner des notifications pour des éléments spécifiques de la catégorie.
- **Serveur SMTP** : Sélectionnez cette action pour configurer les paramètres appropriés pour le serveur de messagerie SMTP. Un seul serveur de messagerie peut être configuré. La même configuration de messagerie est utilisée lors de l'envoi d'alertes à tous les destinataires d'e-mail configurés. Le BMC passe automatiquement d'une connexion sécurisée à une connexion chiffrée pour le transfert de courrier électronique en utilisant la commande STARTTLS uniformément via le port 587, si le serveur de messagerie cible la prend en charge.
  - Entrez le nom d'hôte ou l'adresse IP ainsi que le numéro de port réseau du serveur de messagerie.
  - Si le serveur de messagerie requiert une authentification, sélectionnez la case à cocher **Demande d'authentification** et entrez le nom d'utilisateur et le mot de passe. Sélectionnez le type d'authentification requise par le serveur de messagerie, un mécanisme d'authentification défi-réponse (**CRAM-MD5**) ou des données d'identification (**LOGIN**).
  - Certains réseaux peuvent bloquer les e-mails sortants si la valeur de chemin inversé est différente de celle attendue. Par défaut, XClarity Controller utilisera alertmgr@domain, où le domaine est le nom de domaine indiqué dans la section DDNS de la page Web réseau de XClarity Controller. Vous pouvez spécifier vos propres informations d'expéditeur à la place des informations par défaut.
  - Vous pouvez tester la connexion au serveur de messagerie pour vous assurer que les paramètres de messagerie sont configurés correctement. XClarity Controller affiche un message indiquant si la connexion a ou non abouti.
- **Réessayer et retarder** : Sélectionnez cet élément d'action pour configurer les paramètres appropriés concernant les options Réessayer et retarder.
  - La limite du paramètre Réessayer indique le nombre de fois supplémentaires que XClarity Controller essaiera d'envoyer une alerte si la tentative initiale a échoué.
  - Le délai entre les entrées indique la durée pendant laquelle XClarity Controller patientera après avoir envoyé une alerte à un destinataire avant d'envoyer une alerte au destinataire suivant.
  - Le délai entre tentatives indique la durée pendant laquelle XClarity Controller patientera après une tentative échouée avant d'essayer de nouveau d'envoyer l'alerte.
- **Protocole** : Sélectionnez cette action pour configurer les paramètres appropriés pour le protocole de connexion.
  - Vous pouvez choisir entre le **protocole TCP** ou le **protocole UDP**. Veuillez noter que ce paramètre s'appliquera à tous les destinataires syslog.
- Si des destinataires e-mail ou Syslog ont été créés, ils sont répertoriés dans cette section.
  - Pour modifier les paramètres d'un destinataire e-mail ou Syslog, cliquez sur l'icône de crayon sous l'en-tête d'action en regard du destinataire à configurer.
  - Pour retirer un destinataire e-mail ou syslog, cliquez sur l'icône de corbeille.
  - Pour envoyer une alerte de test à un destinataire e-mail ou Syslog, cliquez sur l'icône représentant un avion de papier.

Les éléments d'action suivants peuvent être effectués dans la partie utilisateur **SNMPv3**.

- **Créer** : Sélectionnez cette action pour créer des destinataire d'interruption SNMPv3.
  - Sélectionnez le compte utilisateur qui doit être associé aux interruptions SNMPv3. Le compte utilisateur doit être l'un des douze comptes utilisateur locaux.
  - Indiquez le nom d'hôte ou l'adresse IP du gestionnaire SNMPv3 qui recevra les interruptions SNMPv3.

- XClarity Controller utilise l'algorithme de hachage HMAC-SHA pour s'authentifier auprès du gestionnaire SNMPv3. Il s'agit du seul algorithme pris en charge.
- Le mot de passe de confidentialité est utilisé avec le protocole de confidentialité pour le chiffrement des données SNMP.
- Le **Paramètre global SNMPv3** s'applique à tous les destinataires d'interruption SNMPv3. Ces paramètres peuvent être configurés lors de la création d'un destinataire d'interruption SNMPv3 ou en cliquant sur l'action Paramètres SNMPv3 dans la partie supérieure de la zone utilisateur **SNMPv3**.
  - Indiquez si les interruptions SNMPv3 doivent être activées ou désactivées. Si elle sont activées, les paramètres restent configurés mais aucune interruption SNMPv3 n'est envoyée.
  - Le contact et les informations d'emplacement BMC sont obligatoires et sont configurés sur la page Web des propriétés de serveur. Pour plus d'informations, voir « Définition de l'emplacement et du contact » à la page 91.
  - Sélectionnez les types d'événements qui déclencheront l'envoi d'interruptions au gestionnaire SNMPv3. Si vous cliquez sur le menu déroulant situé en regard des libellés de catégorie Critique, Attention ou Système, vous pouvez sélectionner ou désélectionner des notifications pour des éléments spécifiques de la catégorie.

  Remarque : Le transfert de données entre le client SNMP et l'agent peut être protégé à l'aide de leur chiffrement. Les méthodes prises en charge pour le **protocole de sécurité** sont CBC-des et AES.
- Si des destinataires d'interruption SNMPv3 ont été créés, ils sont répertoriés dans cette section.
  - Pour modifier les paramètres d'un destinataire SNMPv3 T, cliquez sur l'icône de crayon sous l'en-tête d'action en regard du destinataire à configurer.
  - Pour retirer un destinataire SNMPv3, cliquez sur l'icône de corbeille.

Capture des données d'écran du dernier échec du système d'exploitation

Les informations de cette rubrique vous indiquent comment capturer et afficher un écran d'échec du système d'exploitation.

L'écran du système d'exploitation est automatiquement capturé lorsqu'un dépassement du délai d'attente de l'horloge de surveillance se produit. Si un événement se produit qui entraîne l'arrêt du système d'exploitation, la fonction d'horloge de surveillance du système d'exploitation est déclenchée et le contenu de l'écran est capturé. XClarity Controller stocke une seule capture d'écran. Lorsqu'un dépassement du délai d'attente de l'horloge de surveillance se produit, une nouvelle capture d'écran remplace la capture d'écran précédente. La fonction d'horloge de surveillance du système d'exploitation doit être activée pour capturer l'écran d'échec du système d'exploitation. Pour définir l'heure de l'horloge de surveillance du système d'exploitation, voir « Configuration des délais d'attente du serveur » à la page 92 pour plus d'informations. La fonction de capture d'écran d'échec du système d'exploitation est disponible uniquement avec le niveau de fonctionnalité avancé ou entreprise de XClarity Controller. Pour plus d'information sur le niveau de fonctionnalité XClarity Controller installé sur votre serveur, consultez la documentation de votre serveur.

Cliquez sur l'action **Dernier écran d'échec** dans la section **Console distante** de la page d'accueil de XClarity Controller afin d'afficher une image du système d'exploitation qui a été capturée lorsque s'est produit le dépassement du délai d'attente de l'horloge de surveillance. La capture peut également être affichée en cliquant sur **Service**, puis sur **Dernier écran d'échec** dans la section **Action rapide** de la page d'accueil. Si le système n'a pas détecté de dépassement du délai d'attente de l'horloge de surveillance du système d'exploitation et n'a pas capturé d'écran du système d'exploitation, un message indiquant que l'écran d'échec n'a pas été créé s'affiche.

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

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.

Remarques :

- 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 le mode et 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 le mode d'amorçage du système, les deux options suivantes sont disponibles :

Démarrage UEFI
Sélectionnez cette option pour configurer un serveur qui prend en charge l'interface UEFI (Unified Extensible Firmware Interface). Si vous démarrez les systèmes d'exploitation avec UEFI activé, cette option peut réduire la durée d'initialisation en désactivant la mémoire morte existante d'option.

Démarrage existant
Sélectionnez cette option si vous configurez un serveur pour démarrer un système d'exploitation qui requiert le microprogramme (BIOS) existant. Sélectionnez cette option uniquement si vous démarrez les systèmes d'exploitation avec UEFI non activé.

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.

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 modifiez le type d'amorçage à effectuer à l'aide du dispositif d'amorçage unique, vous pouvez également spécifier que l'amorçage soit un amorçage existant ou un amorçage UEFI. Cliquez sur la case à cocher **Préférer l'amorçage existant** si vous souhaitez que l'amorçage soit un amorçage BIOS existant. Désactivez la case à cocher si voulez un amorçage UEFI. 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 châssis contenant des nœuds de serveurs lame ou à haute densité, le refroidissement et l'alimentation du châssis sont contrôlés par le contrôleur de gestion de châssis au lieu du XClarity Controller.

Configuration de la redondance d'alimentation

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

Remarque : Actuellement, l'utilisateur ne peut pas modifier la politique d'alimentation au sein des systèmes AMD.

Lorsque 2 unités d'alimentation électrique sont installées, le mode de redondance est défini sur Redondance (N+N). Lorsque cette configuration avec 2 unités d'alimentation est utilisée, si l'une des unités d'alimentation est défaillante, si l'alimentation en courant alternatif a été coupée ou a été retirée, un événement de perte de redondance est signalé 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.
- **Redondance (N+1)** : une source d'alimentation principale est en mesure d'alimenter le système. Au moins une source d'alimentation de secours est en outre disponible pour prendre la relève en cas de panne de la source principale. La source de secours est conçue pour fournir suffisamment d'alimentation pour permettre au système de fonctionner jusqu'à ce que la source principale puisse être réparée ou remplacée. La redondance N+1 offre un niveau de tolérance aux pannes de moindre importance par rapport à la redondance N+N.
- **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.

Remarque : Les serveurs de processeur AMD ne prennent pas en charge les utilisateurs pour configurer la fonction de stratégie de plafonnement énergétique.

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**.

Le plafonnement énergétique peut être activé à l'aide des mesures de consommation d'alimentation en courant alternatif ou de consommation électrique en courant continu. Dans le menu déroulant, sélectionnez le type de mesures qui sera utilisé pour déterminer la limite de plafonnement énergétique. En passant du courant alternatif au courant continu, la valeur affichée sur le curseur changera 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.

Remarque : L'option **Règles d'alimentation** n'est pas disponible lorsque XClarity Controller est dans un châssis contenant des nœuds de serveurs lame ou à haute densité. La stratégie d'alimentation est contrôlée par le contrôleur de gestion de châssis au lieu de XClarity Controller.

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.

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

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

Remarque : L'option **Stratégie de restauration de l'alimentation** n'est pas disponible dans un châssis contenant des nœuds de serveurs lame ou à haute densité. La stratégie de restauration d'alimentation est contrôlée par le contrôleur de gestion de châssis au lieu de XClarity Controller.

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 6. 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.
Redémarrez le serveur normalement	Sélectionnez cette action pour arrêter le système d'exploitation et effectuer un cycle d'alimentation du serveur.
Redémarrez le serveur immédiatement	Sélectionnez cette action pour éteindre et rallumer le serveur immédiatement, sans arrêter d'abord le système d'exploitation.
Amorcer et 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.
Cycle d'alimentation en courant alternatif du serveur	Sélectionnez cette action pour effectuer un cycle d'alimentation sur le serveur.
Remarque : 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.	

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.

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 uniquement disponible dans les fonctions de niveau avancé et de niveau entreprise 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 niveau depuis XClarity Controller Standard vers XClarity Controller Avancé ou Enterprise, voir « Mise à niveau de XClarity Controller » à la page 6.

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

- Afficher une vidéo à distance avec une résolution graphique allant jusqu'à 1280 x 1024 à 72 ou 75 Hz, indépendamment de 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 50 Mo peuvent être téléchargés en mémoire XClarity Controller.

Remarques :

- Lorsque la fonction de console distante est démarrée en mode multi-utilisateur, (XClarity Controller avec le jeu de fonctions de niveau entreprise 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 36.
- 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 fonction de console distante

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

Comme mentionné précédemment, la fonctionnalité de console distante de XClarity Controller est uniquement disponible dans les fonctions de niveau avancé et de niveau entreprise 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 avancée de XClarity Controller, installez-la en suivant les instructions sous « Installation d'une clé d'activation » à la page 105.

Pour utiliser la fonctionnalité de console distante, procédez comme suit :

1. Cliquez sur l'image avec une flèche pointant en diagonale dans la section Console distante de la page d'accueil du XClarity Controller ou de la page Web de Console distante.
2. Sélectionnez l'un des modes suivants :
   - Démarrer la console distante en mode mono-utilisateur
   - Démarrer la console distante en mode multi-utilisateur

   Remarque : Le XClarity Controller avec la fonction de niveau entreprise prend en charge jusqu'à six sessions vidéo simultanées en mode multi-utilisateur.
3. Choisissez d'autoriser ou non d'autres utilisateurs à demander l'envoi d'une demande de déconnexion à un utilisateur de console distante lorsque quelqu'un souhaite utiliser la fonction de console distante et que celle-ci est déjà en mode mono-utilisateur, ou lorsque le nombre maximal d'utilisateurs autorisés à utiliser la fonction de console distante en mode multi-utilisateur est atteint. L'option **Intervalle de temps sans réponse** spécifie combien de temps le XClarity Controller attendra avant de déconnecter automatiquement l'utilisateur en l'absence de réponse à la demande de déconnexion.
4. Choisissez d'autoriser ou non l'enregistrement des trois dernières vidéos de démarrage du serveur.
5. Choisissez d'autoriser ou non l'enregistrement des trois dernières vidéos de plantage du serveur.
6. Choisissez d'autoriser ou non la capture d'écran de l'échec du SE avec une erreur HW.
7. Cliquez sur **Lancer la console distante** pour ouvrir la page de la console distante dans un autre onglet. Lorsque toutes les sessions de console distante possibles sont utilisées, une boîte de dialogue s'affiche. Dans cette boîte de dialogue, l'utilisateur peut envoyer une demande de déconnexion à l'utilisateur de la console distante qui a activé le paramètre **Autoriser d'autres personnes à demander la déconnexion de ma session à distance**. L'utilisateur peut accepter ou refuser la demande de déconnexion. Si l'utilisateur ne répond pas dans l'intervalle spécifié par le paramètre **Intervalle de temps sans réponse**, la session utilisateur sera automatiquement terminée par le XClarity Controller.

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.

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

Redémarrez 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 sous le type de fichier PNG.

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 Échap, 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. D'autres macros définies par le serveur peuvent être définies à l'aide de Lenovo XClarity Essentials et être téléchargées depuis le XClarity Controller. Ces macros sont définies pour tous les utilisateurs de la fonction de console distante.
- Cliquez sur **Configurer** pour ajouter ou supprimer des macros définies par l'utilisateur. Les macros définies par l'utilisateur sont définies uniquement pour l'utilisateur actuel de la console distante. Les autres utilisateurs de la console distante ne verront pas les macros définies par les autres utilisateurs.
  - Cliquez sur l'icône Ajouter des macros et appuyez sur les séquences de touches que vous souhaitez. Ensuite, cliquez sur **Ajouter** pour ajouter une nouvelle macro.
  - Pour supprimer une macro définie par l'utilisateur, sélectionnez la macro dans la liste, puis cliquez sur l'icône de corbeille.
  - Pour envoyer une macro définie par l'utilisateur au serveur, sélectionnez l'option **Macros définies par l'utilisateur**, puis cliquez sur la macro que vous souhaitez envoyer.

Prise en charge de la souris de la console distante

Ces informations décrivent les options du contrôle à distance de la souris.

La fenêtre de console distante propose plusieurs options pour le contrôle de la souris, à savoir le contrôle absolu de la souris, le contrôle relatif de la souris (aucune accélération) et le contrôle de la souris (RHEL, Linux plus ancien).

Contrôle absolu et relatif de la souris

Les informations suivantes vous permettent d'accéder aux options de contrôle absolu et relatif de la souris.

Pour accéder aux options de contrôle absolu et relatif de la souris, procédez comme suit :

Etape 1. Dans la fenêtre de la console distante, cliquez sur **Souris**.

Etape 2. Cliquez sur **Paramètres de la souris** dans le menu déroulant.

Etape 3. Sélectionnez l'un des modes **Accélération** suivants de la souris :

Positionnement absolu (Windows, dernière version de Linux et Mac OS X)
Le client envoie au serveur des messages d'emplacement de la souris relatifs à l'origine (angle supérieur gauche) de la zone d'affichage.

Positionnement relatif, pas d'accélération
Le client envoie l'emplacement de la souris en tant que décalage par rapport à la position précédente.

Positionnement relatif (version plus ancienne de Linux)
Ce mode applique un facteur d'accélération pour mieux aligner la souris sur certaines cibles Linux. Les paramètres d'accélération ont été sélectionnés pour optimiser la compatibilité avec les distributions Linux plus anciennes.

Enregistrement/relecture de vidéo à l'écran

Utilisez les informations de cette rubrique pour enregistrer ou relire des vidéos à l'écran en présence à distance.

L'interface Web de XClarity Controller fournit une fonction de type DVR pour permettre la prise charge de l'enregistrement et de la lecture de vidéos à l'écran en présence à distance. Cette fonction prend uniquement en charge l'enregistrement vidéo vers un dossier réseau. Les protocoles NFS et CIFS sont actuellement pris en charge. La section ci-après décrit les étapes de l'utilisation de la fonction d'enregistrement et de relecture.

1. Sur la page Web de la console distante, cliquez sur **Enregistrement de l'écran** pour ouvrir la fenêtre Paramètres.
2. Dans la fenêtre Paramètres, vous devrez peut-être spécifier les informations suivantes.
   - Si le type de montage « CIFS » est sélectionné, indiquez les paramètres de **dossier distant**, de **nom d'utilisateur** et de **mot de passe**. Le format du dossier distant CIFS est « **//<adresse IP distante>/<nom du dossier** ». Par exemple : //xxx.xxx.xxx.xxx/dossier.
   - Si le type de montage « NFS » est sélectionné, indiquez les paramètres de **dossier distant**. Le format du dossier distant NFS est « **<adresse IP distante>:/<nom du dossier>** ». Par exemple : xxx.xxx.xxx.xxx:/dossier.
   - Indiquez le nom du fichier vidéo si nécessaire. Si un nom de fichier a déjà été fourni, une boîte de message d'erreur s'affiche. Pour remplacer le nom de fichier existant, choisissez « Remplacement du nom de fichier ». Si la case « Auto » est cochée, le nom du fichier vidéo sera automatiquement généré.

- La « taille max. de fichier » indique la taille maximale de fichier vidéo avant que l'enregistrement vidéo ne s'arrête automatiquement.
- La « durée max. d'enregistrement » indique la durée maximale d'enregistrement vidéo avant que l'enregistrement ne s'arrête automatiquement.

3. Cliquez sur **Commencer l'enregistrement** pour démarrer l'enregistrement vidéo.
4. Cliquez sur **Arrêter l'enregistrement** pour arrêter l'enregistrement vidéo. Une fenêtre contextuelle indiquant « Enregistrement vidéo terminé » s'affiche et présente les informations d'enregistrement vidéo pertinentes.
5. Téléchargez les vidéos enregistrées à partir de NFS ou CIFS vers votre dossier local. Dans la section Aperçu de la console distante de la page d'accueil de XClarity Controller, cliquez sur **Vidéos enregistrées** et sélectionnez le fichier vidéo à relire.

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 Échap. 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.

Mise à l'échelle de l'écran
Lorsque la mise à l'échelle est activée, l'image vidéo est dimensionnée de sorte que l'image toute entière remplisse la fenêtre de la console.

Écran d'origine
L'image vidéo a les mêmes dimensions que sur le serveur. Les barres de défilement sont affichées si nécessaire pour permettre l'affichage des parties de l'image vidéo qui n'entrent pas dans la fenêtre.

Mode de couleur
Ajuste la profondeur de couleur de la fenêtre de la console distante. Vous disposez de deux options de mode couleur :

- Couleur : 7, 9, 12, 15 et 23 bits
- Nuances de gris : 16, 32, 64 et 128 teintes

Remarque : Les modifications de mode de couleur sont généralement effectuées si votre connexion au serveur distant dispose d'une bande passante limitée et que vous souhaitez réduire la demande de bande passante.

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 fonction 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 fonctions de niveau entreprise de XClarity Controller. Pour monter le support local, cliquez sur **Activer** dans la section **Monter le support local**. Jusqu'à quatre fichiers peuvent être montés simultanément sur le serveur.

  Remarques :

  – Lorsque vous utilisez le navigateur Google Chrome, une option de montage supplémentaires intitulée **Mount files/folders** est disponible pour vous permettre de glisser-déplacer des fichiers/dossiers.

  – Si plusieurs sessions de console distantes concurrentes sont en cours avec un XClarity Controller, cette fonction peut être activée uniquement par l'une des sessions.
- 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.

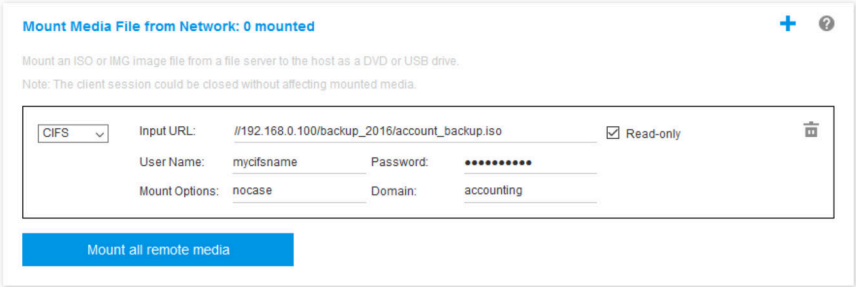
Remarque : Des erreurs peuvent se produire lors du processus de montage pour les certificats de sécurité générés par Microsoft IIS. Si cela se produit, voir « Problèmes liés aux erreurs de montage de support » à la page 89.

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.

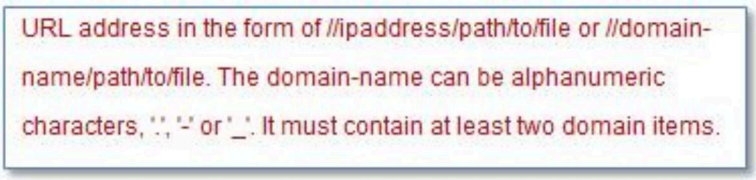
- Jusqu'à deux fichiers peuvent être téléchargés dans la mémoire de XClarity Controller et être montés en tant que support virtuel à l'aide de la fonction RDOC de XClarity Controller. La taille totale des deux fichiers ne doit pas dépasser 50 Mo. Ces fichiers resteront dans la mémoire de XClarity Controller 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.



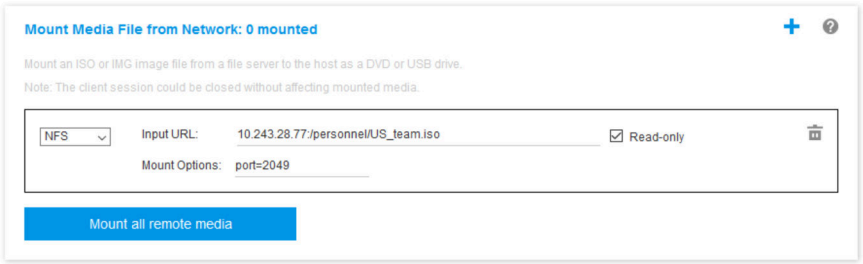
Le module BMC fournit des conseils lors de la spécification de l'URL. Si l'URL entrée n'est pas valide, le bouton de montage apparaîtra grisé et du texte rouge sera affiché sous le champ URL montrant le format attendu de l'URL.



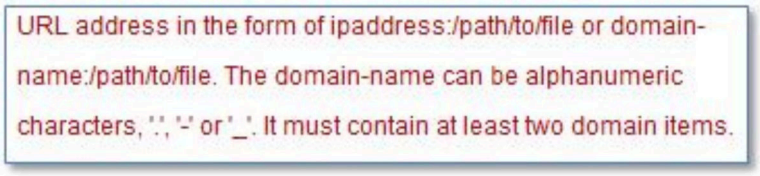
  - **NFS - Network File System** : voir la description ci-dessus pour des détails.

    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.

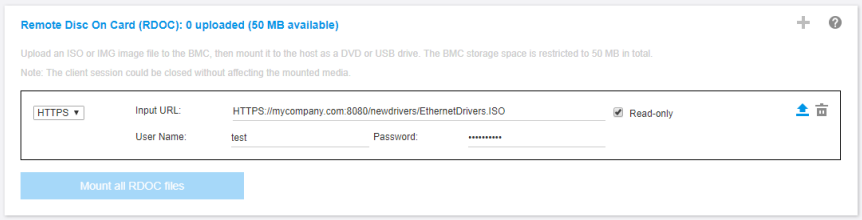


- **HTTPS (Hypertext Transfer Protocol Secure)** :
  - Entrez l'URL qui localise le fichier sur le système distant.
  - Si vous souhaitez que le fichier soit présenté sur le serveur en tant que support virtuel en lecture seule, cochez la case à cocher.
  - Entrez les données d'identification nécessaires 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 89.
  - 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 à cocher.

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
```

Disque distant utilisant le client Java

Cette section explique comment monter un support local à l'aide du client Java.

Vous pouvez utiliser le client Java pour affecter au serveur une unité de CD ou de DVD, une unité de disquette ou une clé USB se trouvant sur votre ordinateur. Vous pouvez également spécifier une image de disque sur votre ordinateur afin que le serveur l'utilise. Vous pouvez utiliser l'unité pour des fonctions telles que le redémarrage (amorçage) du serveur, la mise à jour du code, l'installation de nouveaux logiciels sur le serveur et l'installation ou la mise à jour du système d'exploitation sur le serveur. Vous pouvez accéder au disque distant. Les unités et les images de disque sont affichées en tant qu'unités USB sur le serveur.

Remarques : La console distante Java prend en charge l'un des environnements Java suivants, et elle ne peut être ouverte que si le client HTML5 n'est pas en cours d'exécution.

1. Oracle Java Runtime Environment 1.8/Java SE 8 ou versions plus récentes
2. OpenJDK 8. La distribution d'AdoptOpenJDK avec JVM HotSmos est prise en charge.

Si vous utilisez AdoptOpenJDK, vous devez l'utiliser sous https://openwebstart.com/ OSX, Windows et Linux.

Création d'un fichier image

Pour créer un nouveau fichier image à partir d'un dossier source spécifié, procédez comme suit :

1. Cliquez sur l'option **Créer une image** sous l'onglet **Support virtuel** dans la fenêtre du support virtuel du client Java. La fenêtre Créer une image à partir d'un dossier s'affiche.
2. Cliquez sur le bouton **Parcourir** associé à la zone **Dossier source** pour sélectionner le dossier source spécifique.
3. Cliquez sur le bouton **Parcourir** associé à la zone **Nouveau fichier image** pour sélectionner le fichier image à utiliser.
4. Cliquez sur le bouton **Créer une image**.

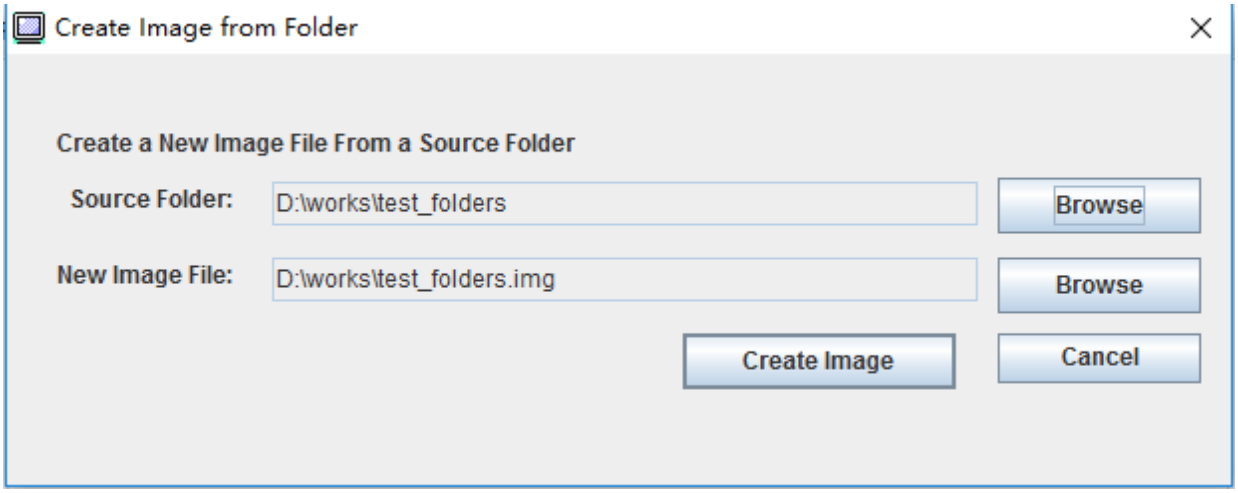


Figure 1. Création d'un fichier image

Sélection des périphériques à monter

Pour monter l'image locale, le dossier et l'unité de CD/DVD/USB, procédez comme suit :

Cliquez sur l'option **Sélectionner les périphériques à monter** sous l'onglet **Support virtuel** dans la fenêtre du support virtuel du client Java. La fenêtre Sélectionner les périphériques à monter s'affiche.

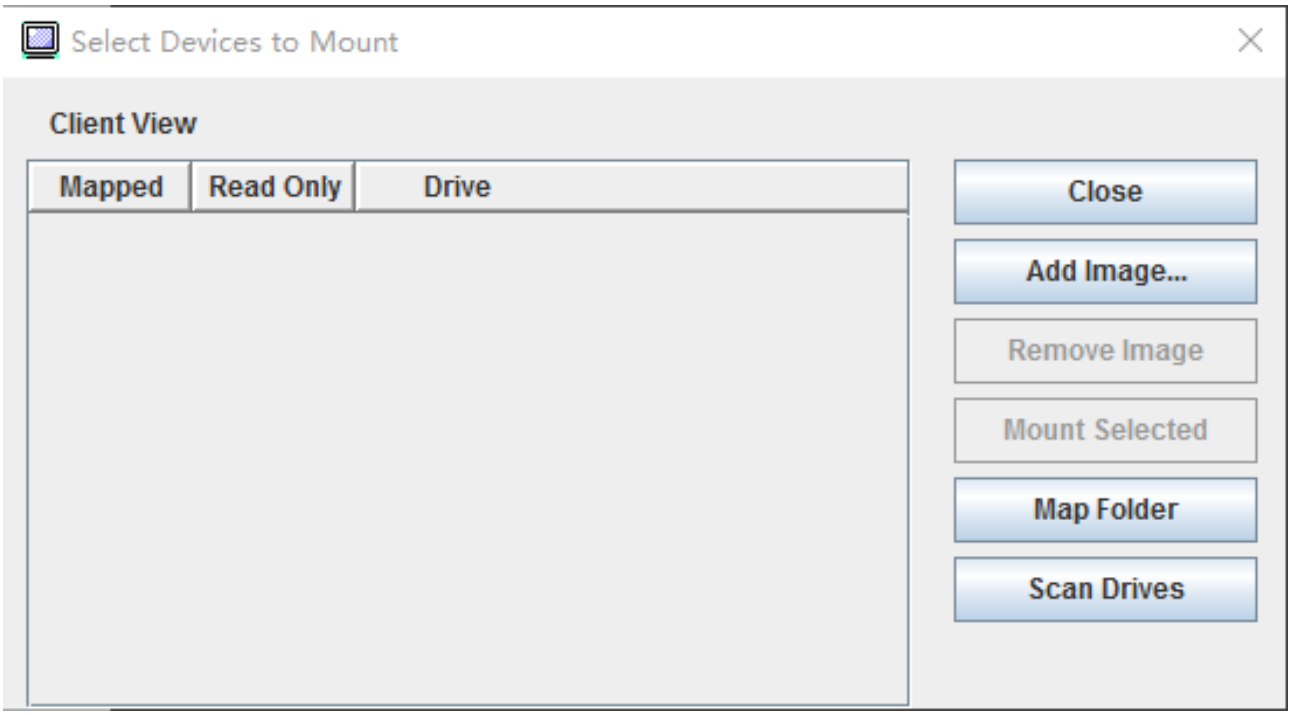


Figure 2. Fenêtre Sélectionner les périphériques à monter

Vous pouvez monter l'image locale, le dossier et l'unité de CD/DVD/USB en procédant comme suit :

- **Monter l'image locale** :
  1. Cliquez sur le bouton **Ajouter une image** pour sélectionner l'image que vous souhaitez monter.
  2. Cochez l'option **Mappé**.
  3. Cochez l'option **Lecture seule** pour activer la fonction si nécessaire.
  4. Cliquez sur le bouton **Monter la sélection** pour réussir le montage de l'image locale.

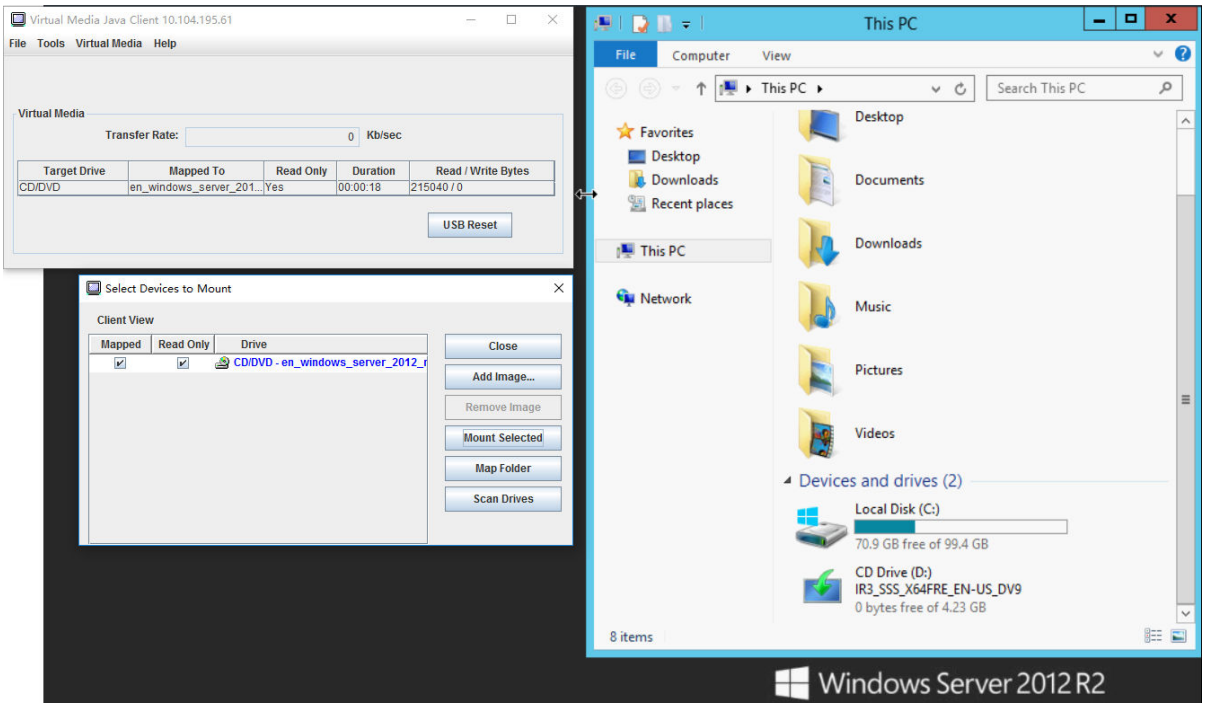


Figure 3. Monter l'image locale

- **Monter le dossier local** :
  1. Cliquez sur le bouton **Mapper un dossier** pour sélectionner le dossier local que vous souhaitez monter.
  2. Cliquez sur le bouton **Monter la sélection** pour réussir le montage du dossier local.

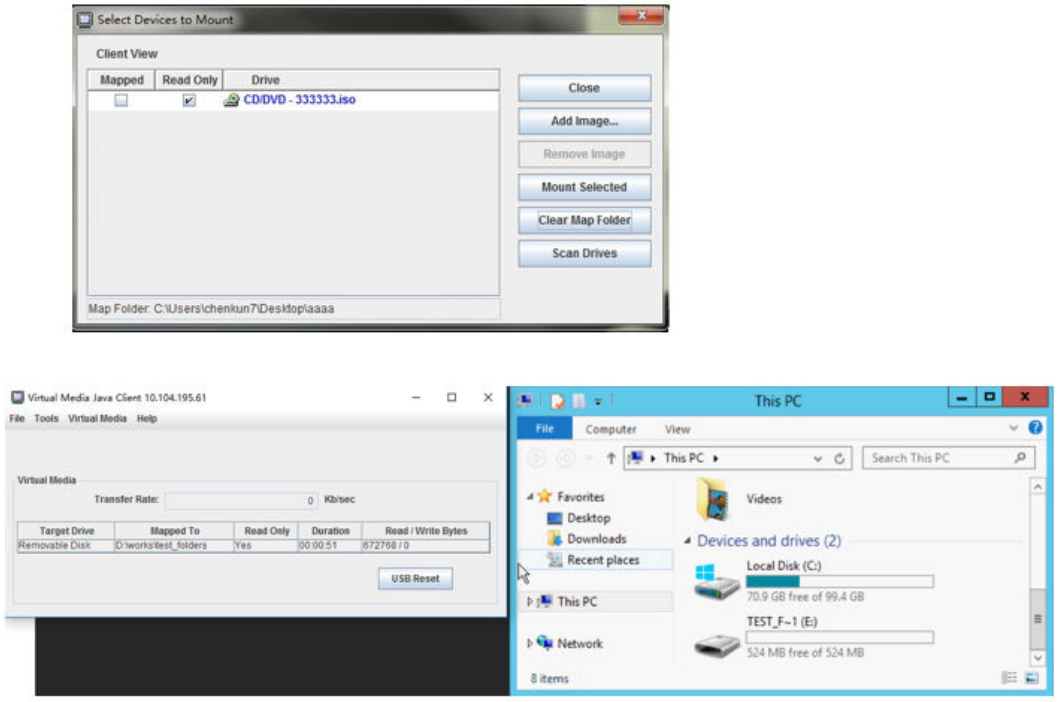


Figure 4. Monter le dossier local

- **Monter une unité de CD/DVD ou USB** :
  1. Cliquez sur le bouton **Rechercher les unités** pour détecter une unité de CD/DVD ou USB branchée.
  2. Cochez l'option **Mappé**.
  3. Cochez l'option **Lecture seule** pour activer la fonction si nécessaire.
  4. Cliquez sur le bouton **Monter la sélection** pour réussir le montage de l'image locale.

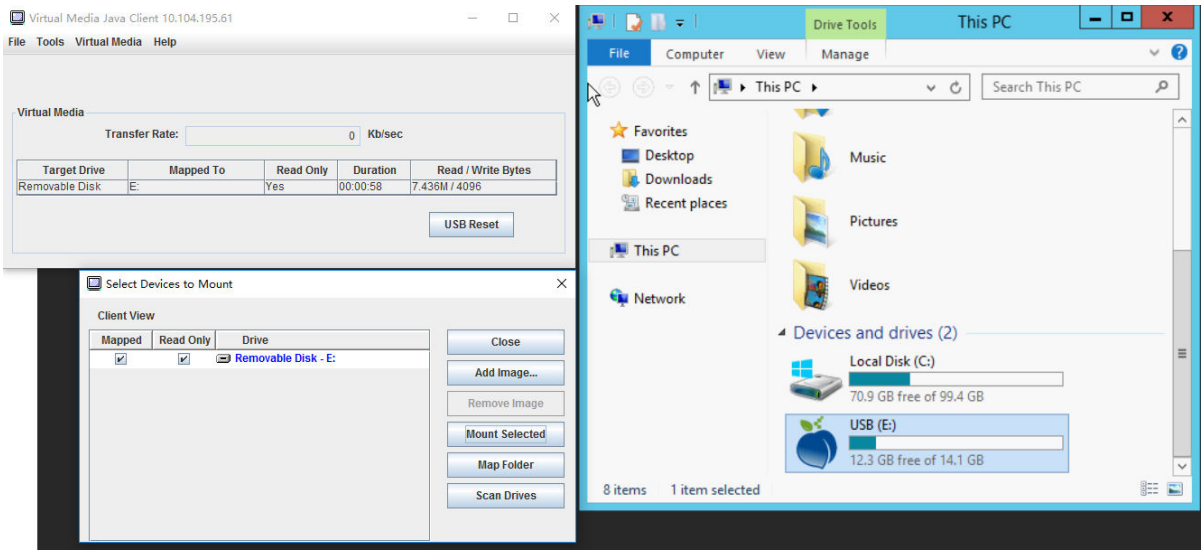


Figure 5. Monter une unité de CD/DVD ou USB

La fenêtre Sélectionner les périphériques à monter contient une liste des périphériques locaux actuellement disponibles pour le montage. Cette fenêtre contient les zones et les boutons suivants :

- La zone **Mappé** contient la case à cocher qui vous permet de sélectionner les périphériques à monter ou à mapper.
- La zone **Lecture seule** contient la case à cocher qui vous permet de sélectionner les périphériques mappés ou montés qui seront en *lecture seule* sur le serveur hôte.
- La zone **Unité** contient le chemin d'accès du périphérique sur la machine locale.
- Cliquez sur le bouton **Fermer** pour fermer la fenêtre Sélectionner les périphériques à monter.
- Cliquez sur le bouton **Ajouter une image** pour rechercher dans votre système de fichiers local l'image de disquette et le fichier image ISO que vous souhaitez ajouter à la liste des périphériques.
- Cliquez sur le bouton **Retirer une image** pour retirer une image qui a été ajoutée à la liste des périphériques.
- Cliquez sur le bouton **Monter la sélection** pour monter ou mapper tous les périphériques sélectionnés en vue de leur montage ou de leur mappage dans la zone **Mappé**.

  Remarque : Le dossier sera monté en lecture seule.
- Cliquez sur le bouton **Rechercher les unités** pour actualiser la liste des périphériques locaux.

Sélection des périphériques à démonter

Pour démonter les périphériques du serveur hôte, procédez comme suit :

1. Cliquez sur l'option **Démonter tout** sous l'onglet **Support virtuel** dans la fenêtre du support virtuel du client Java.
2. Après avoir sélectionné l'option **Démonter tout**, une fenêtre de confirmation Démonter tout s'affiche. Si vous acceptez, *tous* les périphériques du serveur hôte sur le serveur sont démontés.

   Remarque : Vous ne pouvez pas démonter des unités individuellement.

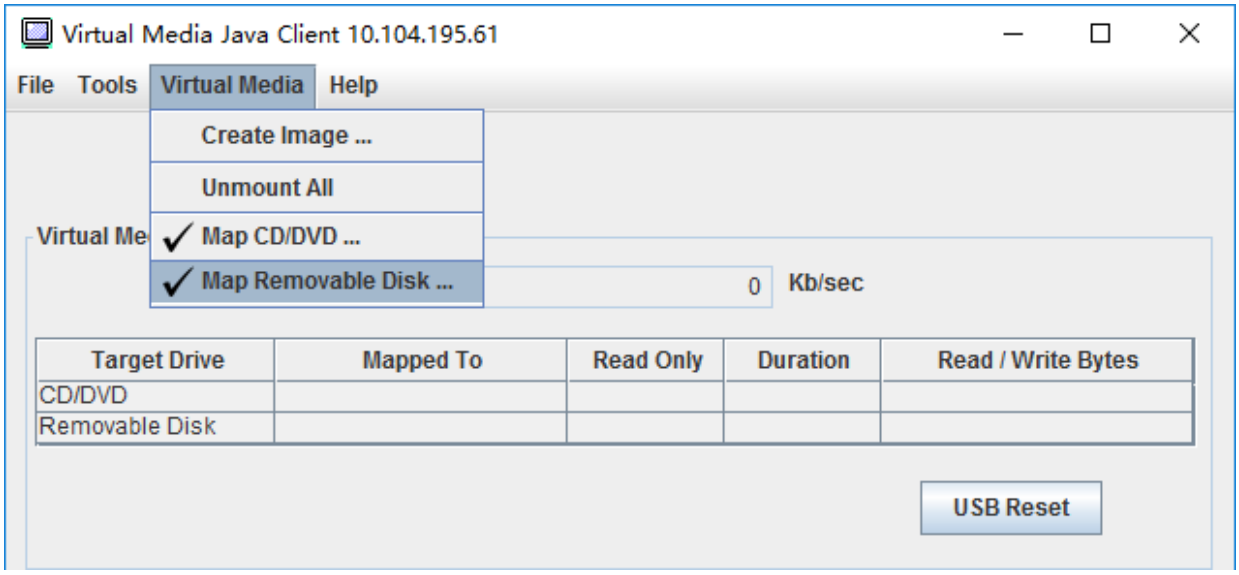


Figure 6. Démonter tout

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.

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 service 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 2.

L'utilisateur peut passer sa souris sur l'option Informations de base, puis cliquer sur la fenêtre flottante afin de consulter les données réelles à exporter.

Les Informations de base sont obligatoires, mais l'utilisateur a la possibilité d'exporter les informations ci-après :

- 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>_xcc_mini-log_<date>-<time>.zip`

Par exemple : 7X2106Z01A_2345678_xcc_mini-log_170511-175656.zip.

En plus du format zip, les données de maintenance peuvent également être téléchargées au format tzz par le biais de l'option **Parcourir l'historique...**. La préparation de tzz nécessite un certain délai. Ainsi, il ne s'affiche pas immédiatement après l'exportation des fichiers zip. Tzz utilise un algorithme de compression différent et peut être extrait avec un utilitaire comme « lzop ».

Parcourir l'historique... permet également de conserver les journaux de service récemment exportés.

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 du contact

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.

Remarque : La zone est facultative et n'est pas configurable dans un nœud Flex.

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.

Remarque : La zone est facultative et n'est pas configurable dans un nœud Flex.

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 :

Programme de surveillance du système d'exploitation
Le programme de surveillance du système d'exploitation permet de surveiller le système d'exploitation pour vérifier qu'il n'est pas bloqué. L'interface Ethernet via USB doit être activée pour activer cette fonction. Pour plus de détails, voir « Configuration d'Ethernet sur USB » à la page 34. Le XClarity Controller contacte le système d'exploitation conformément à un intervalle configuré dans la sélection **Temps du programme de surveillance du système d'exploitation**. Si le système d'exploitation ne répond pas avant l'heure de la vérification suivante, XClarity Controller suppose que le système d'exploitation est bloqué. XClarity Controller capture le contenu de l'écran du serveur puis redémarre le serveur afin de tenter de restaurer le fonctionnement. XClarity Controller redémarre le serveur une seule fois. Si le système d'exploitation est encore bloqué après la réinitialisation, plutôt que de continuer à redémarrer le serveur, celui-ci sera laissé en état de blocage de sorte que le problème puisse être analysé et corrigé. Pour réarmer le programme de surveillance de système d'exploitation, mettez le serveur hors tension, avant de le remettre sous tension. Pour activer le programme de surveillance du système d'exploitation, sélectionnez un intervalle dans le menu Temps du programme de surveillance

du système d'exploitation, puis cliquez sur **Appliquer**. Pour désactiver le programme de surveillance de système d'exploitation, sélectionnez **Aucun** dans le menu déroulant Temps du programme de surveillance du système d'exploitation.

Programme de surveillance du chargeur

Le programme de surveillance du chargeur surveille l'intervalle entre l'achèvement de l'autotest à la mise sous tension (POST) et le début de l'exécution du système d'exploitation. L'interface Ethernet via USB doit être activée pour activer cette fonction. Pour plus de détails, voir « Configuration d'Ethernet sur USB » à la page 34. Lorsque le POST est terminé, XClarity Controller démarre un chronomètre et commencer à contacter le système d'exploitation. Si le système d'exploitation ne répond pas dans l'intervalle de temps configuré dans la sélection Programme de surveillance du chargeur, XClarity Controller suppose que l'amorçage du système d'exploitation est bloqué. XClarity Controller redémarre alors le serveur pour tenter de restaurer le fonctionnement. XClarity Controller redémarre le serveur une seule fois. Si l'amorçage du système d'exploitation est encore bloqué après la réinitialisation, plutôt que de continuer à redémarrer le serveur, celui-ci sera laissé en état de blocage de sorte que le problème puisse être analysé et corrigé. Le programme de surveillance du chargeur est réarmé lorsque le serveur est mis hors tension puis remis sous tension ou que le serveur réussit à démarrer sur le système d'exploitation. Pour activer le programme de surveillance du chargeur, sélectionnez un intervalle dans le menu Programme de surveillance du chargeur, puis cliquez sur **Appliquer**. Pour désactiver le programme de surveillance du chargeur, sélectionnez **Aucun** dans le menu déroulant Programme de surveillance du chargeur.

Activer le délai de mise hors tension

Utilisez le champ Délai de mise hors tension pour spécifier le nombre de minutes pendant lesquelles le sous-système XClarity Controller doit attendre l'arrêt du système d'exploitation avant de forcer la mise 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.

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.
- 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 le heure d'été, vous pouvez également cocher la case à cocher **Régler automatiquement le passage à l'heure d'été**..
- Lorsque vos modifications de configuration sont terminées, cliquez sur **Appliquer**.

Remarques :

- 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.
- Les paramètres de date et d'heure de XClarity Controller ne peuvent pas être modifiés dans un Flex System.

Chapitre 6. 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 :

- Détails
- Configuration RAID

Détails RAID

Exploitez les informations de cette rubrique pour utiliser les fonctions de détails RAID.

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.

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 :

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

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 en cours 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.

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. 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.

      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.

      1) Pour ces types de situations, l'interface Web affiche **Répartition 1** par défaut.
      2) Sélectionnez les unités et cliquez sur **Ajouter un membre** pour ajouter les unités à **Répartition 1**. Lorsque **Répartition 1** n'a pas assez d'unités, désactivez le lien **Ajouter répartition**.
      3) Cliquez sur **Ajouter répartition** pour ajouter **Répartition 2**. Sélectionnez les unités et cliquez sur **Ajouter un membre** pour l'ajouter à **Répartition 2**.
      4) Cliquez sur **Ajouter un membre** pour ajouter des unités à la dernière répartition. Si vous souhaitez ajouter des unités à **Répartition 1** à nouveau, vous devez cliquer sur Répartition 1 et sélectionner les unités à ajouter à **Répartition 1**.
      5) Si le nombre de répartitions atteint la quantité maximale, désactivez **Ajouter répartition**.

   b. Pour créer des disques virtuels dans une grappe de disques existante, vous devez sélectionner une grappe de disques disposant de capacité.
2. **Création d'un disque virtuel**
   a. Par défaut, créez un disque virtuel qui 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. S'il existe plusieurs disques virtuels, l'icône **Retirer** est activée. 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 un disque virtuel** 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** : Affiche l'ID de la grappe de disques, le niveau RAID et le nombre total d'unités.
   - **Contenu du tableau** : Répertorie les propriétés de base ; nom d'unité, état RAID, type, numéro de série, numéro de composant, numéro FRU et 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** : Signale l'unité comme unité de secours globale ou dédiée.
     - **Retirer une unité de secours** : Supprime l'unité de cette fonction.
     - **Marquer l'unité comme hors ligne** : Définit l'unité sur l'état hors ligne.
     - **Marquer l'unité comme en ligne** : Définit l'unité sur l'état en ligne.
     - **Marquer l'unité comme réutilisable** : Définit l'unité comme réutilisable.
     - **Marquer l'unité comme manquante**: Définit l'unité comme manquante.
     - **Rendre l'unité compatible avec JBOD**: Ajoute l'unité dans l'agencement de disque JBOD.
     - **Rendre l'unité non configurée compatible**: Rend l'unité configurable en grappe ou utilisable comme unité de secours.
     - **Rendre l'unité non configurée non compatible**: Marque l'unité comme défectueuse, l'empêchant d'être utilisée en grappe ou comme unité de secours.
     - **Marquer l'unité comme étant prête pour le retrait**: Définit l'unité comme devant être retirée.
2. Si le contrôleur comporte des unités qui n'ont pas encore été configurées, elles seront affichées dans le tableau **Unités 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 : il est possible que XClarity Controller ne puisse pas détecter les propriétés de certaines unités.

Chapitre 7. Mise à jour du microprogramme de serveur

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

Présentation

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

L'option **Mise à jour du microprogramme** du panneau de navigation présente 4 caractéristiques :

- **Microprogramme du système :** présentation de l'état et de la version du microprogramme du système. Et pour effectuer la mise à jour du microprogramme du système.
- **Microprogramme de l'adaptateur :** présentation des microprogrammes d'adaptateur installés, de leur état et de leur version. Et pour effectuer la mise à jour du microprogramme de l'adaptateur.
- **Microprogramme du bloc d'alimentation :** présentation de la version du microprogramme du bloc d'alimentation. Et pour effectuer la mise à jour du microprogramme du bloc d'alimentation.
- **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.

Le statut et les versions en cours des microprogrammes des pilotes et des adaptateurs BMC, UEFI, LXPM, LXPM sont affichés, y compris les versions principale et de sauvegarde du BMC. Il existe quatre catégories de statut de microprogramme :

- **Actif :** le microprogramme est actif.
- **Inactif :** le microprogramme est inactif.
- **En attente :** le microprogramme est en instance de devenir actif.
- **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 étrange ou 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 de 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 73.

Mise à jour à partir du référentiel

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

Remarque : *La fonctionnalité d'historique de microprogramme CIFS/NFS/HTTPS/intégré nécessite une licence XCC Platinum*.

Présentation

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 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 (un appareil électronique) 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

Grâce à la **Mise à jour à partir du référentiel**, l'utilisateur peut configurer XCC pour synchroniser le microprogramme de serveur avec un référentiel de microprogramme CIFS/NFS distant. 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.

Il existe cinq états de 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.

Lorsque l'utilisateur clique sur **Arrêter la mise à jour**, les mises à jour placées en file d'attente sont annulées, et ce, dès la fin de la mise à jour du module d'installation en cours.

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

1. Cliquez sur **Connecter** pour vous connecter au référentiel distant après avoir entré les informations relatives à ce dernier.
2. Cliquez sur **Mettre à jour** pour démarrer la mise à jour par lot.
3. Cliquez sur **Afficher les détails** pour afficher l'état de mise à jour, soit 5 catégories d'état, comme indiqué ci-dessus.
4. 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.
5. Cliquez sur **Déconnecter** pour vous déconnecter du référentiel distant.
6. 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 73.

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.

Mise à jour avec Redfish

L'interface Redfish utilise un fichier de charge utile au format JSON pour faciliter la lecture par ses utilisateurs humains et l'écriture de scripts. XCC Redfish propose une API (SimpleUpdate) standard visant à extraire le fichier de lot de mises à jour à partir d'une URI via HTTP/HTTPS/SFTP/TFTP, ainsi qu'une mise à jour push HTTP Multipart pour envoyer l'UpdateService du fichier de lot de mises à jour. Vous pouvez utiliser une commande, ou un seul outil client Redfish afin d'effectuer des mises à jour de microprogramme et interroger l'état de la mise à jour.

Exemple de commande pour envoyer le fichier de lot vers XCC et générer la tâche en vue du transfert de fichier et de la vérification :

```
curl -s -k -u USERID:PASSW0RD-F 'UpdateParameters={"Targets":[]};type=application/json' -F
 'UpdateFile=@./NY7D72-IB-320.zip;type=application/octet-stream' https://10.240.218.157:443/mfwupdate
{
  "ld": "f2fd6e9d-cOa6-4b11-b9f6-69a17a1 ,
  "Name": "Task f2fd6e9d-cOa6-4b11-b9f6-69a17a1 e579c",
  "@odata.type": "#Task.v1_5_1. Task",
  "@odata.id': "[redfish/v 1 fTaskServicefTasks/f2fd6e9d-cOa6-4b11-b9f6-69a 17a1 e579c",
  "Messages": [l
  "Description": "This resource represents a task for a Redfish implementation."
  "StartTime": "2022-03-21 TOT 16:41 +00:00",
  "TaskMonitor": "/redfish/v1fTaskSen.'ice/c069ed4a-e754-4970-ab9a-922e8a3e076b",
  "@odata.context": "'redfish/v1/$metadata#Task.Task",
  "@odata.etag":
  "PercentCompIete": 0,
  "HidePayload": true,
  "TaskState": "New"
}
```

Exemple de commande pour que l'API réponde avec l'ID de tâche pour la mise à jour du microprogramme une fois le transfert et la validation d'image terminés :

```
https://10.240.218.157/
redfish/v1/TaskService/Tasks/f2fd6e9d c0a6 4b11 b9f6 69a17a1e579c
{
  "@odata.etag": ,
  "Name-: "Task f2fd6e9d-cOa6-4b11-b9f6-69a17a1e579c",
```

```
  Task",
  "IredfishNI/TaskSemcenasksff2fd6e9d-cOa6-4bI I-b9f6-69aI 7a1e579c",
  "Messages": [
    {
      "Resolution": "Follow the referenced job and monitor the job for further updates.",
    "@odata.type":
    'MessageSeverity": "OK",
    "MessageArgs": [
    "IredfishtvI/JobService/JObs/JObROOOOOI-lJPdate"
  ],
  "Messageld": "Update. 1 .O.OperationTransitionedToJob",
  "Message": "The update operation has transitioned to the job at URI 'Iredfsh/vl
 IJobService/Jobs/JobROOOOO1-Update'."
  }
  ],
  "Description": "This resource represents a task for a Redfish implementation.",
  "HidePayIoad": true,
  "StartTime":
  "TaskMonitor: "'redfish1v1/TaskseNice/cO69ed4a-e754-497O-ab9a-922e8a3eO76b",
  "TaskStatus": "OK",
  "@odata.context-: "'redfish/v1/$metadata#Task.Task",
  "ld": "f2fd6e9d-cOa6-4b11-b9f6-6ga17a 1 e579c",
  "Percentcomplete": 1OO,
  "EndTime": 2022-O3-21
  "TaskState": "Completed"
}
```


En interrogeant l'ID de tâche, XCC renvoie les étapes Tâche pour tous les modules de microprogramme dans le lot de mises à jour, comme indiqué ci-dessous :

https://10.240.218.157/redfish/v1/JobService/Jobs/JobR000001-Update


```
{
"@odata.etag": "\"1647847200776\"", "PercentComplete": 100, "@odata.type": "#Job.v1_0_7.Job",
"@odata.id": "/redfish/v1/JobService/Jobs/JobR000001-Update", "Messages": [
{
"Resolution": "None.",
"@odata.type": "#Message.v1_1_2.Message", "MessageSeverity": "OK",
"MessageArgs": [ "NY7D72-IB-320.zip",
"HardDiskDrive"
],
"MessageId": "Update.1.0.UpdateSuccessful ",
"Message": " Device 'HardDiskDrive' successfully updated with image 'NY7D72-IB-320.zip'."
},
{
"Resolution": "None.",
"@odata.type": "#Message.v1_1_2.Message", "MessageSeverity": "OK",
"MessageArgs": [ "NY7D72-IB-320.zip",
"/redfish/v1/UpdateService/FirmwareInventory/UEFI"
],
"MessageId": "Update.1.0.UpdateSuccessful",
"Message": "Device '/redfish/v1/UpdateService/FirmwareInventory/UEFI' successfully
 updated with image 'NY7D72-IB-320.zip'. "
},
{
"Resolution": "None.",
"@odata.type": "#Message.v1_1_2.Message", "MessageSeverity": "Critical",
"MessageArgs": [ "NY7D72-IB-320.zip",
"/redfish/v1/UpdateService/FirmwareInventory/BMC-Primary"
],
"MessageId": "Update.1.0.ApplyFailed",
"Message": "Installation of image 'NY7D72-IB-320.zip' to '/redfish/v1/UpdateService/FirmwareInventory/BMC-Primary' failed."
}
],
```

```
"Description": "This resource is used to represent a job for a Redfish implementation.",
"StartTime": "2022-03-21T07:16:58+00:00",
"Id": "JobR000001-Update",
"EndTime": "2022-03-21T07:20:00+00:00",
"@odata.context": "/redfish/v1/$metadata#Job.Job", "Steps": {
"@odata.id": "/redfish/v1/JobService/Jobs/JobR000001-Update/Steps"
},
"Name": "JobR000001-Update", "StepOrder": [
"lnvgy_fw_drives_all.samsung.pm1735.cq-cq37_anyos_comp.lvt", "lnvgy_fw_uefi_ese103a-1.00_anyos_comp.uxz",
 "lnvgy_fw_xcc_esx301p-0.01_anyos_comp.uxz"
],
"JobState": "Completed"
```


Lorsque l'étape Tâche est interrogée, XCC renvoie des informations supplémentaires aux mises à jour du microprogramme de manière individuelle :

https://10.240.218.157/redfish/v1/JobService/Jobs/JobR000001-Update/Steps/lnvgy_fw_drives_all.samsung.pm1735.cq-cq37_anyos_comp.lvt


```
{
"@odata.etag": "\"1647847202778\"", "PercentComplete": 1, "@odata.type": "#Job.v1_0_7.Job",
"@odata.id": "/redfish/v1/JobService/Jobs/JobR000001-Update/Steps/lnvgy_fw_drives_all.samsung.pm1735.cq-
 cq37_anyos_comp.lvt",
"Messages": [],
"Description": "This resource is used to represent a job for a Redfish implementation.", "StartTime":
 "2022-03-21T07:16:58+00:00",
"@odata.context": "/redfish/v1/$metadata#Job.Job",
"Id": "lnvgy_fw_drives_all.samsung.pm1735.cq-cq37_anyos_comp.lvt", "Name":
 "lnvgy_fw_drives_all.samsung.pm1735.cq-cq37_anyos_comp.lvt", "EndTime": "2022-03-21T07:20:02+00:00",

"JobState": "Completed"
```


Effectuez un téléchargement depuis un référentiel distant, puis effectuez la mise à jour, comme indiqué ci-dessous :

```
system> syncrep
syncrep [options] Launch firmware sync from remote repository options:
-t protocol to connect repository. The local type will reboot host immediately.
 (eg: syncrep -t samba -l url -u user -p password; syncrep -t local -l /bulk/bundle.tgz;
syncrep -t http -l http://IP/bundle.tgz)
-l location of remote repository (URL format)
-u User
-p Password
-o option (extra option string for samba and nfs mounts)
-d domain (domain for samba mount)
-q query current update status
-c cancel the sync process
-r <> firmware rollback
-gl get repository list
```

Chapitre 8. 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 courrier électronique.

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 105, « Retrait d'une clé d'activation » à la page 106 ou « Exportation d'une clé d'activation » à la page 106. 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 148.

Pour enregistrer un ID dans l'administration de votre licence XClarity Controller, cliquez sur le lien suivant : http://thinksystem.lenovofiles.com/help/index.jsp

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

Attention : Vous ne pouvez pas passer directement du niveau de fonctionnalité standard au niveau de fonctionnalité entreprise de XClarity Controller. Vous devez commencer par passer au niveau de fonctionnalité avancé avant de pouvoir activer le niveau de fonctionnalité entreprise.

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 ou sur **Annuler** pour interrompre l'installation. Pour finaliser l'ajout de la clé, cliquez sur **OK** dans la fenêtre d'ajout de clé d'activation ou cliquez sur **Annuler** pour arrêter l'installation.

La fenêtre Success indique que la clé d'activation est installée.

Remarques :

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

Etape 4. Cliquez sur **OK** pour fermer la fenêtre Success.

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 de confirmation de suppression de la clé, cliquez sur **OK** pour confirmer la suppression de la clé d'activation ou cliquez sur **Annuler** pour conserver le fichier de clés.
La clé d'activation sélectionnée est retirée du serveur et n'apparaît plus dans 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 l'exportation de la clé d'activation ou cliquez sur **Annuler** pour annuler la demande d'exportation de clé.

Etape 4. Sélectionnez le répertoire de sauvegarde du fichier.
La clé d'activation sélectionnée est exportée du serveur.

Chapitre 9. Gestion de groupe voisin

La gestion de groupe voisin de Lenovo XClarity Controller est un groupe de gestion virtuel pour les serveurs Lenovo ThinkSystem afin de gérer plusieurs serveurs sur un seul XCC.

Lenovo XClarity Controller (XCC) est un processeur de service intégré qui remplace l'habituel contrôleur de gestion de la carte mère (BMC) pour les serveurs Lenovo ThinkSystem. Des fonctions de configuration de serveur, de gestion et de moniteur sont alors mises en place.

Habituellement, XCC ne peut gérer qu'un seul serveur. Toutefois, Lenovo XClarity Administrator (LXCA), son logiciel de gestion centralisée, facilite la gestion de l'évolutivité sur plusieurs serveurs. Si LXCA n'est pas déployé dans la zone, en particulier pour les utilisateurs SMB, les nœuds doivent être configurés un par un. Ce processus est inefficace. Pour faire face à cette éventualité, la fonctionnalité de groupe voisin de XCC a été conçue pour créer un groupe de gestion virtuel dédié aux serveurs Lenovo ThinkSystem afin de gérer plusieurs serveurs à l'aide d'un seul XCC. Ceci permet tout simplement d'initier un déploiement rapide pour plusieurs serveurs dans le cadre d'un segment de réseau local.

Fonctionnalités prises en charge

Informations générales relatives aux fonctionnalités prises en charge par le groupe voisin.

Le **groupe voisin XCC** propose les fonctionnalités ci-après :

- Détection des nœuds voisins situés dans le même segment de réseau local.
- Surveillance de l'intégrité du système et de l'état d'alimentation des nœuds voisins.
- Configuration du groupe voisin dans le nœud principal.
- Clonage de la configuration système vers plusieurs membres du groupe voisin.
- Mise en route de mises à jour du microprogramme simultanées vers plusieurs membres du groupe voisin.
- Le nœud principal XCC prend en charge un maximum de 200 nœuds.

Serveurs ThinkSystem qui prennent en charge les fonctionnalités du groupe voisin XCC

Serveur	Type(s) de machine
ThinkSystem SR630 V3	7D72, 7D73
ThinkSystem SR650 V3	7D75, 7D76
Lenovo ThinkSystem ST650 V3	7D7A, 7D7B, 7D7C
Lenovo ThinkSystem SD650 V3	7D7M
Lenovo ThinkSystem SD650–I V3	7D7L
Lenovo ThinkSystem SR635 V3	7D9G, 7D9H
Lenovo ThinkSystem SR645 V3	7D9C,7D9D
Lenovo ThinkSystem SR655 V3	7D9E,7D9F
Lenovo ThinkSystem SR665 V3	7D9A, 7D9B
ThinkSystem SD665 V3	7D9P
ThinkSystem SR675 V3	7D9Q, 7D9R

Remarque : La fonctionnalité de groupe voisin XCC sera intégrée aux versions ultérieures des serveurs Lenovo ThinkSystem.

Détection de nœuds voisins

Les informations de cette rubrique vous indiquent comment détecter des nœuds voisins.

Chaque instance XCC détecte les serveurs voisins situés dans le même segment de réseau local à l'aide d'un message multidiffusion Simple Service Discovery Protocol (SSDP).

Les prérequis pour qu'un serveur puisse être détecté par une instance XCC sont les suivants :

1. Le port Simple Service Discovery Protocol (SSDP) 1900 doit être activé dans XCC (**Configuration BMC –> Réseau –> SSDP**).
2. La gestion de groupe voisin doit être activée (elle est désactivée par défaut).

La page Détection vous permet de surveiller les informations système, l'alimentation en temps réel et l'état d'intégrité de tous les nœuds détectés. La colonne **Dernière activité** indique l'horodatage de réception du dernier message SSDP des nœuds voisins. Cette information est régulièrement mise à jour, sauf si le nœud voisin est hors ligne, ou si le paramètre Gestion de groupe voisin/SSDP est désactivé.

Configuration de groupe voisin

Les informations de cette rubrique vous indiquent comment configurer un groupe voisin.

Vous pouvez trouver un groupe voisin à la page Web XCC en indiquant le nom du groupe.

Le nouveau nom de groupe doit être unique. Il ne doit pas exister dans le segment de réseau local.

Une fois qu'un nouveau groupe est créé :

- L'instance XCC en cours est automatiquement ajoutée à ce groupe.
- L'instance XCC actuelle devient le nœud principal du nouveau groupe voisin XCC.
- Toutes les autres instances XCC du même segment de réseau local sont immédiatement notifiées. La page Web de détection de voisins XCC de chaque serveur est alors mise à jour.
- Le nœud principal d'un groupe peut sélectionner un serveur voisin, ou plusieurs serveurs voisins en vue de rejoindre le groupe en spécifiant les données d'identification d'administrateur XCC du serveur voisin.
- Une fois que le ou les nœuds voisins vérifient avec succès les données d'identification de l'utilisateur, ils acceptent la demande du nœud principal. Ils rejoignent ensuite ce groupe en tant que nouveaux membres.

Approvisionnement de groupe voisin

Les informations de cette rubrique vous indiquent comment approvisionner des groupes voisins.

L'approvisionnement de groupe voisin est une fonctionnalité visant à distribuer la configuration à plusieurs membres du groupe. Cette dernière comprend la **configuration de clone** et la **mise à jour à partir du référentiel.**

La **configuration de clone** sert à propager la configuration du système XCC actuel aux membres sélectionnés du même type de machine. La configuration qui fait l'objet d'un clonage comprend :

1. Configuration du serveur : options d'amorçage, stratégie d'alimentation, propriétés du serveur.
2. Configuration BMC : réseau (à l'exception de l'adresse IP et des paramètres associés), sécurité, utilisateur/LDAP (dont les comptes utilisateur et les mots de passe), appel vers Lenovo.

La **mise à jour à partir du référentiel** débute la mise à jour du microprogramme simultanément pour certains membres en spécifiant un référentiel de microprogramme partagé par le biais des protocoles CIFS ou Network File System (NFS). La mise à jour du microprogramme peut être appliquée à plusieurs types de machine à la fois, tant que les images du microprogramme applicables sont disponibles dans le référentiel partagé.

Une fois la mise à jour du microprogramme du groupe voisin en cours, sa progression peut être consultée dans les colonnes État et Détails.

Chapitre 10. API REST REDFISH de Lenovo XClarity Controller

Le Lenovo XClarity Controller fournit un ensemble d'API REST simples d'utilisation et compatibles avec Redfish qui permettent d'accéder aux données et services de Lenovo XClarity Controller depuis des applications s'exécutant à l'extérieur de l'infrastructure de Lenovo XClarity Controller.

Il est ainsi facile d'intégrer des fonctions Lenovo XClarity Controller à d'autres logiciels, que le logiciel s'exécute sur le même système que le serveur Lenovo XClarity Controller ou sur un système distant au sein du même réseau. Ces API reposent sur les API REST Redfish standards et sont accessibles via le protocole HTTPS.

Le guide d'utilisation de l'API REST Redfish de XClarity Controller est disponible à cet emplacement : https://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.restapi.doc/xcc_restapi_book.pdf.

Lenovo fournit un exemple de scripts Redfish open source qui peuvent être utilisés en tant que référence pour le développement de logiciels qui communiquent avec l'API REST Redfish de Lenovo. Ces exemples de scripts peuvent être consultés ici :

- Python : https://github.com/lenovo/python-redfish-lenovo
- PowerShell : https://github.com/lenovo/powershell-redfish-lenovo

Les spécifications DMTF relatives à l'API Redfish sont disponibles à l'emplacement suivant : https://redfish.dmtf.org/. Ce site Web fournit des spécifications générales et d'autres documents de référence sur l'API REST Redfish.

Chapitre 11. 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 113 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.

Vous êtes connecté à la ligne de commande. 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 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 Echap, puis entrez une parenthèse gauche. L'invite CLI s'affiche pour indiquer le retour à l'interface de ligne de commande IMM.

```
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 sur 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> ?
  ```
- Sur un système Flex System, certains paramètres sont gérés par le module CMM et ne peuvent pas être modifiés dans XClarity Controller.

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 :

- « Commande accseccfg » à la page 132
- « Commande adapter » à la page 200
- « Commande alertcfg » à la page 134
- « Commande alertentries » à la page 181

- « Commande asu » à la page 134
- « Commande backup » à la page 137
- « Commande batch » à la page 184
- « Commande chconfig » à la page 187
- « Commande chlog » à la page 189
- « Commande chmanual » à la page 189
- « Commande clearcfg » à la page 184
- « Commande clearlog » à la page 118
- « Commande clock » à la page 185
- « Commande console » à la page 132
- « Commande dbgshimm » à la page 203
- « Commande dhcpinfo » à la page 138
- « Commande dns » à la page 139
- « Commande encaps » à la page 141
- « Commande ethtousb » à la page 141
- « Commande exit » à la page 117
- « Commande fans » à la page 119
- « Commande ffdc » à la page 119
- « Commande firewall » à la page 142
- « Commande fuelg » à la page 130
- « Commande gprofile » à la page 143
- « Commande hashpw » à la page 144
- « Commande help » à la page 117
- « Commande history » à la page 118
- « Commande hreport » à la page 121
- « Commande identify » à la page 185
- « Commande ifconfig » à la page 145
- « Commande info » à la page 186
- « Commande keycfg » à la page 148
- « Commande ldap » à la page 149
- « Commande led » à la page 122
- « Commande mhlog » à la page 121
- « Commande mvstor » à la page 202
- « Commande ntp » à la page 151
- « Commande portcfg » à la page 152
- « Commande portcontrol » à la page 153
- « Commande ports » à la page 154
- « Commande power » à la page 127
- « Commande pxeboot » à la page 131
- « Commande rdmount » à la page 155
- « Commande readlog » à la page 124

- « Commande reset » à la page 129
- « Commande restore » à la page 155
- « Commande restoredefaults » à la page 156
- « Commande roles » à la page 157
- « Commande seccfg » à la page 158
- « Commande set » à la page 158
- « Commande smtp » à la page 158
- « Commande snmp » à la page 159
- « Commande snmpalerts » à la page 161
- « Commande spreset » à la page 186
- « Commande srcfg » à la page 163
- « Commande sshcfg » à la page 164
- « Commande ssl » à la page 165
- « Commande sslcfg » à la page 166
- « Commande storage » à la page 190
- « Commande storekeycfg » à la page 170
- « Commande syncrep » à la page 171
- « Commande syshealth » à la page 125
- « Commande temps » à la page 125
- « Commande thermal » à la page 172
- « Commande timeouts » à la page 173
- « Commande tls » à la page 173
- « Commande trespass » à la page 174
- « commande trespass » à la page 175
- « Commande usbeth » à la page 176
- « Commande usbfp » à la page 176
- « Commande users » à la page 176
- « Commande volts » à la page 126
- « Commande vpd » à la page 127

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 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.

Le tableau suivant présente les arguments pour les options.

Tableau 7. Commande clearlog

Le tableau suivant, à une ligne et deux colonnes, comporte les options et leurs descriptions.

Option	Description
-t <all | platform | audit>	Type d'événement ; choisissez le type d’événement à effacer. Si rien n'est spécifié, tous les types d'événement sont sélectionnés.

Descriptions de type d'événement

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

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 ffdc

Cette commande permet de générer un nouveau fichier de données de maintenance.

Utilisez la commande **ffdc** (capture de données à la première défaillance) pour générer et transférer les données de maintenance au support Lenovo.

La liste suivante montre les commandes pouvant être utilisées avec la commande **ffdc** :

- **generate**, pour créer un nouveau fichier de données de maintenance
- **status**, pour vérifier l'état du fichier de données de maintenance
- **copy**, pour copier les données de maintenance existantes
- **delete**, pour supprimer les données de maintenance existantes

Le tableau suivant présente les arguments pour les options.

Tableau 8. Commande ffdc

Le tableau suivant, à plusieurs lignes et trois colonnes, comporte les options, les descriptions d'option, ainsi que les valeurs associées pour les options.

Tableau 8. Commande ffdc (suite)

Option	Description	Valeurs
-t	Numéro type	1 (cliché de processeur) et 4 (données de maintenance). Le vidage de processeur contient tous les journaux et les fichiers disponibles. Les données de maintenance contiennent uniquement un sous-ensemble des journaux et des fichiers. La valeur par défaut est 1.
-f [1]	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 [1]	Adresse du serveur tftp/sftp	
-pn [1]	Numéro de port du serveur tftp/sftp	La valeur par défaut est 69/22.
-u [1]	Nom d'utilisateur du serveur sftp	
-pw [1]	Mot de passe du serveur sftp	

1. Argument supplémentaire pour les commandes **generate** et **copy**

Syntaxe :

```
ffdc [options]
option:
  -t 1 or 4
  -f
  -ip ip_address
  -pn port_number
  -u username
  -pw password
```

Exemple :

```
system> ffdc generate
Generating ffdc...
system> ffdc status
Type 1 ffdc: in progress
system> ffdc copy -t 1 -ip 192.168.70.230 -u User2 -pw Passw0rd -f /tmp/
Waiting for ffdc.....
Copying ffdc...
ok
system> ffdc status
Type 1 ffdc: completed
8737AC1_DSY0123_xcc_120317-153327.tgz


system> ffdc generate
Generating ffdc...
system> ffdc status
Type 1 ffdc: in progress
system> ffdc status
Type 1 ffdc: in progress
system> ffdc copy -ip 192.168.70.230
Copying ffdc...
ok
system> ffdc status
Type 1 ffdc: completed
8737AC1_DSY0123_xcc_120926-105320.tgz
```

```
system>
```

Commande hreport

Utilisez cette commande pour afficher le rapport d'intégrité intégré.

Le tableau suivant présente les commandes hreport.

Tableau 9. commandes hreport

Le tableau suivant, à plusieurs lignes et deux colonnes, comporte les descriptions des différentes commandes hreport.

Option	Description
générer	Créer un nouveau rapport d'intégrité
état	Vérifier l'état
copier	Copier le rapport d'intégrité existant
supprimer	Supprimer le rapport d'intégrité existant

Le tableau suivant affiche les arguments des options generate et copy.

Tableau 10. commande generate et copy

Le tableau suivant, à plusieurs lignes et deux colonnes, comporte les options des commandes generate et copy et leurs descriptions.

Option	Description
-f	Répertoire cible sftp ou nom de fichier distant (par défaut, un nom généré par le système (pour sftp, utilisez le chemin complet ou un/de fin après le nom du répertoire (~/ ou /tmp/))
-ip	Adresse du serveur tftp/sftp
-pn	Numéro de port du serveur tftp/sftp (69/22 par défaut)
-u	Nom d'utilisateur du serveur sftp
-pw	Mot de passe du serveur sftp

Commande mhlog

Utilisez cette commande pour afficher les entrées du journal d'activité de l'historique de maintenance.

Le tableau suivant présente les arguments pour les options.

Tableau 11. Commande mhlog

Le tableau suivant, à plusieurs lignes et deux colonnes, comporte les options et leurs descriptions.

Option	Description
-c <nombre>	Afficher le « nombre » d'entrées (1-250)
-i <index>	Afficher les entrées à partir de l'index (1-250)
-f	Nom de fichier distant du fichier journal

Tableau 11. Commande mhlog (suite)

Option	Description
-ip	Adresse du serveur tftp/sftp
-pn	Numéro de port du serveur tftp/sftp (69/22 par défaut)
-u	Nom d'utilisateur du serveur sftp
-pw	Mot de passe du serveur sftp

Exemple

L'affichage ressemble à ce qui suit :

```
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
```

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.

Tableau 12. commande led

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
-l	Obtenir l'état de tous les voyants du système et de ses sous-composants	
-chklog	Désactiver le voyant de vérification des journaux	off
-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)

Syntaxe :

```
led [options]
option:
  -l
  -chklog off
```

-identify *state*
-d *time*

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.

readlog affiche les cinq premières entrées dans le journal des événements, en commençant par la plus récente, à sa première exécution, et les cinq suivantes à chaque appel ultérieur.

readlog -a affiche toutes les entrées dans le journal des événements, en commençant par les plus récentes.

readlog -f réinitialise le compteur et affiche les 5 premières entrées dans le journal des événements, en commençant par la plus récente.

readlog -date *date* affiche les entrées du journal des événements pour la date indiquée au format mm/jj/aa. Il peut s'agir d'une liste de dates séparées par des barres verticales (|).

readlog -sev *gravité* affiche les entrées du journal des événements pour le niveau de gravité indiqué (E, W, I). Il peut s'agir d'une liste de niveaux de gravité séparés par des barres verticales (|).

readlog -i *ip_address* définit l'adresse IP IPv4 ou IPv6 du serveur TFTP ou SFTP où le journal des événements est sauvegardé. Les options de commande **-i** et **-l** sont utilisées conjointement pour indiquer l'emplacement.

readlog -l *nom_fichier* définit le nom du fichier contenant le journal des événements. Les options de commande **-i** et **-l** sont utilisées conjointement pour indiquer l'emplacement.

readlog -pn *port_number* affiche ou définit le numéro de port du serveur TFTP ou SFTP (69/22 par défaut).

readlog -u *nom_utilisateur* indique le nom d'utilisateur du serveur SFTP.

readlog -pw *mot_de_passe* indique le mot de passe du serveur SFTP.

Syntaxe :

```
readlog [options]
option:
  -a
  -f
  -date date
  -sev severity
  -i ip_address
  -l filename
  -pn port_number
  -u username
  -pw password
```

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 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 (inclut 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 [argument]
argument:
  summary      -display the system health summary
  activeevents -display active events
  cooling - display cooling devices health status
  power - display power modules health status
  storage - display local storage health status
  processors - display processors health status
  memory - display memory health status
```

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.

```
Example
system> temps
Temperatures are displayed in degrees Fahrenheit/Celsius

         WR       W       T       SS      HS
-------------------------------------------------
CPU1     N/A     N/A    80/27    N/A     N/A
CPU2     N/A     N/A    80/27    N/A     N/A
DASD1   66/19   73/23   82/28   88/31   92/33
Amb     59/15   70/21   83/28   90/32   95/35
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.

```
Example:
system> volts

      i HSL    SSL    WL     WRL    V      WRH    WH    SSH    HSH
-------------------------------------------------------------------
5v     5.02   4.00   4.15   4.50   4.60   5.25   5.50   5.75   6.00
3.3v   3.35   2.80   2.95   3.05   3.10   3.50   3.65   3.70   3.85
12v   12.25  11.10  11.30  11.50  11.85  12.15  12.25  12.40  12.65
-5v   -5.10  -5.85  -5.65  -5.40  -5.20  -4.85  -4.65  -4.40  -4.20
-3.3v -3.35  -4.10  -3.95  -3.65  -3.50  -3.10  -2.95  -2.80  -2.70
VRM1                              3.45
VRM2                              5.45
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.

Exemple :
```
vpd sys  - displays Vital Product Data for the system
vpd bmc  - displays Vital Product Data for the management controller
vpd uefi - displays Vital Product Data for system BIOS
vpd lxpm  - displays Vital Product Data for system LXPM
vpd fw   - displays Vital Product Data for the system firmware
vpd comp - displays Vital Product Data for the system components
vpd pmem - displays Vital Product Data for Intel Optane PMem
vpd pcie - displays Vital Product Data for PCIe devices
```

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).

Le tableau suivant contient un sous-ensemble de commandes pouvant être utilisées avec la commande **power**.

Tableau 13. Commande power

Le tableau suivant, à plusieurs lignes et trois colonnes, comporte les commandes d'alimentation, les descriptions de commande, ainsi que les valeurs associées pour les commandes.

Tableau 13. Commande power (suite)

Commande	Description	Valeur
mise sous tension	Utilisez cette commande pour mettre le serveur sous tension.	on, off
mise hors tension	Utilisez cette commande pour mettre le serveur hors tension. **Remarque :** L'option **-s** arrête le système d'exploitation avant la mise hors tension du serveur.	on, off
power cycle	Utilisez cette commande pour mettre le serveur hors puis sous tension. **Remarque :** L'option **-s** arrête le système d'exploitation avant la mise hors tension du serveur.	
power enterS3	Utilisez cette commande pour placer le système d'exploitation en mode S3 (mise en veille). **Remarque :** Cette commande est utilisée uniquement lorsque le système est sous tension. Le mode S3 n'est pas pris en charge sur tous les serveurs.	
power rp	Utilisez cette option pour spécifier la stratégie de restauration de l'alimentation hôte.	alwayson|alwaysoff|restore
power S3resume	Utilisez cette commande pour sortir le système d'exploitation du mode S3 (mise en veille). **Remarque :** Cette commande est utilisée uniquement lorsque le système est sous tension. Le mode S3 n'est pas pris en charge sur tous les serveurs.	
power state	Utilisez cette commande pour afficher l'état d'alimentation du système, ainsi que l'état en cours du serveur.	on, off

Le tableau suivant répertorie les options des commandes **power on**, **power off** et **power cycle**.

Tableau 14. Commande power

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
-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.	**Remarque :** Les valeurs de cette option sont présentées sur des lignes distinctes en raison de limitations d'espace. Sun|Mon|Tue|Wed|Thu| Fri|Sat|Day|clear
-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

Tableau 14. Commande power (suite)

Option	Description	Valeurs
-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**.	

Syntaxe :
```
power on
power off [-s]
power state
power cycle [-s]
```

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 13:00
```

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.

Le tableau suivant présente les arguments pour les options.

Tableau 15. Commande reset

Le tableau suivant, à plusieurs lignes et trois colonnes, comporte les options, les descriptions d'option, ainsi que les valeurs associées pour les options.

Tableau 15. Commande reset (suite)

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.	

Syntaxe :
```
reset [option]
option:
-s
-d
-nmi
```

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. Le tableau suivant présente les arguments pour les options.

Tableau 16. Commande fuelg

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
-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.	input, output
-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
-period	Une valeur numérique pour afficher l'historique (1, 6, 12, 24 heures)	valeur numérique en 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) • **ort**- redondant N_1 avec régulation
-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

Tableau 16. Commande fuelg (suite)

Option	Description	Valeurs
-perf	Afficher l'utilisation de l'ordinateur actuelle, y compris le système, le microprocesseur et les E-S.	pourcentage
-pc	Afficher la consommation électrique actuelle	• **output**- Afficher la consommation d'énergie actuelle en CC. Pour les serveurs en armoire et au format tour, ceci inclut la consommation d'énergie du système, de l'unité centrale, de la mémoire et des autres composants. Pour les serveurs lame ITE, ceci inclut uniquement la consommation d'énergie du système. • **input**- Afficher la consommation d'énergie actuelle, y compris la consommation d'énergie du système.

Syntaxe :
```
fuelg [options]
option:
  -pme on|off
  -pcapmode input|output
  -pcap
  -history
  -period
  -pm bt|r|rt
  -zm on|off
  -perf
  -pc input|output
```

Exemple :
```
system> fuelg
-pme: on
system>
```

Commande pxeboot

Cette commande permet d'afficher et de définir la condition du PXE (Preboot eXecution Environment).

L'exécution de **pxeboot** sans option renvoie les paramètres actuels du Preboot eXecution Environment. Le tableau suivant présente les arguments pour les options.

Tableau 17. Commande pxeboot

Le tableau suivant, à une seule ligne et trois colonnes, comporte l'option, la description d'option, ainsi que les valeurs associées pour l'option.

Option	Description	Valeurs
-en	Définit la condition du Preboot eXecution Environment pour le prochain redémarrage du système.	enabled, disabled

Syntaxe :
```
pxeboot [options]
option:
  -en state
```

Exemple :
```
system> pxeboot
-en disabled
system>
```

Commande Serial redirect

Cette rubrique décrit la commande Serial redirect.

Une seule commande Serial redirect est disponible : la « Commande console » à la page 132.

Commande console

Cette commande permet de démarrer une session de console de redirection.

Utilisez la commande **console** pour lancer un session console de redirection série vers le port série IMM désigné.

Syntaxe :
```
console 1
```

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.

L'exécution de la commande **accseccfg** sans option affiche toutes les informations de sécurité des comptes. Le tableau suivant présente les arguments pour les options.

Tableau 18. Commande accseccfg

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
-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

Tableau 18. Commande accseccfg (suite)

Option	Description	Valeurs
-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

Syntax:

```
accseccfg [options]
option:
   -legacy
   -high
   -custom
   -am authentication methoc
   -lp lockout_period
   -pe time_period
   -pr state
   -pc state
   -pd number_characters
   -pl number_characters
   -ci minimum_interval
   -lf number_failures
   -chgnew state
   -rc reuse_cycle
   -wt timeout
```

Exemple :

```
system> accseccfg
-legacy
-am local
-lp 2
-pe 0
-pr off
-pd 1
```

```
-pl 4
-ci 0
-lf 0
-chgnew off
-rc 0
-wt user
system>
```

Commande alertcfg

Utilisez cette commande pour afficher et configurer les paramètres d'alerte à distance IMM globaux.

L'exécution de la commande **alertcfg** sans option affiche tous les paramètres d'alerte à distance globaux. Le tableau suivant présente les arguments pour les options.

Tableau 19. Commande alertcfg

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
-dr	Définit le temps d'attente entre deux tentatives avant que le module IMM renvoie une alerte.	0 à 4,0 minutes, par incréments de 0,5 minute
-da	Définit le temps d'attente avant que le module IMM envoie une alerte au prochain destinataire de la liste.	0 à 4,0 minutes, par incréments de 0,5 minute
-rl	Définit combien de fois le module IMM tentera d'envoyer un alerte, si les tentatives précédentes ont échoué.	0 à 8

Syntaxe :

```
alertcfg [options]
  options:
    -rl retry_limit
    -dr retry_delay
    -da agent_delay
```

Exemple :

```
system>alertcfg
-dr 1.0
-da 2.5
-rl 5
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.

Le tableau suivant contient un sous-ensemble de commandes pouvant être utilisé avec la commande **asu**.

Tableau 20. Commande asu

Le tableau suivant, à plusieurs lignes et trois colonnes, comporte un sous-ensemble des commandes pouvant être utilisées conjointement avec la commande **asu**. Les informations descriptives et les valeurs associées aux commandes sont fournies.

Commande	Description	Valeur
supprimer	Utilisez cette commande pour supprimer une instance ou un enregistrement de paramètre. Le paramètre doit être une instance qui autorise la suppression, par exemple, iSCSI.AttemptName.1.	*setting_instance*
aide	Utilisez cette commande pour afficher des informations d'aide pour un ou plusieurs paramètres.	*paramètre*
définir	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. »	*valeur de paramètre*
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.	*paramètre*
show	Utilisez cette commande pour afficher la valeur actuelle d'un ou plusieurs paramètres.	*paramètre*
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.	*paramètre*

Remarques :

- Dans la syntaxe de commande, *paramètre* est le nom d'un paramètre que vous souhaitez afficher ou modifier, et *valeur* est la valeur que vous placez sur le paramètre.
- *Paramètre* peut contenir plus d'un nom, sauf lorsque vous utilisez la commande **set**.
- *Paramètre* peut contenir des caractères génériques, par exemple, un astérisque (*) ou un point d'interrogation (?)
- *Paramètre* peut être un groupe, un nom de paramètre ou **all**.

Liste d'exemples de syntaxe pour la commande **asu** :

- Pour afficher toutes les options de commande asu, entrez `asu --help`.
- Pour afficher l'aide détaillée pour toutes les commandes, entrez `asu -v --help`.
- Pour afficher l'aide détaillée pour une commande, entrez `asu -v set --help`.
- Pour modifier une valeur, entrez `asu set` *setting value*.
- Pour afficher la valeur en cours, entrez `asu show` *setting*.
- Pour afficher les paramètres au format long par lots, entrez `asu show -l -b all`
- Pour afficher toutes les valeurs possibles pour un paramètre, entrez `asu showvalues` *setting*. 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>
```

Le tableau suivant présente les arguments pour les options.

Tableau 21. 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**.	
--help[1]	Afficher l'aide pour la commande. L'option --help est placée après la commande, par exemple **asu show --help**.	
-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 22. 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.

Le tableau suivant présente les arguments pour les options.

Tableau 23. Commande backup

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
-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
-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

Syntaxe :

```
backup [options]
  option:
   -f    filename
   -pp   password
   -ip   ip address
   -pn   port number
   -u    username
   -pw   password
   -fd   filename
```

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 eth0
```

```
Example:
system> dhcpinfo eth0
   -server :  10.240.0.10
   -n      :  XCC-7X19-123456789A
   -i      :  10.243.4.66
   -i6     :  ::
   -g      :  10.243.0.1
   -s      :  255.255.240.0
   -d      :  labs.lenovo.com
   -d6     :
   -dns1   :  10.240.0.10
   -dns2   :  10.240.0.11
   -dns3   :  0.0.0.0
   -dns61  :  ::
   -dns62  :  ::
   -dns63  :  ::
```

Le tableau suivant décrit la sortie de cet exemple.

Tableau 24. Commande dhcpinfo

Le tableau suivant, à plusieurs lignes et deux colonnes, décrit les options qui sont utilisées dans l'exemple précédent.

Option	Description
-server	Serveur DHCP ayant affecté la configuration
-n	Nom d'hôte affecté
-i	Adresse IPv4 affectée
-g	Adresse de passerelle affectée
-s	Masque de sous-réseau affecté
-d	Nom de domaine 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
-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.

Remarque : Sur un système Flex System, les paramètres DNS ne peuvent pas être modifiés sur le module IMM. Les paramètres DNS sont gérés par le module CMM.

L'exécution de la commande **dns** sans option affiche toute l'information sur la configuration DNS. Le tableau suivant présente les arguments pour les options.

Tableau 25. Commande dns

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
-state	État du DNS	on, off
-ddns	État du DDNS	enabled, disabled
-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.
-p	Priorité IPv4/IPv6	ipv4, ipv6

Syntaxe :
```
dns [options]
option:
  -state state
  -ddns state
  -i1 first_ipv4_ip_address
  -i2 second_ipv4_ip_address
  -i3 third_ipv4_ip_address
  -i61 first_ipv6_ip_address
  -i62 second_ipv6_ip_address
  -i63 third_ipv6_ip_address
  -p priority
```

Remarque : L'exemple suivant présente une configuration IMM où DNS est désactivé.

Exemple :
```
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>
```
Le tableau suivant décrit les options utilisées dans l'exemple précédent.

Tableau 26. sortie de la commande dns

Le tableau suivant, à plusieurs lignes et deux colonnes, décrit les options qui sont utilisées dans l'exemple précédent.

Option	Description
-state	État du DNS (`on` ou `off`)
-i1	Adresse IP du serveur DNS IPv4 principal
-i2	Adresse IP du serveur DNS IPv4 secondaire
-i3	Adresse IP du serveur DNS IPv4 tertiaire
-i61	Adresse IP du serveur DNS IPv6 principal
-i62	Adresse IP du serveur DNS IPv6 secondaire
-i63	Adresse IP du serveur DNS IPv6 tertiaire
-ddns	État du DDNS (`enabled` ou `disabled`)
-dnsrc	Nom de domaine DDNS préféré (`dhcp` ou `manual`)
-ddn	DDN spécifié manuellement
-ddncur	DDN en cours (lecture seule)
-p	Serveurs DNS préférés (`ipv4` ou `ipv6`)

Commande encaps

Utilisez cette commande pour que le contrôleur BMC quitte le mode d'encapsulation.

Le tableau suivant présente les arguments pour les options.

Tableau 27. commande encaps

Le tableau suivant, à une ligne et deux colonnes, comporte les options et leurs descriptions.

Option	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.

L'exécution de la commande **ethtousb** sans option affiche des informations sur Ethernet-via-USB. Le tableau suivant présente les arguments pour les options.

Tableau 28. Commande ethtousb

Le tableau suivant, à plusieurs lignes et trois colonnes, comporte les options, les descriptions d'option, ainsi que les valeurs associées pour les options.

Tableau 28. Commande ethtousb (suite)

Option	Description	Valeurs
-en	État de Ethernet-via-USB	enabled, disabled
-m*x*	Configurer le mappage de port pour l'index *x*	Paire de ports, séparés par deux points (:), au format *port1:port2* 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	Supprimer le mappage de port pour l'index indiqué	1 à 10 Les index de mappage de port sont affichés à l'aide de la commande **ethtousb** sans option.

Syntaxe :
```
ethtousb [options]
option:
  -en state
  -mxport_pair
  -rm map_index
```

Exemple :
```
system> ethtousb  -en enabled -m1 100:200 -m2 101:201
system> ethtousb
 -en enabled
 -m1 100:200
 -m2 101:201
system> ethtousb -rm 1
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.

Le tableau suivant présente les arguments pour les options.

Tableau 29. Commande firewall

Le tableau suivant, à plusieurs lignes et trois colonnes, comporte les options et leurs descriptions.

Option	Description	Valeurs
-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.
-bbd	Bloquer la date de début	Date au format <AAAA-MM-JJ>

Tableau 29. Commande firewall (suite)

Option	Description	Valeurs
-bed	Bloquer la date de fin	Date au format <AAAA-MM-JJ>
-bbt	Bloquer l'heure de début	Heure au format <HH:MM>
-bet	Bloquer l'heure de fin	Heure au format <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
-iplf	Nombre maximum d'échecs de connexion avant le verrouillage de l'adresse IP. **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>*	Valeur numérique comprise entre 0 et 32, 0 = aucun verrouillage
-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

Exemple :

```
· “firewall”: Show all options’ value and IP addresses blocking list.
· “firewall -bips  192.168.1.1,192.168.1.0/24,192.168.1.1-192.168.1.5”: Block the access from multi IPs
· “firewall -bti 01:00-02:00,05:05-10:30,14:15-20:00”: Block all access during 01:00-02:00,05:05-10:30,14:15-20:00 every day.
· “firewall –clr all”: Clear all rules of “Block List and Time Restriction”.
· “firewall -iplp 60”:Set IP address lockout period to 60 minutes.
· “firewall -iplf 5”:Set maximum number of login failures to 5 timesi.
· “firewall -ipbl -del 192.168.100.1”:Delete 192.168.100.1 from IP address blocking list.
· “firewall –ipbl -del 3fcc:1234::2”:Delete 3fcc:1234::2 from IP address blocking list.
· “firewall –ipbl –clrall”:  Delete all blocking IP addresses.
· “firewall –ipbl –show”:    Show all blocking IP addresses.
```

Commande gprofile

Utilisez cette commande pour afficher et configurer les profils de groupe pour le module IMM.

Le tableau suivant présente les arguments pour les options.

Tableau 30. Commande gprofile

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
-clear	Suppression d'un groupe	enabled, disabled
-n	Nom du groupe	Chaîne pouvant comprendre jusqu'à 63 caractères pour *nom_groupe*. *Nom_groupe* doit être unique.
-a	Niveau d'autorisation basé sur les rôles	supervisor, operator, rbs <role list>: nsc|am|rca|rcvma|pr|bc|cel|ac Les valeurs de la liste de rôles doivent être spécifiées en les séparant par une barre verticale.
-h	Permet d'afficher l'utilisation de la commande et ses options	

Syntaxe :

```
gprofile [1 - 16 group_profile_slot_number] [options]
options:
-clear state
-n  group_name
-a  authority level:
    -nsc network and security
    -am user account management
    -rca remote console access
    -rcvma remote console and remote disk access
    -pr remote server power/restart access
    -bc basic adapter configuration
    -cel ability to clear event logs
    -ac advanced adapter configuration
-h help
```

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.

Le tableau suivant présente les arguments pour les options.

Tableau 31. Commande hashpw

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
-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.

Entrez `ifconfig eth0` 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.

Remarque : Sur un système Flex System, les paramètres VLAN sont gérés par un module CMM Flex System et ne peuvent pas être modifiés sur le module IMM.

Le tableau suivant présente les arguments pour les options.

Tableau 32. Commande ifconfig

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	Adresse MAC gravée (en lecture seule et non configurable)	
-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)
-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.
-r	Vitesse de transfert	10, 100, auto
-d	Mode duplex	full, half, auto
-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).
-dn	Nom de domaine	Nom de domaine avec format valide.
-auto	Paramètre de négociation automatique qui détermine si les paramètres réseau Data rate et Duplex sont configurables	true, false

Tableau 32. Commande ifconfig (suite)

Option	Description	Valeurs
-ghn	Obtenir le nom d'hôte auprès de DHCP	disabled, enabled
-nic	Changer le mode de la carte d'interface réseau (NIC)[1]	shared, dedicated, shared:nixX[2]
-failover[2]	Mode de basculement	none, shared, shared:nicX
-nssync[3]	Synchronisation des paramètres réseau	enabled, disabled
-address_table	Table des adresses IPv6 générées automatiquement et de leurs longueurs de préfixes **Remarque :** Cette option n'est visible que si IPv6 et la configuration automatique sans état sont activés.	Cette valeur est en lecture seule et n'est pas configurable.
-ipv6	État IPv6	disabled, enabled
-lla	Adresse lien-local **Remarque :** L'adresse lien-local n'apparaît que si IPv6 est activé.	L'adresse lien-local est déterminée par le module IMM. Cette valeur est en lecture seule et n'est pas configurable.
-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	État DHCPv6	enabled, disabled
-sa6	État de configuration automatique IPv6 sans état	enabled, disabled
-vlan	Activer ou désactiver le marquage VLAN	enabled, disabled
-vlanid	Balise d'identification de paquet réseau pour le module IMM	Valeur numérique comprise entre 1 et 4094.

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:nicX 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.

Syntaxe :

```
ifconfig eth0 [options]
options:

  -state interface_state
  -c config_method
  -i static_ipv4_ip_address
  -g ipv4_gateway_address
  -s subnet_mask
  -n hostname
  -r data_rate
  -d duplex_mode
  -m max_transmission_unit
  -l locally_administered_MAC
  -b burned_in_MAC_address
  -dn domain_name
  -auto state
  -nic state
  -failover mode
  -nssync state
  -address_table
  -lla ipv6_link_local_addr
  -dhcp6 state
  -ipv6 state
  -ipv6static state
  -sa6 state
  -i6 static_ipv6_ip_address
  -g6 ipv6_gateway_address
  -p6 length
  -vlan state
  -vlanid VLAN ID
```

Exemple :

```
system> ifconfig eth0
-state    :   enabled
-c        :   dthens
-ghn      :   disabled
-i        :   192.168.70.125
-g        :   0.0.0.0
-s        :   255.255.255.0
-n        :   IMM00096B9E003A
-auto     :   true
-r        :   auto
-d        :   auto
-vlan     :   disabled
-vlanid   :   1
-m        :   1500
-b        :   00:09:6B:9E:00:3A
-l        :   00:00:00:00:00:00
-dn       :
-ipv6     :   enabled
-ipv6static :  disabled
-i6       :   ::
-p6       :   64
-g6       :   ::
-dhcp6    :   enabled
-sa6      :   enabled
-lla      :   fe80::6eae:8bff:fe23:91ae
-nic :  shared:nic3
       nic1: dedicate
       nic2: ext card slot #3
```

```
      nic3: ext card slot #5  [active]
-address_table    :

system> ifconfig eth0 -c static -i 192.168.70.133
These configuration changes will become active after the next reset of the IMM.
```

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 :

- 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.
- 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.

Le tableau suivant présente les arguments pour les options.

Tableau 33. Commande keycfg

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
-add	Ajouter une clé d'activation	Valeurs des options de commandes -ip, -pn, -u, -pw et -f
-ip	Adresse IP du serveur TFTP avec clé d'activation à ajouter	Adresse IP valide du serveur TFTP
-pn	Numéro de port du serveur TFTP/SFTP avec clé d'activation à ajouter	Numéro de port valide du serveur TFTP/SFTP (69/22 par défaut)
-u	Nom d'utilisateur du serveur SFTP avec clé d'activation à ajouter	Nom d'utilisateur valide du serveur SFTP
-pw	Mot de passe du serveur SFTP avec clé d'activation à ajouter	Mot de passe valide du serveur SFTP
-f	Nom de fichier de la clé d'activation à ajouter	Nom de fichier valide du fichier de la clé d'activation
-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

Syntaxe:
`keycfg [`*options*`]`

```
option:
  -add
     -ip tftp/sftp server ip address
     -pn pn port number of tftp/sftp server (default 69/22)
     -u  username for sftp server
     -pw password for sftp server
     -f  filename
     -del   n ( where n is a valid ID number from listing)
     -deltype x ( where x is a Type value)
```

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.

Le tableau suivant présente les arguments pour les options.

Tableau 34. Commande ldap

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
-a	Méthode d'authentification utilisateur	local only, LDAP only, local first then LDAP, LDAP first then local
-aom	Mode d'authentification uniquement	enabled, disabled
-b	Méthode de liaison	anonymous, bind with ClientDN and password, bind with Login Credential
-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*
-f	Filtre de groupe	Chaîne pouvant comprendre jusqu'à 127 caractères pour *group_filter*
-fn	Nom de la forêt	Pour les environnements Active Directory. Chaîne pouvant comprendre jusqu'à 127 caractères.
-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*

Tableau 34. Commande ldap (suite)

Option	Description	Valeurs
-pc	Confirmer le 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.
-ep	Mot de passe chiffré	Mot de passe de sauvegarde/restauration (à usage interne uniquement)
-r	Nom distinctif d'entrée racine (DN)	Chaîne pouvant comprendre jusqu'à 127 caractères pour *root_dn*
-rbs	Sécurité étendue basée rôles pour les utilisateurs d'Active Directory	enabled, disabled
-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*
-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*
-t	Nom de cible serveur	Lorsque l'option rbs est activée, cette zone spécifie un nom de cible qui peut être associé à un ou plusieurs rôles sur le serveur Active Directory via l'outil du composant logiciel enfichable Role-Based Security (RBS).
-u	Attribut de recherche UID	Chaîne pouvant comprendre jusqu'à 63 caractères pour *search_attrib*
-v	Obtention de l'adresse du serveur LDAP via DNS	off, on
-h	Affiche la syntaxe et les options de la commande	

Syntaxe :

```
ldap [options]
options:
   -a loc|ldap|locId|ldloc
   -aom enable/disabled
   -b anon|client|login
   -c client_dn
   -d search_domain
   -f group_filter
   -fn forest_name
   -g group_search_attr
   -l string
   -p client_pw
```

-pc *confirm_pw*
-ep *encrypted_pw*
-r *root_dn*
-rbs *enable|disabled*
-s1ip *host name/ip_addr*
-s2ip *host name/ip_addr*
-s3ip *host name/ip_addr*
-s4ip *host name/ip_addr*
-s1pn *port_number*
-s2pn *port_number*
-s3pn *port_number*
-s4pn *port_number*
-t *name*
-u *search_attrib*
-v *off|on*
-h

Commande ntp

Utilisez cette commande pour afficher et configurer le protocole NTP (Network Time Protocol).

Le tableau suivant présente les arguments pour les options.

Tableau 35. Commande ntp

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
-en	Active ou désactive le protocole NTP (Network Time Protocol).	enabled, disabled
-i[1]	Nom ou adresse IP du serveur Network Time Protocol. Il s'agit du numéro d'index du serveur Network Time Protocol.	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.
-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.

1. -i correspond à i1.

Syntaxe :
```
ntp [options]
options:
-en state
-i  hostname/ip_addr
-f  frequency
-synch
```

Exemple :
```
system> ntp
-en: disabled
-f: 3 minutes
```

```
-i: not set
```

Commande portcfg

Utilisez cette commande pour configurer IMM pour la fonction de redirection série.

Le module IMM doit être configuré pour correspondre aux paramètres du port série interne du serveur. Pour modifier la configuration du port série, entrez les options voulues, suivies par leurs valeurs. Pour modifier la configuration du port série, vous devez disposer au moins de l'autorisation Adapter Networking and Security Configuration.

Remarque : Le port série externe du serveur peut uniquement être utilisé par le module IMM pour la fonctionnalité IPMI. L'interface CLI n'est pas prise en charge via le port série. Les options **serred** et **cliauth** présentes dans l'interface CLI du Remote Supervisor Adapter II ne sont pas prises en charge.

L'exécution de la commande **portcfg** sans option affiche la configuration du port série. Le tableau suivant présente les arguments pour les options.

Remarque : Le nombre de bits d'information (8) est défini dans le matériel et ne peut pas être modifié.

Tableau 36. commande portcfg

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	Débit en bauds	9600, 19200, 38400, 57600, 115200
-p	Parité	none, odd, even
-s	Bits d'arrêt	1, 2
-climode	Mode CLI	0, 1, 2 Où : • 0 = none : l'interface de ligne de commande est désactivée • 1 = cliems : l'interface de ligne de commande est activée avec des séquences de touches compatibles avec EMS • 2 = cliuser : l'interface de ligne de commande est activée avec des séquences de touches définies par l'utilisateur

Syntaxe :

```
portcfg [options]
 options:
   -b baud_rate
   -p parity
   -s stopbits
   -climode mode
```

Exemple :

```
system> portcfg
-b: 57600
-climode: 2 (CLI with user defined keystroke sequence)
-p: even
-s: 1
system> portcfg -b 38400
ok
system>
```

Commande portcontrol

Utilisez cette commande pour activer ou désactiver un port de service réseau.

Actuellement, cette commande prend en charge uniquement le contrôle du port pour le protocole IPMI. Tapez **portcontrol** pour afficher l'état du port IPMI. Pour activer ou désactiver le port réseau IPMI, tapez l'option **-ipmi** suivie de la valeur **on** ou **off**.

Tableau 37. Commande portcontrol

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
-all	Activer ou désactiver toutes les interfaces et tous les protocoles de reconnaissance.	on, off
-cim	Activer ou désactiver la reconnaissance CIM	on, off
-ipmi	Activer ou désactiver l'accès IPMI via LAN	on, off
-ipmi-kcs	Activer ou désactiver l'accès IPMI via le serveur	on, off
-rest	Activer ou désactiver la reconnaissance REST	on, off
slp	Activer ou désactiver la reconnaissance SLP	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

Syntaxe:

```
portcontrol [options]
 options:
   -ipmi on/off
```

Exemple :

```
system> portcontrol
cim : on
ipmi : on
ipmi-kcs : on
rest : on
slp : on
snmp : off
ssdp : on
cli : on
web : on
```

Commande ports

Utilisez cette commande pour afficher et configurer les ports IMM.

L'exécution de la commande **ports** sans option affiche des informations sur tous les ports IMM. Le tableau suivant présente les arguments pour les options.

Tableau 38. Commande ports

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
-open	Afficher les ports ouverts	
-reset	Restaurer les ports aux paramètres par défaut	
-httpp	Numéro de port HTTP	Numéro de port par défaut : 80
-httpsp	Numéro de port HTTPS	Numéro de port par défaut : 443
-sshp	Numéro de port CLI existant SSH	Numéro de port par défaut : 22
-snmpap	Numéro de port de l'agent SNMP	Numéro de port par défaut : 161
-snmptp	Numéro de port d'interruptions SNMP	Numéro de port par défaut : 162
-rpp	Numéro de port de Présence à distance	Numéro de port par défaut : 3900
-cimhp	Numéro de port CIM via HTTP	Numéro de port par défaut : 5988
-cimhsp	Numéro de port CIM via HTTPS	Numéro de port par défaut : 5989

Syntaxe :

```
ports [options]
option:
  -open
  -reset
  -httpp port_number
  -httpsp port_number
  -sshp port_number
  -snmpap port_number
  -snmptp port_number
  -rpp port_number
  -cimhp port_number
  -cimhsp port_number
```

Exemple :

```
system> ports
-httpp 80
-httpsp 443
-rpp 3900
-snmpap 161
-snmptp 162
-sshp 22
-cimhp 5988
-cimhsp 5989
system>
```

Commande rdmount

Utilisez cette commande pour monter des images disque ou des partages réseau à distance

Le tableau suivant présente les arguments pour les options.

Tableau 39. commande rdmount

Le tableau suivant, à plusieurs lignes et deux colonnes, comporte les options et leurs descriptions.

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 fonction 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.

Option	Description
-r	Opération rdoc (si utilisée, doit être la première option) -r -mappage : monter les images RDOC -r -supprimer le mappage de<filename> : démonter les images RDOC montées -r -liste de mappage : 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 lecture seule -rw lecture-écriture -u utilisateur -p mot_de_passe -l emplacement du fichier (format URL) -o option (chaîne d'option supplémentaire pour les montages samba et nfs) -d domaine (domaine pour montage samba)
-maplist	affiche les images mappés
-supprimer le mappage <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.

Le tableau suivant présente les arguments pour les options.

Tableau 40. Commande restore

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
-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
-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

Syntaxe :
```
restore [options]
option:
  -f filename
  -pp password
  -ip ip_address
  -pn port_number
username
  -pw password
```

Exemple :
```
system> restore f xcc-back.cli pp xxxxxx ip 192.168.70.200
ok
system>
```

Commande restoredefaults

Utilisez cette commande pour restaurer tous les paramètres IMM aux paramètres usines par défaut.

- La commande **restoredefaults** ne possède aucune option.
- Il vous sera demandé de confirmer la commande avant son traitement.

Syntaxe :
```
restoredefaults
```

Exemple :
```
system> restoredefaults

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 roles

Utilisez cette commande pour afficher ou configurer les rôles.

Le tableau suivant présente les arguments pour les options.

Tableau 41. Commande roles

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
-n	Rôle à configurer	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 la console distante • **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	

Syntaxe

```
   roles [-options] - display/configure roles
   - role_account -role number[3-31]
options:
   -n        - role name (limited to 32 characters)
   -p        - privilege (custom:am|rca|rcvma|pr|cel|bc|nsc|ac|us)
      am     - User account management access
      rca    - Remote console access
      rcvma  - Remote console and remote disk (virtual media) access
      pr     - Remote server power/restart access
      cel    - Ability to clear event logs
      bc     - Adapter Configuration (basic)
      nsc    - Adapter Configuration (network and security)
      ac     - Adapter Configuration (advanced)
      us     - UEFI Security
      Note: the above custom permission flags can be used in any combination
   -d        - delete a row
```

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 seccfg

Utilisez cette commande pour effectuer une annulation de microprogramme.

Le tableau suivant présente les arguments pour les options.

Tableau 42. commande seccfg

Le tableau suivant, à plusieurs lignes et deux colonnes, comporte les options et leurs descriptions.

Option	Description	Valeur
-fwrb	Permet l'annulation du microprogramme et un retour à une version antérieure	yes, no
-aubp	Active ou désactive la fonction de promotion du principal à la sauvegarde automatique	enabled, disabled

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 43. 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	Définit 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 smtp

Utilisez cette commande pour afficher et configurer les paramètres de l'interface SMTP.

L'exécution de la commande **smtp** sans option affiche toutes les informations sur l'interface SMTP. Le tableau suivant présente les arguments pour les options.

Tableau 44. Commande smtp

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
-auth	Prise en charge de l'authentification SMTP	enabled, disabled
-authepw	Mot de passe chiffré de l'authentification SMTP	Chaîne de mot de passe valide
-authmd	Méthode d'authentification SMTP	CRAM-MD5, LOGIN
-authn	Nom d'utilisateur d'authentification SMTP	Chaîne (limitée à 256 caractères)
-authpw	Mot de passe d'authentification SMTP	Chaîne (limitée à 256 caractères)
-pn	Numéro de port SMTP	Numéro de port valide
-s	Nom d'hôte ou adresse IP du serveur SMTP	Nom d'hôte ou adresse IP valide (63 caractères maximum)

Syntaxe :
```
smtp [options]
option:
  -auth enabled|disabled
  -authepw password
  -authmd CRAM-MD5|LOGIN
  -authn username
  -authpw password
  -s ip_address_or_hostname
  -pn port_number
```

Exemple :
```
system> smtp
-s test.com
-pn 25
system>
```

Commande snmp

Utilisez cette commande pour afficher et configurer les informations sur l'interface SNMP.

L'exécution de la commande **snmp** sans option affiche toutes les informations sur l'interface SNMP. Le tableau suivant présente les arguments pour les options.

Tableau 45. Commande snmp

Le tableau suivant, à plusieurs lignes et trois colonnes, comporte les options, les descriptions d'option, ainsi que les valeurs associées pour les options.

Tableau 45. Commande snmp (suite)

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.
-t1	Interruptions SNMPv1	on, off
-t2	Interruptions SNMPv2	on, off
-t	Interruptions SNMPv3	on, off
-l	Emplacement du 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 du 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 «»).
-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 «»).
-ct	Nom de la communauté d'interruption 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 "").
-ci	Adresse IP de la communauté SNMP/nom de l'hôte	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.

Tableau 45. Commande snmp (suite)

Option	Description	Valeurs
-cti	Adresse IP/nom d'hôte de la communauté d'interruption sNMPv2	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)

Syntaxe :
```
snmp [options]
option:
 -a3 state
  -t state
  -l location
  -cn contact_name
  -t1 state
  -c community name
  -ci community IP address/hostname
  -t2 state
  -ct community name
  -cti community IP address/hostname
  -eid engine id
```

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.

L'exécution de **snmpalerts** sans option affiche tous les paramètres d'alerte SNMP. Le tableau suivant présente les arguments pour les options.

Tableau 46. Commande snmpalerts

Le tableau suivant, à plusieurs lignes et trois colonnes, comporte les options, les descriptions d'option, ainsi que les valeurs associées pour les options.

Tableau 46. Commande snmpalerts (suite)

Option	Description	Valeurs
-status	État de l'alerte SNMP	on, off
-crt	Définit les événements critiques devant envoyer des alertes	all, none, custom:te|vo|po|di|fa|cp|me|in|re|ot 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
-crten	Envoyer les alertes d'événements critiques	enabled, disabled
-wrn	Définit les événements d'avertissement envoyant des alertes	all, none, custom:rp|te|vo|po|fa|cp|me|ot 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
-wrnen	Envoyer des alertes d'événements d'avertissement	enabled, disabled

Tableau 46. Commande snmpalerts (suite)

Option	Description	Valeurs
-sys	Définit les événements de routine envoyant des alertes	all, none, custom:lo|tio|ot|po|bf|til|pf|el|ne 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
-sysen	Envoyer des alertes d'événements de routine	enabled, disabled

Syntaxe :
```
snmpalerts [options]
   options:
     -status status
     -crt event_type
     -crten state
     -wrn event_type
     -wrnen state
     -sys event_type
     -sysen state
```

Commande srcfg

Utilisez cette commande pour indiquer la séquence de touches permettant d'accéder à l'interface CLI à partir du mode de redirection série.

Pour modifier la configuration de la redirection série, entrez les options voulues, suivies par leurs valeurs. Pour modifier la configuration de la redirection série, vous devez disposer au moins de l'autorisation Adapter Networking and Security Configuration.

Remarque : Le matériel IMM n'offre pas la possibilité de passer d'un port série à un port série passe-système. Par conséquent, les options `-passthru` et `entercliseq` qui sont présentes dans l'interface CLI du Remote Supervisor Adapter II ne sont pas prises en charge.

L'exécution de la commande **srcfg** sans option affiche la séquence de frappe de la redirection série en cours. Le tableau suivant affiche les arguments de l'option de commande `srcfg -entercliseq`.

Tableau 47. Commande srcfg

Le tableau suivant, à une seule ligne et trois colonnes, comporte l'option, la description d'option, ainsi que les informations de valeur associées pour l'option.

Tableau 47. Commande srcfg (suite)

Option	Description	Valeurs
-entercliseq	Séquence de touches pour accéder à une interface CLI	Séquence de touches définie par l'utilisateur permettant d'accéder à l'interface CLI. **Remarque :** Cette séquence doit comporter un caractère minimum et 15 caractères maximum. Le symbole caret (^) possède une signification spéciale dans cette séquence. Il représente Ctrl dans le mappage des touches aux séquences Ctrl (par exemple, ^[pour la touche Echap et ^M pour le retour chariot). Toutes les occurrences de ^ sont interprétées comme faisant partie d'une séquence Ctrl. Pour obtenir une liste complète des séquences Ctrl, reportez-vous à un tableau de conversion ASCII-touche. La valeur par défaut de cette zone est ^[(ce qui correspond à Esc suivi de (.

Syntaxe :
```
srcfg [options]
options:
-entercliseq entercli_keyseq
```

Exemple :
```
system> srcfg
-entercliseq ^[Q
system>
```

Commande sshcfg

Utilisez cette commande pour afficher et configurer les paramètres SSH.

L'exécution de la commande **sshcfg** sans option affiche tous les paramètres SSH. Le tableau suivant présente les arguments pour les options.

Tableau 48. Commande sshcfg

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
-cstatus	État de l'interface de ligne de commande SSH	enabled, disabled
-hk gen	Générer la clé privée du serveur SSH	
-hk rsa	Afficher la clé publique RSA du serveur	

Syntaxe :
```
sshcfg [options]
option:
  -cstatus state
  -hk gen
  -hk rsa
```

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 ssl

Utilisez cette commande pour afficher et configurer les paramètres SSL.

Pour pouvoir activer un client SSL, un certificat client doit être installé. L'exécution de la commande **ssl** sans option affiche les paramètres SSL. Le tableau suivant présente les arguments pour les options.

Tableau 49. Commande ssl

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
-ce	Active ou désactive un client SSL	on, off
-se	Active ou désactive un serveur SSL	on, off
-cime	Active ou désactive le CIM via HTTPS sur le serveur SSL	on, off

Syntaxe :

```
portcfg [options]
 options:
  -ce state
  -se state
  -cime state
```

Paramètres : les paramètres suivants sont présentés avec l'affichage du statut de la commande **ssl** et sont extraits uniquement à partir de l'interface de ligne de commande :

Server secure transport enable
Ce statut est en lecture seule et ne peut pas être défini directement.

Server Web/CMD key status
Ce statut est en lecture seule et ne peut pas être défini directement. Les valeurs en sortie possibles de la ligne de commande sont les suivantes :

Clé privée et Certificat/CSR (demande de signature de certificat) non disponible

Clé privée et Certificat signé par autorité de certification installés

Clé privée et Certificat autosigné à génération automatique installés

Clé privée et Certificat autosigné installés

Clé privée stockée, demande de signature de certificat disponible au téléchargement

État de clé CSR du serveur SSL
Ce statut est en lecture seule et ne peut pas être défini directement. Les valeurs en sortie possibles de la ligne de commande sont les suivantes :

Clé privée et Certificat/CSR (demande de signature de certificat) non disponible

Clé privée et Certificat signé par autorité de certification installés

Clé privée et Certificat autosigné à génération automatique installés

Clé privée et Certificat autosigné installés

Clé privée stockée, demande de signature de certificat disponible au téléchargement

État de clé LDAP du client SSL

Ce statut est en lecture seule et ne peut pas être défini directement. Les valeurs en sortie possibles de la ligne de commande sont les suivantes :

Clé privée et Certificat/CSR (demande de signature de certificat) non disponible

Clé privée et Certificat signé par autorité de certification installés

Clé privée et Certificat autosigné à génération automatique installés

Clé privée et Certificat autosigné installés

Clé privée stockée, demande de signature de certificat disponible au téléchargement

État de clé CSR du client SSL

Ce statut est en lecture seule et ne peut pas être défini directement. Les valeurs en sortie possibles de la ligne de commande sont les suivantes :

Clé privée et Certificat/CSR (demande de signature de certificat) non disponible

Clé privée et Certificat signé par autorité de certification installés

Clé privée et Certificat autosigné à génération automatique installés

Clé privée et Certificat autosigné installés

Clé privée stockée, demande de signature de certificat disponible au téléchargement

Commande sslcfg

Utilisez cette commande pour afficher et configurer SSL pour le module IMM et gérer les certificats.

L'exécution de la commande **sslcfg** sans option affiche toute l'information sur la configuration SSL. La commande **sslcfg** permet de générer une nouvelle clé de chiffrement et un certificat autosigné ou une demande de signature de certificat (CSR). Le tableau suivant présente les arguments pour les options.

Tableau 50. Commande sslcfg

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
-server	État du serveur SSL	enabled, disabled **Remarque :** Le serveur SSL peut uniquement être activé si un certificat valide est en place.
-client	État du client SSL	enabled, disabled **Remarque :** Le client SSL peut uniquement être activé si un certificat client ou serveur valide est en place.
-cim	État CIM via HTTPS	enabled, disabled **Remarque :** CIM via HTTPS 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.

Tableau 50. Commande sslcfg (suite)

Option	Description	Valeurs
-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.
-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	Télécharger le fichier de certificat	Cette option ne prend aucun argument mais doit également spécifier des valeurs pour l'option de commande **-cert** ou **-csr** (suivant le type de certificat étant téléchargé). Cette option ne prend aucun argument mais doit également spécifier des valeurs pour l'option de commande **-i** et l'option de commande **-l** (facultatif).
-upld	Importe 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 3 dans l'option de commande.
-c	Pays	Code pays (2 lettres) **Remarque :** Requis lors de la génération d'un certificat auto-signé ou d'une demande de signature de certificat.
-sp	Département ou province	Chaîne entre guillemets (60 caractères maximum) **Remarque :** Requis lors de la génération d'un certificat auto-signé ou d'une demande de signature de certificat.
-cl	Ville ou localité	Chaîne entre guillemets (50 caractères maximum) **Remarque :** Requis lors de la génération d'un certificat auto-signé ou d'une demande de signature de certificat.
-on	Nom de l'organisation	Chaîne entre guillemets (60 caractères maximum) **Remarque :** Requis lors de la génération d'un certificat auto-signé ou d'une demande de signature de certificat.
-hn	Nom d'hôte du IMM	Chaîne (60 caractères maximum) **Remarque :** Requis lors de la génération d'un certificat auto-signé ou d'une demande de signature de certificat.

Tableau 50. Commande sslcfg (suite)

Option	Description	Valeurs
-cp	Personne de contact	Chaîne entre guillemets (60 caractères maximum) **Remarque :** Facultatif lors de la génération d'un certificat auto-signé ou d'une demande de signature de certificat.
-ea	Adresse électronique de la personne à contacter	Adresse e-mail valide (60 caractères maximum) **Remarque :** Facultatif lors de la génération d'un certificat auto-signé ou d'une demande de signature de certificat.
-ou	Unité organisationnelle	Chaîne entre guillemets (60 caractères maximum) **Remarque :** Facultatif lors de la génération d'un certificat auto-signé ou d'une demande de signature de certificat.
-s	Nom de famille	Chaîne entre guillemets (60 caractères maximum) **Remarque :** Facultatif lors de la génération d'un certificat auto-signé ou d'une demande de signature de certificat.
-gn	Prénom	Chaîne entre guillemets (60 caractères maximum) **Remarque :** Facultatif lors de la génération d'un certificat auto-signé ou d'une demande de signature de certificat.
-in	Initiales	Chaîne entre guillemets (20 caractères maximum) **Remarque :** Facultatif lors de la génération d'un certificat auto-signé ou d'une demande de signature de certificat.
-dq	Qualificatif du nom de domaine	Chaîne entre guillemets (60 caractères maximum) **Remarque :** Facultatif lors de la génération d'un certificat auto-signé ou d'une demande de signature de certificat.
-cpwd	Mot de passe de demande d'authentification	Chaîne (6 caractères minimum, 30 caractères maximum) **Remarque :** Facultatif lors de la génération d'une demande de signature de certificat.
-un	Nom non structuré	Chaîne entre guillemets (60 caractères maximum) **Remarque :** Facultatif lors de la génération d'une demande de signature de certificat.

Syntaxe :

```
sslcfg [options]
option:
  -server state
  -client state
  -cim state
  -cert certificate_type
  -csr certificate_type
  -i ip_address
port_number
username
  -pw password
  -l filename
  -dnld
  -upld
  -tc xaction
  -c country_code
  -sp state_or_province
  -cl city_or_locality
  -on organization_name
  -hn bmc_hostname
  -cp contact_person
  -ea email_address
```

-ou *organizational_unit*
-s *surname*
-gn *given_name*
-in *initials*
-dq *dn_qualifier*
-cpwd *challenge_password*
-un *unstructured_name*

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 CIM 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 Lenovo -hn XCC-5cf3fc6e0c9d
  -cp Contact -ea "" -ou""
  ok
  ```

  L'exemple ci-dessus s'affiche sur plusieurs lignes en raison du manque d'espace.

- Pour télécharger un certificat du module IMM vers un autre, entrez 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 Lenovo -hn XCC-5cf3fc6e0c9d
  -cp Contact -ea "" -ou "
  ok
  ```

  L'exemple ci-dessus s'affiche sur plusieurs lignes en raison du manque d'espace.

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 storekeycfg

Cette commande vous permet de configurer le nom d'hôte ou l'adresse IP et le port réseau d'un serveur SKLM.

Vous pouvez configurer jusqu'à quatre cibles de serveur SKLM. La commande **storekeycfg** est également utilisée pour installer et retirer les certificats utilisés par le module IMM pour l'authentification auprès du serveur SKLM.

Le tableau suivant présente les arguments pour les options.

Tableau 51. Commande storekeycfg

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
-add	Ajouter la clé d'activation	Les valeurs sont les options de commandes -ip, -pn, -u, -pw et -f
-ip	Nom d'hôte ou adresse IP du serveur TFTP/SFTP	Nom d'hôte ou adresse IP valide du serveur TFTP/SFTP
-pn	Numéro de port du serveur TFTP ou SFTP	Numéro de port valide du serveur TFTP/SFTP (valeur par défaut 69/22)
-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
-f	Nom de fichier de la clé d'activation	Nom de fichier valide du fichier de la clé d'activation
-del	Cette commande vous permet de supprimer la clé d'activation par numéro d'index	Numéro d'index de la clé d'activation valide de la liste keycfg
-dgrp	Ajouter le groupe d'appareils	Nom du groupe d'appareils
-sxip	Ajouter le nom d'hôte ou l'adresse IP du serveur SKLM	Nom d'hôte ou adresse IP valide du serveur SKLM. Valeur numérique 1, 2, 3 ou 4.
-sxpn	Ajouter le numéro de port du serveur SKLM	Numéro de port valide du serveur de SKLM. Valeur numérique 1, 2, 3 ou 4.
-testx	Tester la configuration et la connexion au serveur SKLM	Valeur numérique 1, 2, 3 ou 4
-h	Permet d'afficher l'utilisation de la commande et ses options	

Syntaxe :

```
storekeycfg [options]
 options:
  -add state
  -ip ip_address
  -pn port_number
  -u username
  -pw password
```

```
-f filename
-del key_index
-dgrp device_group_name
-sxip ip_address
-sxpn port_number
-testx numeric value of SKLM server
-h
```

Exemples :

Pour importer le certificat de serveur SKLM, entrez la commande suivante :

```
system> storekeycfg
add -ip 192.168.70.200 -f tklm-server.der
system> ok
```

Pour configurer l'adresse du serveur et le numéro de port de SKLM, entrez la commande suivante :

```
system> storekeycfg
-s1ip 192.168.70.249
system> ok
```

Pour définir le nom de groupe d'unités, entrez la commande suivante :

```
system> storekeycfg
-dgrp IBM_SYSTEM_X_SED
system> ok
```

Commande syncrep

Utilisez cette commande pour lancer la synchronisation du microprogramme à partir d'un référentiel distant.

Le tableau suivant présente les arguments pour les options.

Tableau 52. Commande syncrep

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
-t	Protocole pour connecter le référentiel	samba, nfs
-l	Emplacement du référentiel distant	Au format URL
-u	Utilisateur	
-p	Mot de passe	
-o	Option	Chaîne d'option supplémentaire pour les montages samba et nfs
-d	Domaine	Domaine pour montage samba
-q	Interroger l'état de mise à jour actuel	
-c	Annuler le processus de synchronisation	

Syntaxe

```
syncrep [options]  Launch firmware sync from remote repository
options:
    -t <samba|nfs> protocol to connect repository
    -l location of remote repository (URL format)
```

```
-u User
-p Password
-o option (extra option string for samba and nfs mounts)
-d domain (domain for samba mount)
-q query current update status
-c cancel the sync process
```

Exemple

```
(1) start sync with repository
system> syncrep -t samba -l url -u user -p password
(2) query current update status
system> syncrep -q
(3)cancel the sync process
system> syncrep -c
```

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.

Tableau 53. thermal, commande

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
-mode	Permet d'afficher la stratégie du mode thermique et de configurer le tableau thermique des systèmes hôte (en lecture uniquement)	normal, performance, minimal, efficiency, custom
-table <vendorID_deviceID><table_number>	<vendorID_deviceID> permet d'indiquer l'ID du fournisseur et de l'appareil du composant qui doit bénéficier d'un refroidissement différent.	8 caractères hexadécimaux
	<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

Syntaxe :

```
thermal [options]
option:
  -mode thermal_mode
  -table vendorID_devicetable_number
```

Exemple :

```
system> thermal
-mode normal
-table 80860126 1 10DE0DFA 3
```

```
system>
```

Commande timeouts

Utilisez cette commande pour afficher ou modifier les valeurs de délai d'attente.

- Pour afficher les délais d'attente, entrez `timeouts`.
- Pour modifier les valeurs de délai d'attente, entrez les options voulues, suivies par leurs valeurs.
- Pour modifier les valeurs de délai d'attente, vous devez disposer au moins de l'autorisation Adapter Configuration.

Le tableau suivant présente les arguments pour les valeurs de délai d'attente. Ces valeurs correspondent aux options des graduations du menu déroulant pour les délais d'attente du serveur dans l'interface Web.

Tableau 54. Commande timeouts

Le tableau suivant, à plusieurs lignes et quatre colonnes, comporte les options, les descriptions d'option, ainsi que les valeurs associées pour les options.

Option	Délai d'attente	Unités	Valeurs
-f	Délai de mise hors tension	minutes	disabled, 0.5, 1, 2, 3, 4, 5, 7.5, 10, 15, 20, 30, 60, 120
-l	Délai d'attente du programme de chargement	minutes	disabled, 0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, 5, 7.5, 10, 15, 20, 30, 60, 120
-o	Délai d'attente du système d'exploitation	minutes	disabled, 2.5, 3, 3.5, 4
-s	Capture d’écran de l’échec du SE avec erreur HW	/	disabled, enabled

Syntaxe :
```
timeouts [options]
options:
-f power_off_delay_watchdog_option
-o OS_watchdog_option
-l loader_watchdog_option
-s OS failure screen capture with HW error
```

Exemple :
```
system> timeouts
-o disabled
-l 3.5
-f disabled
-s disabled
system> timeouts -o 2.5
ok
system> timeouts
-o 2.5
-l 3.5
-f disabled
-s disabled
```

Commande tls

Utilisez cette commande pour définir le niveau TLS minimal.

Le tableau suivant présente les arguments pour les options.

Tableau 55. Commande tls

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
-min	Sélectionner le niveau TLS minimal	1.1, 1.2[1], 1.3
-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.

Utilisation :

```
tls [-options] - configures the minimum TLS level
   -min <1.1 | 1.2 | 1.3> - Selects the minimum TLS level
   -h - Lists usage and options
```

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.

Le tableau suivant présente les arguments pour les options.

Tableau 56. commande trespass

Le tableau suivant, à plusieurs lignes et deux colonnes, comporte les options et leurs descriptions.

Tableau 56. commande trespass (suite)

Option	Description
-s	Configurer les messages Trespass
-h	Afficher les utilisations et les options

Syntaxe :

```
usage:
   trespass display the trespass message
   -s <trespass message> configure trespass message
   -h - Lists usage and options
```

Exemple :

Remarque : Le message Trespass ne contient pas d'espace.

```
system> trespass -s testingmessage
ok
system> trespass
testingmessage

The trespass message contains spaces:
system> trespass -s "testing message"
ok
system> trespass
testing message
```

commande trespass

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.

Le tableau suivant présente les arguments pour les options.

Tableau 57. Commande uefipw

Le tableau suivant, à plusieurs lignes et deux colonnes, comporte les options et leurs descriptions.

Option	Description
-cp	Mot de passe actuel (limité à 20 caractères)
-p	Nouveau de passe (limité à 20 caractères)
-cep	Mot de passe actuel chiffré
-ep	Nouveau mot de passe chiffré

Syntaxe :

```
usage:
   uefipw [-options] - Configure the UEFI admin password
options:
   -cp      - current password (limited to 20 characters)
   -p       - new password (limited to 20 characters)
```

```
-cep     - current password encrypted
-ep      - new password encrypted
```

Commande usbeth

Utilisez cette commande pour activer l'interface LAN over USB intrabande.

Syntaxe :

```
usbeth [options]
options:
-en <enabled|disabled>
```

Exemple :

```
system>usbeth
-en : disabled
system>usbeth -en enabled
ok
system>usbeth
-en : disabled
```

Commande usbfp

Utilisez cette commande pour contrôler l'utilisation par le BMC du port USB du panneau frontal

Le tableau suivant présente les arguments pour les options.

Tableau 58. commande usbfp

Le tableau suivant, à plusieurs lignes et deux colonnes, comporte les options et leurs descriptions.

Option	Description
-mode <bmc | server | shared>	Définit le mode d'utilisation à BMC, serveur ou partagé
-it <minutes>	Délai d'attente d'inactivité en minutes (mode partagé)
-btn <on | off>	Active l'utilisation du bouton d'identification pour activer/désactiver le propriétaire (mode partagé)
-own <bmc | server >	Définit le propriétaire à bmc ou serveur (mode partagé)

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. Le tableau suivant présente les arguments pour les options.

Tableau 59. Commande users

Le tableau suivant, à plusieurs lignes et trois colonnes, comporte les options, les descriptions d'option, ainsi que les valeurs associées pour les options.

Tableau 59. Commande users (suite)

Option	Description	Valeurs
-user_index	Numéro d'index du compte utilisateur	1 à 12 inclus, ou `all` pour tous les utilisateurs.
-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 20 caractères. Null crée un compte sans mot de passe que l'utilisateur doit définir au cours de la première connexion.
-r	Nom du rôle	Comme indiqué dans la commande « Commande roles » à la page 157
-ep	Mot de passe de chiffrement (pour sauvegarde/restauration)	Mot de passe valide
-clear	Effacer le compte utilisateur spécifié Si vous êtes autorisé 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.	Le numéro d'index du compte utilisateur à effacer doit être spécifié au format : `users -clear -`*user_index*
-curr	Afficher les utilisateurs actuellement connectés	
-sauth	Protocole d'authentification SNMPv3	HMAC-SHA, aucun
-spriv	Protocole de confidentialité SNMPv3	CBC-DES, AES, none
-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, set
-strap	Nom d'hôte de message d'interruption SNMPv3	Nom d'hôte valide

Tableau 59. Commande users (suite)

Option	Description	Valeurs
-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. • Pour les nœuds Flex, les commandes utilisateur sont limitées aux comptes IPMI et SNMP locaux. L'option `-pk` n'est pas prise en charge pour Flex Systems.
-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. **Remarques :** • 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`. • Pour les nœuds Flex, les commandes utilisateur sont limitées aux comptes IPMI et SNMP locaux. L'option `-remove` n'est pas prise en charge pour Flex Systems.
-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=="` • Pour les nœuds Flex, les commandes utilisateur sont limitées aux comptes IPMI et SNMP locaux. L'option `-add` n'est pas prise en charge pour Flex Systems.

Tableau 59. Commande users (suite)

Option	Description	Valeurs
-upld	Télécharger une clé publique SSH *(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`. • Pour les nœuds Flex, les commandes utilisateur sont limitées aux comptes IPMI et SNMP locaux. L'option `-upld` n'est pas prise en charge pour Flex Systems.
-dnld	Télécharger la clé publique SSH indiquée *(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 59. Commande 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."`.

Syntaxe :

```
users [-options] - display/configure user accounts
options:
   -[1-12]  - user account number
   -l       - display password expiration days
   -n       - username (limited to 16 characters)
   -p       - password (limited to 32 characters)
   -shp     - set hashpassword (total 64 characters)
   -ssalt   - set salt (limited to 64 characters)
   -ghp     - get hashpassword
   -gsalt   - get salt
   -ep      - encrypted password (used with backup/restore )
   -r       - role name as listed in roles command
   -clear   - clear user account
   -curr    - display current users
   -sauth   (none|HMAC-SHA)           - snmpv3 authentication protocol
   -spriv   (none|CBC-DES|AES)        - snmpv3 privacy protocol
   -spw     password                    - snmpv3 privacy password
   -sepw    encryptedpassword          - snmpv3 privacy password (encrypted)
   -sacc    (Get)                  - snmpv3 Access type
   -strap   hostname                    - snmpv3 trap hostname

   -pk      - SSH public keys options:
       -e       - Displays the entire key in OpenSSH format
       -remove  - Removes the specified key for the specified user
       -add     - Adds a public key for the specified user
       -upld    - Used to upload a public key in OpenSSH/RFC4716 format
       -dnld    - Used to download the specified public key to a TFTP/SFTP server
       -i       - IP address of the TFTP/SFTP
       -pn      - port number of tftp/sftp server (default 69/22)
       -u       - username for sftp server
       -pw      - password for sftp server
       -l       - Filename of the key file when uploading or downloading via TFTP/SFTP
       -af      - accept connections from host, in the format: from="<list>", where
                  <list> is a comma-separated list of hostnames and IP addresses
                  (limited to 511 characters)
       -cm      - comment (limited to 255 characters, must be quote-delimited)
```

Exemple :

```
system> users
 Account      Login ID      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
 Account      Login ID      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  Admini
system> users -5 ghp
292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
system> users -5 gsalt
abc
```

Commandes de contrôle de IMM

Cette rubrique fournit une liste alphabétique des commandes CLI de contrôle de IMM.

Il existe actuellement 7 commandes de contrôle de IMM :

Commande alertentries

Utilisez cette commande pour gérer les destinataires d'alertes.

- **alertentries** sans option affiche tous les paramètres d'entrée d'alerte.
- **alertentries -number -test** génère une alerte test au numéro d'index du destinataire indiqué.
- **alertentries -number** (nombre compris entre 0 et 12) affiche les paramètres d'entrée d'avertissement du numéro d'index du destinataire indiqué et permet de modifier les paramètres d'alerte de ce destinataire.

Le tableau suivant présente les arguments pour les options.

Tableau 60. Commande alertentries

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
-number	Numéro d'index du destinataire de l'alerte à afficher, ajouter, modifier ou supprimer	1 à 12
-status	État du destinataire de l'alerte	on, off
-type	Type d'alerte	e-mail, syslog
-log	Inclure le journal des événements dans l'e-mail d'alerte	on, off
-n	Nom du destinataire de l'alerte	String
-e	Adresse électronique du destinataire de l'alerte	Adresse électronique valide
-ip	Nom d'hôte ou adresse IP syslog	Nom d'hôte ou adresse IP valide
-pn	Numéro de port syslog	Numéro de port valide

Tableau 60. Commande alertentries (suite)

Option	Description	Valeurs
-del	Supprimer le numéro d'index du destinataire indiqué	
-test	Générer une alerte test au numéro d'index du destinataire spécifié	
-crt	Définit les événements critiques devant envoyer des alertes	all, none, custom:te|vo|po|di|fa|cp|me|in|re|ot Les paramètres d'alerte critique personnalisés sont spécifiés à l'aide d'une liste de valeurs séparées par des barres telle que **alertentries -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
-crten	Envoyer les alertes d'événements critiques	enabled, disabled
-wrn	Définit les événements d'avertissement envoyant des alertes	all, none, custom:rp|te|vo|po|fa|cp|me|ot Les paramètres d'alerte des avertissements personnalisés sont spécifiés à l'aide d'une liste de valeurs séparées par des barres verticales telle que **alertentries -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
-wrnen	Envoyer des alertes d'événements d'avertissement	enabled, disabled

Tableau 60. Commande alertentries (suite)

Option	Description	Valeurs
-sys	Définit les événements de routine envoyant des alertes	all, none, custom:lo|tio|ot|po|bf|til|pf|el|ne Les paramètres d'alertes de routine personnalisés sont spécifiés à l'aide d'une liste de valeurs séparées par des barres verticales au format **alertentries -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
-sysen	Envoyer des alertes d'événements de routine	enabled, disabled

Syntaxe :

```
alertentries [options]
   options:
   -number recipient_number
      -status status
      -type alert_type
      -log include_log_state
      -n recipient_name
      -e email_address
      -ip ip_addr_or_hostname
      -pn port_number
      -del
      -test
      -crt event_type
      -crten state
      -wrn event_type
      -wrnen state
      -sys event_type
      -sysen state
```

Exemple :

```
system> alertentries
1. test
2. <not used>
3. <not used>
4. <not used>
5. <not used>
6. <not used>
7. <not used>
8. <not used>
9. <not used>
10. <not used>
11. <not used>
12. <not used>
```

```
system> alertentries -1
-status off
-log off
-n test
-e test@mytest.com
-crt all
-wrn all
-sys none
system>
```

Commande batch

Utilisez cette commande pour exécuter une ou plusieurs commandes CLI contenues dans un fichier.

- 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.

Le tableau suivant présente les arguments pour les options.

Tableau 61. Commande batch

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
-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

Syntaxe :

```
batch [options]
option:
  -f filename
  -ip ip_address
  -pn port_number
 username
  -pw password
```

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 clearcfg

Utilisez cette commande pour rétablir la configuration IMM à ses paramètres usine par défaut.

Vous devez disposer au moins des droits Advanced Adapter Configuration pour émettre cette commande. Après l'effacement de la configuration IMM, le module IMM est redémarré.

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.

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.

Pour un décalage UTC de +2, -7, -6, -5, -4 et -3, des paramètres d'heure d'été spéciaux 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).

Syntaxe:
```
clock [options]
options:
-u UTC offset
-dst on/off/special case
-host - local | utc , format of time obtained from host (default: utc)
Windows systems use local, Linux uses utc
```

Exemple :
```
system> clock
12/12/2011 13:15:23 GMT-5:00 dst on
```

Commande identify

Utilisez cette commande pour activer ou désactiver le voyant d'identification du châssis ou pour le faire clignoter.

L'option **-d** peut être utilisée avec l'option **-s on** pour activer uniquement le voyant pendant le nombre de secondes spécifié par l'option **-d**. Une fois ce délai écoulé, le voyant est désactivé.

Syntaxe :
```
identify [options]
options:
-s on/off/blink
-d seconds
```

Exemple :

```
system> identify
-s off
system> identify -s on -d 30
ok
system>
```

Commande info

Utilisez cette commande pour afficher et configurer les informations sur le module IMM.

L'exécution de la commande **info** sans option affiche toutes les informations de contact et d'emplacement du module IMM. Le tableau suivant présente les arguments pour les options.

Tableau 62. Commande info

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
-name	Nom du IMM	String
-contact	Nom de la personne à contacter pour le module IMM	String
-location	Emplacement du IMM	String
-room[1]	Identificateur de la salle du module IMM	String
-rack[1]	Identificateur de l'armoire du module IMM	String
-rup[1]	Position du module IMM dans l'armoire	String
-ruh	Hauteur de l'armoire	Lecture seule
-bbay	Emplacement de la baie lame	Lecture seule

1. La valeur est en lecture seule et ne peut pas être restaurée si le module IMM réside sur Flex System.

Syntaxe :

```
info [options]
option:
  -name xcc_name
  -contact contact_name
  -location xcc_location
  -room room_id
  -rack rack_id
  -rup rack_unit_position
  -ruh rack_unit_height
  -bbay blade_bay
```

Commande spreset

Utilisez cette commande pour redémarrer le module IMM.

Vous devez disposer au moins des droits Advanced Adapter Configuration pour émettre cette commande.

Commandes de Service Advisor

Cette rubrique fournit une liste alphabétique des commandes CLI Service Advisor.

Il existe actuellement 3 commandes de Service Advisor :

Commande chconfig

Utilisez cette commande pour afficher et configurer les paramètres Service Advisor.

- Vous devez accepter les dispositions de l'assistant de service (Service Advisor Terms and Conditions), à l'aide de l'option de commande **chconfig -li**, avant de configurer tout autre paramètre.
- Toutes les zones d'informations de contact, ainsi que la zone **Service Support Center** (en utilisant l'option de commande chconfig -sc), doivent être renseignées pour pouvoir activer le support Lenovo de Service Advisor.
- Toutes les zones HTTP Proxy doivent être définies si un proxy HTTP est requis.

Le tableau suivant présente les arguments pour les options.

Tableau 63. Commande chconfig

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
-li	Afficher ou accepter les dispositions Service Advisor Terms and Conditions **Remarque :** Les conditions générales doivent être acceptées avant de configurer d'autres paramètres.	view, accept
-sa	Statut Support de l'assistant Service Advisor **Remarques :** Pour activer Service Advisor, les critères suivants doivent être remplis : • Le code pays est requis. • Toutes les options de la section informations de contact de Service Advisor sont requises.	enabled, disabled
-sc	Code pays pour le centre d'assistance	Code pays ISO à deux caractères
Options d'informations de contact de Service Advisor :		
-cn	Nom du contact principal	Chaîne entre guillemets (30 caractères maximum)
-cph	Numéro de téléphone du contact principal	Chaîne entre guillemets (5 à 30 caractères)
-ce	Adresse électronique du contact principal **Remarque :** Les caractères alphanumériques « . », « - » ou « _ » sont acceptés en tant qu'ID utilisateur ou nom d'hôte. L'adresse e-mail doit contenir au moins deux éléments de domaine. Le dernier élément de domaine doit comporter 2 à 4 caractères alphabétiques.	Adresse électronique valide, au format `userid@hostname` (30 caractères maximum)
-co	Nom de l'organisation ou de la société du contact principal	Chaîne entre guillemets (30 caractères maximum)
-ca	Adresse de l'emplacement de la machine	Chaîne entre guillemets (30 caractères maximum)

Tableau 63. Commande chconfig (suite)

Option	Description	Valeurs
-cci	Ville de l'emplacement de la machine	Chaîne entre guillemets (30 caractères maximum)
-cs	État de l'emplacement de la machine	Chaîne entre guillemets (30 caractères maximum)
-cz	Code postal de l'emplacement de la machine	Chaîne entre guillemets (9 caractères maximum)
Options d'informations du contact Service Advisor suppléant :		
-an	Nom du contact suppléant	Chaîne entre guillemets (30 caractères maximum)
-aph	Numéro de téléphone du contact suppléant	Chaîne entre guillemets (5 à 30 caractères)
-ae	Adresse électronique du contact suppléant **Remarque :** Les caractères alphanumériques « . », « - » ou « _ » sont acceptés en tant qu'ID utilisateur ou nom d'hôte. L'adresse e-mail doit contenir au moins deux éléments de domaine. Le dernier élément de domaine doit comporter 2 à 4 caractères alphabétiques.	Adresse électronique valide, au format `userid@hostname` (30 caractères maximum)
-ao	Nom de l'organisation ou de la société du contact suppléant	Chaîne entre guillemets (30 caractères maximum)
-aa	Adresse de l'emplacement de la machine suppléante	Chaîne entre guillemets (30 caractères maximum)
-aci	Ville de l'emplacement de la machine suppléante	Chaîne entre guillemets (30 caractères maximum)
-as	État de l'emplacement de la machine suppléante	Chaîne entre guillemets (30 caractères maximum)
-az	Code postal de l'emplacement de la machine suppléante	Chaîne entre guillemets (9 caractères maximum)
Options de paramètres proxy HTTP :		
-loc	Emplacement proxy HTTP	Nom d'hôte qualifié complet ou adresse IP du proxy HTTP (63 caractères maximum)
-po	Port du proxy HTTP	Numéro de port valide (1 - 65535)
-ps	Statut du proxy HTTP	enabled, disabled
-pw	Mot de passe du proxy HTTP	Mot de passe valide, entre guillemets (15 caractères maximum)
-epw	Mot de passe chiffré du proxy HTTP	Mot de passe valide, entre guillemets (15 caractères maximum)
-u	Nom d'utilisateur du proxy HTTP	Nom d'utilisateur valide, entre guillemets (30 caractères maximum)
-test	Proxy HTTP test	

Syntaxe :
```
chconfig [options]
option:
```

-li *view|accept*
-sa *enable|disable*
-sc *service_country_code*
-ce *contact_email*
-cn *contact_name*
-co *company_name*
-cph *contact_phone*
-cpx *contact_extension_phone*
-an *alternate_contact_name*
-ae *alternate_contact_email*
-aph *alternate_contact_phone*
-apx *alternate_contact_extension_phone*
-mp *machine_phone_number*
-loc *hostname/ip_address*
-po *proxy_port*
-ps *proxy_status*
-pw *proxy_pw*
-ccl *machine_country_code*
-u *proxy_user_name*

Commande chmanual

Utilisez cette commande pour générer une demande manuelle d'appel vers Lenovo.

Remarque : Les destinataires de message d'appel vers Lenovo sont configurés à l'aide de la commande **chconfig**.

- La commande **chmanual -test** génère un message de test d'appel vers Lenovo.

Le tableau suivant présente les arguments pour les options.

Tableau 64. Commande chmanual

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
-test	Génère un message de test pour les destinataires d'appel vers Lenovo	

Syntaxe :
```
chmanual [options]
Generates a manual Call Home or a Test Call Home
  -test: Generate a test Call Home.
```

Commande chlog

Utilisez cette commande pour afficher les cinq derniers événements d'appel vers Lenovo et annuler l'incident associé à l'événement par caseNumber.

La commande **chlog** affiche les cinq dernières entrées du journal d'activité d'appel vers Lenovo générées par le serveur ou l'utilisateur. L'entrée d'appel vers Lenovo la plus récente est affichée en premier. Le serveur n'enverra pas les événements en double s'ils ne sont pas reconnus comme corrigés dans le journal d'activité.

Le tableau suivant présente les arguments pour les options.

Tableau 65. Commande chconfig

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
-c	annuler l'incident associé à l'événement par caseNumber	

Syntaxe :

```
chlog[-options]
      Displays the last five call home events that were generated either by
      the system or the user (most recent call home entry first.)

      -c: cancel the case associated with the event by caseNumber
```

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 plate-forme prend en charge cette commande) des informations sur les dispositifs de stockage du serveur qui sont gérés par le module IMM.

Le tableau suivant présente les arguments pour les options.

Tableau 66. Commande storage

Le tableau suivant, à plusieurs lignes et trois colonnes, comporte les options, les descriptions d'option, ainsi que les valeurs associées pour les options.

Tableau 66. Commande storage (suite)

Option	Description	Valeurs
-list	Afficher une liste des cibles de stockage gérées par le module IMM.	*controllers*|*pools*|*volumes*|*drives* Où *target* est : • *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 -target *target_id*	Afficher la liste des *cibles* de stockage gérées par le module IMM en fonction des *target_id*.	*pools*|*volumes*|*drives ctrl[x]*|*pool[x]* Où *target* et *target_id* sont : • *pools ctrl[x]* : liste des pools de stockage associés au contrôleur RAID, suivant target_id[1] • *volumes ctrl[x]*|*pool[x]* : liste des volumes de stockage associés au contrôleur RAID, suivant target_id[1] • *drives ctrl[x]*|*pool[x]* : liste des unités de stockage associées au contrôleur RAID, suivant target_id[1]
-list flashdimms	Afficher la liste des mémoires DIMM Flash gérées par le module IMM.	
-list devices	Afficher l'état de tous les disques et mémoires DIMM Flash 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]* |*flashdimm[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]* |*flashdimm[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]*|*flashdimm[x]*[2]
-showlog *target_id<m:n*|*all>*[3]	Afficher les journaux des événements de la cible sélectionnée, gérée par le module IMM.	Où *target_id* est : *ctrl[x]*[4] *m:n*|*all* Où *m:n* est l'un des nombres maximaux des journaux des événements Où *all* représente l'ensemble des journaux des événements

Tableau 66. Commande storage (suite)

Option	Description	Valeurs
-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 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]
-config drv -mkgood -target *target_id*[3]	Remplacer une unité incorrecte non configurée par une unité correcte non configurée. ou Convertir l'unité JBOD (Just a Bunch Of Disks) en une unité correcte non configurée.	Où *target_id* est : *disk[x]*[5]
-config drv -addhsp -*[dedicated pools]* -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 -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 66. Commande 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*>] est la stratégie d'écriture dans le cache : – Entrer *0* pour la stratégie d'écriture immédiate – Entrer *1* pour la stratégie d'écriture différée – Entrer *2* pour la stratégie BBU (WBACK AVEC BBU) • [-r <*0*|*1*|*2*>] est la stratégie de lecture dans le cache : – Entrer *0* pour la stratégie Pas de lecture anticipée – Entrer *1* pour la stratégie Lecture anticipée – Entrer *2* pour la stratégie Lecture anticipée adaptative • [-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*|*1ERLQ0*|*1E0RLQ0*>] 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 66. Commande storage (suite)

Option	Description	Valeurs
		• [-w <*0*|*1*|*2*>] est la stratégie d'écriture dans le cache : – Entrer *0* pour la stratégie d'écriture immédiate – Entrer *1* pour la stratégie d'écriture différée – Entrer *2* pour la stratégie BBU (WBACK AVEC BBU) • [-r <*0*|*1*|*2*>] est la stratégie de lecture dans le cache : – Entrer *0* pour la stratégie Pas de lecture anticipée – Entrer *1* pour la stratégie Lecture anticipée – Entrer *2* pour la stratégie Lecture anticipée adaptative
-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 bande du volume, par exemple, 128 k ou 1 M • -target *target_id* est : – *ctrl[x]* (nouveau pool de stockage)[5] – *pool[x]* (pool de stockage existant)[5]

Tableau 66. Commande 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|1ERLQ0|1E0RLQ0>*] 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]
-help	Permet d'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.

Syntaxe :
```
storage [options]
option:
  -config ctrl|drv|vol -option [-options] -target target_id
  -list controllers|pools|volumes|drives
  -list pools -target ctrl[x]
  -list volumes -target ctrl[x]|pool[x]
  -list drives -target ctrl[x]|pool[x]
  -list devices
  -list flashdimms
  -show target_id
  -show {ctrl[x]|pool[x]|disk[x]|vol[x]|flashdimm[x]} info
  -show {ctrl[x]|disk[x]|flashdimm[x]}firmware
  -showlog ctrl[x]m:n|all
  -h help
```

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 flashdimms
flashdimm[1]    Flash DIMM 1
flashdimm[4]    Flash DIMM 4
flashdimm[9]    Flash DIMM 9
system>
system> storage
-list pools
pool[0-0]    Storage Pool 0
pool[0-1]    Storage Pool 1
system>
system> storage
-list volumes
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.: 1234567890
FRU No.: 5005076049CC4
Part No.: LSI2004
Cache Model Status: Unknown
Cache Model Memory Size: 300MB
Cache Model Serial No.: PBKUD0XTA0P04Y
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
storage[0-0]    Pool 0
storage[0-1]    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 flashdimm[15]
Name: CPU1 DIMM 15
Health Status: Normal
Operational Status: Online
Capacity(GB): 400GB
Model Type: DDR3
Part Number: 93E40400GGM101PAT
FRU S/N: 44000000
Manuf ID: Diablo Technologies
Temperature: 0C
Warranty Writes: 100%
Write Endurance: 100%
F/W Level: A201.0.0.49152
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.

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.`
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.

Le tableau suivant présente les arguments pour les options.

Tableau 67. Commande adapter

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
-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|chips]* 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 • *chips* : afficher toutes les informations sur la puce GPU de l'adaptateur
-h	Permet d'afficher l'utilisation de la commande et ses options	

Syntaxe :
```
adapter [options]
option:
  -list
  -show target_id [info|firmware|ports|chips]
  -h help
```

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> 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
```

Commande mvstor

Utilisez cette commande pour obtenir les informations d'inventaire associées à M.2 et gérer les volumes virtuels.

Le tableau suivant présente les arguments pour les options.

Tableau 68. Commande mvstor

Le tableau suivant, à plusieurs lignes et deux colonnes, comporte les options et leurs descriptions.

Option	Description
-h/?	Imprimer les informations d'aide pour cette commande
-version	Afficher les informations du microprogramme du contrôleur
-disks	Afficher les informations des disques de support
-volumes	Afficher les informations des volumes virtuels
-create	Créer un volume virtuel. Les éléments VD_Name, RaidLevel et StripeSize peuvent être spécifiés
-delete	Supprimer un volume virtuel
-import	Importer un volume virtuel étranger Une fois le volume virtuel importé, un réamorçage du système régénère automatiquement le volume virtuel.

Utilisation

```
   mvstor [-options] - raid configuration for SATA/NVMe RAID boot solution.
options:
   -version                    - displays controller firmware version.
   -disks                      - displays information of media disks.
   -volumes                    - displays information of virtual disks
   -create -slot <slot_no> -name <vd name> -level <0|1> -stripe <32|64|128|256|512> - create virtual volume.
       Marvell SATA RAID: stripe size can only be 32k or 64k
       Marvell NVMe RAID: vd name is unapplicable. The name will always be VD_0.
   -delete -slot <slot_no> -id <0|1>          - delete the virtual volume
   -import -slot <slot_no> -id <0|1>          - import a foreign virtual volume
```

Exemple

```
system> mvstor -version
    Controller Slot      Device Name                                              Version
1                ThinkSystem M.2 SATA 2-Bay RAID Enablement Kit        2.3.20.1203


system> mvstor -disks
  Controller Slot 1    M.2 Bay0         128GB M.2 SATA SSD     LEN
  Controller Slot 1    M.2 Bay1         128GB M.2 SATA SSD     LEN

system> mvstor -volumes
Controller Slot 1:
```

```
    VD_ID:         0
    VD_Name:       VD_Test
    PD_Member:     0,1
    RaidLevel:     1
    StripSize:     64k
    VD_Capacity:   117 GB
    VD_Status:     Optimal
       1              64k           29 GB            Optimal

system> mvstor -delete –slot 1 -id 0
VD_ID 0 is deleted

system> mvstor -create –slot 1 -name M2RAID -level 1 -strip 64
New volume is created

system> mvstor -import –slot 1 -id 0
VD_ID 0 is imported
```

Commandes Support

Cette rubrique fournit une liste alphabétique des commandes Support.

Une seule commande Support est disponible : la « Commande dbgshimm » à la page 203.

Commande dbgshimm

Utilisez cette commande pour déverrouiller l'accès réseau au shell de débogage sécurisé.

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

Le tableau suivant présente les arguments pour les options.

Tableau 69. commande dbgshimm

Le tableau suivant, à plusieurs lignes et deux colonnes, comporte les options et leurs descriptions.

Option	Description
état	Afficher l'état
activer	Activer l'accès au débogage (valeur par défaut en l'absence d'option spécifiée)
désactivation	Désactiver l'accès au débogage

Chapitre 12. 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 205.

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 205.

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	données1 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 données2 00h = canal 0 01h = canal 1 etc. Si données2 n'est pas spécifiée dans la demande, le canal 0 est utilisé par défaut

L'octet de données1 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 données2 est utilisé pour indiquer le canal pour le module logique, si le module est un périphérique NCSI. Si les données2 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 données2 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 données1 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 données2 est utilisé pour indiquer le canal pour le module logique, si le module est un périphérique NCSI. Si les données2 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 données2 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 Stark, le paramètre de négociation automatique ne peut pas être modifié car il risque de rompre le chemin de communication réseau via CMM et 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 :

Obtention/définition 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		

Obtention/définition de 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.

Obtention/définition du 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	Obtention/définition du 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>Obtention/ définition du 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>Activé</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>Activé</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>Commuta-teur 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>

Chapitre 13. Serveurs Edge

Cette rubrique décrit les fonctions spécifiques associées aux serveurs Edge.

Remarques :

1. Le système requiert que vous modifiez le mot de passe XCC lors de votre première connexion.
2. Le IPMI sur LAN est désactivé par défaut.
3. Le IPMI sur KCS est désactivé par défaut.

Mode de verrouillage du système

Lorsque le **mode de verrouillage du système** est en état activé, cela signifie que le système est en mode verrouillage. Vous pouvez activer le système et le déverrouiller, sinon le système hôte n'est pas autorisé à démarrer.

Cliquez sur **Sécurité** sous **Configuration BMC** et faites défiler jusqu'à **Mode de verrouillage du système**.

Mode de verrouillage du système

Pour activer le système et quitter le **mode de verrouillage du système**, procédez comme suit.

1. Cliquez sur le bouton **Inactif** et une fenêtre contextuelle **Key Vault Activation** va afficher une **question secrète**.
2. Contactez votre administrateur informatique et fournissez une **question secrète**.
3. Obtenez la **réponse secrète** de votre administrateur informatique et entrez-la dans la fenêtre **Key Vault Activation**.
4. Cliquez sur le bouton **OK**, puis sur **Appliquer**.
5. Si tous les paramètres fonctionnent correctement, vous verrez que le **mode de verrouillage du système** est maintenant **inactif**.

Remarque : Lorsque le mode de verrouillage du système est activé, tout accès aux secrets système, par exemple, les clés d'authentification SED, est **refusé**.

Pour forcer le système à entrer en mode de verrouillage du système, procédez comme suit.

1. Cliquez sur le bouton **Actif**.
2. Cliquez sur le bouton **OK**, puis sur **Appliquer**.

Détection de mouvement

Vous pouvez activer cette fonction pour protéger votre serveur en détectant tout déplacement physique de votre serveur.
Si la détection de mouvement est activée, vous pouvez définir les éléments suivants en fonction de vos préférences et de votre configuration.

- **Niveau de sensibilité** : sélectionnez le niveau de sensibilité, de **faible**, **moyen** et **élevé**, en fonction de vos préférences.
- **Orientation** : sélectionnez votre configuration à partir des options suivantes : **bureau debout**, **montage mural (horizontal)**, **, montage mural (vertical)**, **bibliothèque** et **montage plafond**.

Remarque : La détection de mouvement est automatiquement désactivée lorsque le système est en mode verrouillage.

Détection d'intrusion de châssis

Vous pouvez activer cette fonction pour protéger votre serveur en détectant tout déplacement physique du carter supérieur.

Configurations supplémentaires

Si le module LOM compatible sans fil est installé, il existe trois paramètres que vous pouvez choisir pour un événement d'altération détecté.

Dans certaines circonstances inhabituelles, la **question secrète** risque de ne pas être vérifiée par ThinkShield Key Vault Portal. Il peut être alors nécessaire de réinitialiser le compteur interne du périphérique avant d'activer le périphérique à la demande de votre administrateur informatique.

Gestionnaire de clé d’authentification (AK) SED

Pour le système équipé de SED (unité à chiffrement automatique), cette fonctionnalité contrôle le module BMC pour déployer la clé d’authentification SED. Vous pouvez utiliser la clé d’authentification SED pour chiffrer des unités d’amorçage et de données et pour amorcer le système sans intervention manuelle

Remarque : Cette opération n’est pas autorisée lorsque le système n’est pas activé (le mode de verrouillage du système est validé), ou lorsque l’utilisateur actuel ne dispose pas des droits pour gérer la clé d’authentification SED.

Cliquez sur **Sécurité** sous **Configuration BMC** et faites défiler jusqu'à **Gestionnaire de clé d’authentification (AK) SED**.

Modification de la clé SED AK

Génération d'une clé SED AK à partir d'une phrase passe : définissez le mot de passe et entrez-le à nouveau pour confirmation. Cliquez sur **Générer à nouveau** pour obtenir la nouvelle clé SED AK.

Génération d'une clé SED AK de manière aléatoire : cliquez sur **Générer à nouveau** pour obtenir une clé SED AK aléatoire.

Sauvegarde de la SED AK : définissez le mot de passe et entrez-le à nouveau pour confirmation. Cliquez sur **Démarrer la sauvegarde** pour sauvegarder la clé SED AK, puis téléchargez le fichier de clé SED AK et stockez-le en lieu sûr en vue d'un usage ultérieur.

Remarque : Si vous utilisez le fichier de sauvegarde de clé SED AK pour restaurer une configuration, le système vous demandera le mot de passe que vous avez défini ici.

Récupération de la clé SED AK : vous ne pouvez effectuer cette tâche que si la SED ne fonctionne pas correctement. Il existe deux méthodes pour récupérer la clé SED AK :

- **Récupération de la clé SED AK à l'aide d'une phrase passe** : utilisez le mot de passe défini dans le mode **Génération d'une clé SED AK à partir d'une phrase passe** pour récupérer la clé SED AK.
- **Récupération de la clé SED AK à partir d'un fichier de sauvegarde** : téléchargez le fichier de sauvegarde généré dans le mode **Sauvegarde de la SED AK** et entrez le mot de passe de fichier de sauvegarde correspondant afin de récupérer la clé SED AK.

Réseaux Edge

Cette page de fonction n'est prise en charge que lorsque le module LOM compatible sans fil est installé.

Pour les tableaux prédéfinis de la topologie de réseau, voir https://thinksystem.lenovofiles.com/help/topic/SE350/pdf_files.html pour plus de détails.

Connectivité Wi-Fi

Cliquez sur **Activé** pour pouvoir configurer les paramètres en fonction de votre configuration Wi-Fi.

Connectivité LTE

Ceci vous permet de contrôler la connectivité LTE pour la carte réseau Edge.

Adresse de la carte réseau Edge

État de **l'IPv4 ou IPv6**	État du **serveur DHCP**	**Méthode**
Désactivé	**Désactivé**	**Obtenir l'adresse IP de DHCP**
Activé	**Activé**	**Utiliser une adresse IP statique**
Activé	**Désactivé**	**Procurez-vous l'adresse IP de DHCP** ou **utilisez une adresse IP statique** en fonction de votre utilisation.

Pont réseau BMC

Vous pouvez accéder au module BMC par l'intermédiaire des **ports de liaison descendante**, des **ports Wi-Fi**, des **ports de liaison montante** ou d'**aucun** port.

Remarque : Sélectionner **Aucun** indique que cette fonction est désactivée.

Dépannage de la carte réseau Edge

Redémarrer immédiatement : vous pouvez redémarrer la carte réseau à l'aide de ce bouton.
Réinitialiser aux paramètres d'usine : vous pouvez réinitialiser la carte réseau aux valeurs par défaut à l'aide de ce bouton.

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 :

http://thinksystem.lenovofiles.com/help/index.jsp

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 le 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 http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc2.doc/NN1ia_c_servicesandsupport.html.
  - Pour plus d'informations sur l'utilisation de l'interface CLI pour collecter les données de maintenance, voir http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc2.doc/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 http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/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 http://sysmgt.lenovofiles.com/help/topic/toolsctr_cli_lenovo/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 70. 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 :

http://thinksystem.lenovofiles.com/help/index.jsp

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

Accès de l'unité
  gestion des certificats 170
  sécurité 170
accès distant 2
accseccfg, commande 132
adressage de serveur
  DNS (Directory Name System) 139
Adressage IPv4
  DNS (Directory Name System) 139
Adressage IPv6
  DNS (Directory Name System) 139
Adresse IP
  configuration 9
  IPv4 9
  IPv6 9
  Serveur LDAP 149
  Serveur SMTP 158
adresse IP statique par défaut 10
adresse IP statique, valeur par défaut 10
Adresse IP statique, valeur par défaut 10
Adresse MAC
  gestion 145
affectations de ports
  configuration 36
  paramètres 36
affecté automatiquement
  certificat 47
affichage en cours
  utilisateurs 176
affichage et configuration des unités virtuelles 95
afficher les informations sur le microprogramme
  serveur 127
afficher les ports ouverts 154
aide 233
alimentation
  gestion à l'aide de commandes IPMI 74
  surveillance à l'aide de commandes IPMI 74
alimentation et redémarrage du serveur
  Commandes du plug-in 127
appel vers Lenovo
  configuration 53
approvisionnement de groupe voisin
  groupe voisin 108
attribut d'autorisation de connexion
  LDAP 149
attribut de recherche de groupe
  LDAP 149
Attribut de recherche UID
  Serveur LDAP 149
Authentification des tentatives de connexion 17

B

backup, commande 137
batch, commande 184
BIOS (Basic Input/Output System) 1

C

capture d'écran bleu 78
capture d'écran du système d'exploitation 78
certificat du serveur
  gestion 50
Certificat SKLM
  gestion 46–47
chconfig, commande 187
CIM via HTTPS
  gestion des certificats 165–166
  sécurité 165–166
classifications de certificat
  affecté automatiquement 47
  Signé par une autorité de certification 47
clé d'activation
  exporter 106
  gestion 148
  installation 105, 148
  retrait 106, 148
clés de chiffrement
  gestion centralisée 45
Clés SSH
  utilisateur 176
client
  gestion des certificats 47
collecte des données de maintenance 234
collecte du journal des données de maintenance 91
Commande adapter 200
Commande alertcfg 134
Commande alertentries 181
Commande asu 134
Commande chlog 189
Commande chmanual 189
Commande clearcfg 184
Commande clearlog 118
Commande clock 185
commande dbgshimm 203
Commande dns 139
Commande encaps 141
commande ethtousb 141
Commande exit 117
Commande ffdc 119
Commande firewall 142
Commande fuelg 130
Commande gprofile 143
Commande hashpw 144
Commande help 117
Commande hreport 121
Commande identify 185
Commande ifconfig 145
Commande info 186
Commande led 122
Commande mhlog 121
Commande mvstor 202
commande portcfg 152
Commande portcontrol 153
Commande ports 154
Commande power 127
commande rdmount 155
Commande readlog 124
Commande reset 129
Commande restore 155
Commande restoredefaults 156
Commande roles 157
Commande seccfg 158
commande Serial redirect 132
Commande set 158
Commande snmpalerts 161
Commande spreset 186
Commande sshcfg 164
Commande sslcfg 166
Commande storage 190
  dispositifs de stockage 190
Commande storekeycfg 170
Commande syncrep 171

Commande timeouts 173
Commande TLS 173
Commande trespass 174
Commande uefipw 175
Commande usbeth 176
commande usbfp 176
commande vpd 127
commandes d'utilitaire 117
commandes de configuration 132
Commandes de contrôle de IMM 181
commandes de Service Advisor 186
commandes de surveillance 118
Commandes du plug-in
  accseccfg 132
  adaptateur 200
  aide 117
  alertcfg 134
  alertentries 181
  alimentation 127
  asu 134
  batch 184
  chconfig 187
  chlog 189
  chmanual 189
  clearcfg 184
  clearlog 118
  clock 185
  console 132
  dbgshimm 203
  définir 158
  dhcpinfo 138
  dns 139
  encaps 141
  ethtousb 141
  ffdc 119
  fuelg 130
  gprofile 143
  hashpw 144
  history 118
  hreport 121
  identification 185
  ifconfig 145
  info 186
  keycfg 148
  ldap 149
  led 122
  mhlog 121
  mvstor 202
  ntp 151
  pare-feu 142
  portcfg 152
  portcontrol 153
  ports 154
  pxeboot 131
  quitter 117
  rdmount 155
  readlog 124
  réinitialisation 129
  restaurer 155
  restoredefaults 156
  rôles 157
  sauvegarde 137
  seccfg 158
  smtp 158
  snmp 159
  snmpalerts 161
  spreset 186
  srcfg 163
  sshcfg 164
  ssl 165
  sslcfg 166
  stockage 190
  storekeycfg 170
  syncrep 171
  syshealth 125
  temps 125
  thermal 172
  timeouts 173
  TLS 173
  trespass 174
  uefipw 175
  usbeth 176
  usbfp 176
  utilisateurs 176
  ventilateurs 119
  volts 126
  vpd 127
commandes ipmi
  consommation électrique 74
Commandes IPMI OEM 218
Commandes sans agent 190
Commandes Support 203
Commandes, liste alphabétique 115
commandes, types
  alimentation et redémarrage du serveur 127
  configuration 132
  contrôle de IMM 181
  moniteur 118
  Sans agent 190
  Serial redirect 132
  service advisor 186
  Support 203
  utilitaire 117
comment éviter de revenir au niveau antérieur du microprogramme du système
  configuration 45
Communautés SNMPv1
  gestion 159
commutateur
  mode de sécurité 42
compte local
  création 19
compte utilisateur
  création 176
  suppression 21
Comptes utilisateurs SNMPv3
  configuration 176
configuration
  affectations de ports 36
  comment éviter de revenir au niveau antérieur du microprogramme du système 45
  Comptes utilisateurs SNMPv3 176
  DDNS 139
  DNS (Directory Name System) 139
  Enveloppement du journal IPMI SEL 45
  Ethernet 145
  Ethernet sur USB, paramètres 34
  Ethernet via USB 141
  Groupe d'appareils SKLM 46
  IMPI sur accès KCS 44
  Interruptions SNMPv1 159
  IPMI 35
  IPv4 145
  IPv6 145
  LDAP 149
  limite de connexions simultanées par compte utilisateur 50
  liste de blocage et restriction de temps 37
  niveaux de sécurité du compte utilisateur 132
  Paramètres d'alerte SNMPv3 35
  paramètres de connexion globaux 23
  paramètres de sécurité 39
  Paramètres DNS 33
  Paramètres du DDNS 33
  Paramètres Ethernet 31, 206
  Paramètres LDAP 25
  port de service réseau 153
  port série 152
  port USB du panneau frontal pour la gestion 38
  ports 154
  Protection du système 51

protocoles réseau 31
redirection série à SSH 113
security password manager 50
Serveur LDAP 149
Serveur SSH 44
Serveurs de référentiel principal SKLM 46
SMTP 158
SNMPv1 159
USB 141
configuration de groupe voisin
groupe voisin 108
configuration de XClarity Controller
options de configuration
XClarity Controller 17
Configuration de XClarity Controller
configuration de l'appel vers Lenovo 53
configuration des délais d'attente du serveur 92
configuration du serveur
options de configuration
serveur 69
Configuration du serveur
Configuration RAID 95
Détails RAID 95
informations sur l'adaptateur 69
configuration du stockage
options de configuration
du stockage 95
configuration par défaut
IMM 156
Configuration RAID
Configuration du serveur 95
configuration requise
navigateur Web 6
système d'exploitation 6
connexion à XClarity Controller 12
connexion globale
paramètres 23
connexion réseau 10
adresse IP statique par défaut 10
adresse IP statique, valeur par défaut 10
Adresse IP statique, valeur par défaut 10
consignes et notices 8
console distante
capture d'écran 78
commandes de contrôle de l'alimentation et de redémarrage 77
contrôle absolu de la souris 79
contrôle relatif de la souris 79
contrôle relatif de la souris pour Linux (accélération Linux par défaut) 79
prise en charge de la souris 79
prise en charge du clavier 78
session de support virtuel 76
Visualisation de vidéo 76
console, commande 132
consommation électrique
commandes ipmi 74
Contact SNMPv1
définir 159
Contact SNMPv3
définir 159
contamination gazeuse 239
contamination particulaire et gazeuse 239
contrôle à distance de l'alimentation 77
contrôle absolu de la souris 79
contrôle de la souris
absolu 79
relatif 79
relatif avec accélération Linux par défaut 79
contrôle relatif de la souris 79
contrôle relatif de la souris pour Linux (accélération Linux par défaut) 79
Contrôleur de gestion de la carte mère
demande de signature de certificat 47
contrôleur de gestion de la carte mère (BMC) 1
création
compte utilisateur 176
création d'une page Web de support personnalisée 233

D

date
définir 185
date et heure, XClarity Controller
paramètre 93
dcmi
fonctions et commandes 75
gestion de l'alimentation 75
DDNS
configuration 139
gestion 139
nom de domaine personnalisé 139
Nom de domaine spécifié par le serveur DHCP 139
source de nom de domaine 139
Déclaration BSMI RoHS pour Taïwan 241
déclaration réglementaire relative aux télécommunications 239
définir
Contact SNMPv1 159
Contact SNMPv3 159
date 185
délai d'attente d'inactivité Web 132
heure 185
méthode d'authentification utilisateur 132
MTU 145
négociation automatique 145
nom d'hôte 145
Port CIM via HTTP 154
Port CIM via HTTPS 154
Port CLI SSH 154
Port d'interruptions SNMP 154
port de console distante 154
Port de l'agent SNMP 154
Port du serveur LDAP 149
Port HTTP 154
Port HTTPS 154
Séquence de touches de l'interface de ligne de commande 152
unité de transmission maximale 145
définir les numéros de port 154
définition de l'emplacement et du contact 91
Délai d'attente d'inactivité de session Web 23
délai d'attente d'inactivité Web
définir 132
délais d'attente du serveur
sélections 92
demande de signature de certificat
Contrôleur de gestion de la carte mère 47
Destinataires d'interruption SNMP 65
Détails RAID
Configuration du serveur 95
détection de nœuds voisins
nœud voisin 108
dhcpinfo, commande 138
dispositifs de stockage
Commande storage 190
DNS (Directory Name System)
adressage de serveur 139
Adressage IPv4 139
Adressage IPv6 139
configuration 139
Serveur LDAP 149
documentation en ligne
informations de mise à jour de la documentation 1
informations de mise à jour du microprogramme 1
informations sur les codes d'erreur 1
domaine de recherche
Serveur LDAP 149
Données d'écran d'échec du système d'exploitation

capture 67
données de maintenance 234

E

enregistrement/relecture de vidéo à l'écran
gestion du serveur 79
Enveloppement du journal IPMI SEL
configuration 45
Enveloppement du journal IPMI SEL 45
état d'intégrité du matériel 59
état du serveur
surveillance 59
étendue, sécurité basée sur les rôles
LDAP 176
Ethernet
configuration 145
Ethernet via USB
configuration 141
réacheminement de port 141
Ethernet, paramètres
paramètres 31, 206
événements système actifs
présentation 59
exigences relatives au navigateur 6
Exigences relatives au navigateur Web 6
exigences relatives au système d'exploitation 6
exporter
clé d'activation 106

F

fans, commande 119
Features on Demand (FoD)
gestion 148
installer une fonction 148
supprimer une fonction 148
fenêtre d'événement
journal 63–64
filtre de groupe
LDAP 149
Flex System 1
FoD
gestion 148
installer une fonction 148
supprimer une fonction 148
fonction de console distante 76
fonctionnalité de console distante 76
activation 77
fonctionnalités de niveau standard 2
fonctions de XClarity Controller 2
Fonctions de XClarity Controller
niveau standard 2
sur l'interface Web 13
Fonctions de XClarity Controller fonctionnalités du niveau platinum
niveau platinum 5
fonctions et commandes
dcmi 75
gestionnaire de nœud 74

G

gestion
Adresse MAC 145
certificat du serveur 50
Certificat SKLM 46–47
clé d'activation 148
Communautés SNMPv1 159
DDNS 139
Features on Demand (FoD) 148
FoD 148
utilisateur 176
Gestion BMC
Configuration BMC
réinitialisation des paramètres d'usine 56
restauration de la configuration BMC 56
sauvegarde et restauration de la configuration BMC 55
sauvegarder la configuration BMC 56
gestion centralisée
clés de chiffrement 45
Gestion de groupe voisin 107
gestion de l'alimentation
à l'aide de commandes IPMI 74
dcmi 75
passerelle ipmi 74
Gestion de XClarity Controller
configuration des comptes utilisateur 17
configuration LDAP 17
créer un nouvel utilisateur local 19
créer un rôle 18
paramètres de sécurité 39
Propriétés XClarity Controller
date et heure 93
suppression d'un compte utilisateur 21
gestion des certificats
Accès de l'unité 170
CIM via HTTPS 165–166
client 47
LDAP 165–166
serveur 50
Serveur HTTPS 165–166
Serveur SSH 164
gestion des certificats du client
affecté automatiquement 47
Signé par une autorité de certification 47
Gestion des certificats SKLM
page d'accès de l'unité 46–47
Gestion des licences 105
gestion du serveur
délais d'attente du serveur, configuration 92
Données d'écran d'échec du système d'exploitation 67
enregistrement/relecture de vidéo à l'écran 79
microprogramme de serveur 99–100
mode d'amorçage du système 69
ordre d'amorçage du système 69
unique 70
gestionnaire de nœud
fonctions et commandes 74
groupe d'appareils
page d'accès de l'unité 46
Groupe d'appareils SKLM
configuration 46
groupe voisin
approvisionnement 108
configuration 108
fonctionnalité 107
groupe voisin 107

H

heure
définir 185
historique de maintenance 65
history, commande 118

I

IMM
configuration par défaut 156
réinitialisation 186
restaurer la configuration 155–156

spreset 186
IMPI sur accès KCS
configuration 44
Informations de contact pour l'importation et l'exportation de Taïwan 241
informations sur l'adaptateur
Configuration du serveur 69
informations système 60
affichage 60
installation
clé d'activation 105, 148
installer une fonction
Features on Demand (FoD) 148
FoD 148
interface de ligne de commande (CLI)
accès 113
connexion 113
description 113
fonctionnalités et limitations 114
syntaxe de commande 114
Interface IPMI
description 205
interface Web
connexion à l'interface Web 12
interface Web, ouverture et utilisation 9
Interruptions SNMPv1
configuration 159
Introduction aux MIB 8
inventaire de stockage 96
IPMI
configuration 35
gestion du serveur à distance 205
IPMItool 205
IPv4
configuration 145
IPv6 9
configuration 145

J

journal d'audit 64
Journal d'audit étendu
journal d'audit étendu 50
journal des données de maintenance
collecte 91
téléchargement en cours 91
Journal des événements 63

K

keycfg, commande 148

L

LDAP
attribut d'autorisation de connexion 149
attribut de recherche de groupe 149
configuration 17, 149
étendue, sécurité basée sur les rôles 176
filtre de groupe 149
gestion des certificats 165–166
nom de cible serveur 149
sécurité 165–166
sécurité étendue basée sur les rôles 176
Utilisateurs Active Directory 176
ldap, commande 149
limite de connexions simultanées par compte utilisateur
configuration 50
Limite de connexions simultanées par compte utilisateur
limite de connexions simultanées par compte utilisateur 50
liste de blocage et restriction de temps
paramètres 37
Liste des commandes par ordre alphabétique 115

M

marques 238
méthode d'authentification utilisateur 17
définir 132
méthode de liaison
Serveur LDAP 149
méthodes de montage de support 80
microprogramme
serveur de vues 127
microprogramme de serveur
mise à jour 99–100
Microprogramme de serveur ThinkSystem
description 1
microprogramme, serveur
mise à jour 99–100
minimum, niveaux
TLS 173
modes d'écran de console distante 80
module de gestion avancée 1
mot de passe
Serveur LDAP 149
utilisateur 176
mot de passe crypté 21
MTU
définir 145

N

négociation automatique
définir 145
niveaux basés sur les rôles
opérateur 143
rbs 143
superviseur 143
niveaux de sécurité du compte utilisateur
configuration 132
nœud voisin
détection 108
nom d'hôte
définir 145
Serveur LDAP 149
Serveur SMTP 158
nom d'hôte, serveur
LDAP 149
nom de cible serveur
LDAP 149
nom distinctif du client
Serveur LDAP 149
nom distinctif racine
Serveur LDAP 149
nom distinctif, client
Serveur LDAP 149
nom distinctif, racine
Serveur LDAP 149
notifications par courrier électronique et notifications syslog 65
nouveau rôle
création 18
ntp, commande 151
numéro de port
Serveur LDAP 149
Serveur SMTP 158
numéros de port
définir 154
numéros de téléphone du service et support logiciel 235

O

Obtenir de l'aide 233
OneCLI 1
Onglet d'accès de l'unité
  option de sécurité 45–47
Onglet Server Management
  option de gestion de l'alimentation 71
option
  SKM 45
option de gestion de l'alimentation
  actions d'alimentation 73
  Onglet Server Management 71
  redondance de l'alimentation 71
  stratégie de plafonnement énergétique 72
  stratégie de restauration de l'alimentation 72
option de message Trespass 93
option de sécurité
  Onglet d'accès de l'unité 45–46
Option de sécurité
  Onglet d'accès de l'unité 46–47
outils
  IPMItool 205

P

page d'accès de l'unité
  configuration 46
  Gestion des certificats SKLM 46–47
  groupe d'appareils 46
  serveurs de gestion de clé 46
page Web de support personnalisée 233
page Web de support, personnalisée 233
paramètre
  définition des date et heure XClarity Controller 93
paramètres
  affectations de ports 36
  Alerte SNMP 35
  avancés 31, 51, 206
  connexion globale 23
    paramètres de stratégie de sécurité de compte 24
  DDNS 33
  DNS (Directory Name System) 33
  Ethernet 31, 206
  Ethernet via USB 34
  LDAP 25
  liste de blocage et restriction de temps 37
  Protection du système 51
  sécurité 39
  Serveur SSH 44
Paramètres cryptographiques
  Paramètres cryptographiques 51
paramètres de connexion globaux
  paramètres de stratégie de sécurité de compte 24
paramètres réseau
  Commandes IPMI 35
Paramètres SNMPv3
  utilisateur 176
particulaire, contamination 239
passerelle ipmi
  gestion de l'alimentation 74
  via XClarity Controller 74
personnalisé, nom de domaine
  DDNS 139
Port CIM via HTTP
  définir 154
Port CIM via HTTPS
  définir 154
Port CLI SSH
  définir 154
Port d'interruptions SNMP
  définir 154
port de console distante
  définir 154
Port de l'agent SNMP
  définir 154
port de service réseau
  configuration 153
Port du serveur LDAP
  définir 149
Port HTTP
  définir 154
Port HTTPS
  définir 154
port série
  configuration 152
ports
  afficher ouverts 154
  configuration 154
  définir les numéros 154
préconfiguré
  Serveur LDAP 149
présentation 59
  mode de sécurité 39
  protection du système 51
  ssl 42
  tableau de bord de sécurité 39
prise en charge de la souris dans la console distante 79
prise en charge de la souris par la fonction de console distante 79
prise en charge du clavier dans la console distante 78
problèmes liés aux erreurs de montage de support 89
propriétés du protocole de réseau
  affectations de ports 36
  comment éviter de revenir au niveau antérieur du microprogramme du système 45
  DDNS 33
  DNS (Directory Name System) 33
  Ethernet via USB 34
  IMPI sur accès KCS 44
  IPMI 35
  liste de blocage et restriction de temps 37
  Paramètres d'alerte SNMP 35
  Paramètres Ethernet 31, 206
propriétés du serveur
  définition de l'emplacement et du contact 91
  serveur, configuration 91
protection du système
  Protection du système 51
Protection du système
  paramètres 51
pxeboot, commande 131

R

réacheminement de port
  Ethernet via USB 141
redémarrage de XClarity Controller 57
redirection série à SSH 113
réinitialisation
  IMM 186
remarques 237
remarques importantes 238
restaurer la configuration
  IMM 155–156
retrait
  clé d'activation 106, 148

S

sécurité
  Accès de l'unité 170
  CIM via HTTPS 165–166
  Gestion des certificats SSL 43
  LDAP 165–166
  passer à un autre mode de sécurité 42

Présentation de la protection du système 51
présentation de SSL 42
présentation du mode de sécurité 39
présentation du tableau de bord de sécurité 39
Serveur HTTPS 165–166
Serveur SSH 44, 164
traitement des certificats SSL 42
sécurité étendue basée sur les rôles
LDAP 176
security password manager
configuration 50
security password manager 50
Séquence de touches de l'interface de ligne de commande
définir 152
Serial over LAN 205
serveur
gestion des certificats 50
options de configuration 69
Serveur HTTPS
gestion des certificats 165–166
sécurité 165–166
Serveur LDAP
Adresse IP 149
Attribut de recherche UID 149
configuration 149
DNS (Directory Name System) 149
domaine de recherche 149
méthode de liaison 149
mot de passe 149
nom d'hôte 149
nom distinctif du client 149
nom distinctif racine 149
numéro de port 149
préconfiguré 149
Serveur SSH
gestion des certificats 164
sécurité 164
serveur, configuration
propriétés du serveur 91
serveurs de gestion de clé
configuration 46
page d'accès de l'unité 46
Serveurs Flex 1
service et support
avant d'appeler 233
logiciel 235
matériel 235
service et support matériel et numéros de téléphone 235
Signé par une autorité de certification
certificat 47
SKLM
serveurs de gestion de clé 46
SKM
option 45
SMTP
adresse IP du serveur 158
configuration 158
nom d'hôte du serveur 158
numéro de port serveur 158
smtp, commande 158
snmp, commande 159
SNMPv1
configuration 159
sortie de la session de console distante 91
source de nom de domaine
DDNS 139
spécifié par le serveur DHCP, nom de domaine
DDNS 139
srcfg, commande 163
SSL
gestion des certificats 43
traitement des certificats 42
ssl, commande 165
stockage
options de configuration 95
support multilingue 7
supprimer
utilisateur 176
supprimer groupe
enable, disable (activer, désactiver) 143
supprimer une fonction
Features on Demand (FoD) 148
FoD 148
surveillance de l'alimentation
à l'aide de commandes IPMI 74
surveillance de l'état du serveur 59
syshealth, commande 125
système, utilisation
affichage 62

T

téléphone, numéros 235
temps, commande 125
thermal, commande 172
TLS
niveau minimum 173

U

unique
Configuration 70
unité de transmission maximale
définir 145
USB
configuration 141
users, commande 176
utilisateur
Clés SSH 176
gestion 176
mot de passe 176
Paramètres SNMPv3 176
supprimer 176
utilisateurs
affichage en cours 176
Utilisateurs Active Directory
LDAP 176
utilisation
événements dans le journal d'audit 64
événements dans le journal des événements 63
fonction de console distante 76
utilisation du système 62

V

Visualisation de vidéo
capture d'écran 78
commandes de contrôle de l'alimentation et de redémarrage 77
contrôle absolu de la souris 79
contrôle relatif de la souris 79
contrôle relatif de la souris pour Linux (accélération Linux par défaut) 79
mode couleur vidéo 78
prise en charge de la souris 79
voisin, groupe
approvisionnement 108
configuration 108
fonctionnalité 107
voisin, nœud
détection 108
volts, commande 126

X

XClarity Controller
caractéristiques 2
configurer le protocole réseau 31
connexion réseau 10
description 1
interface Web 9
Niveau Platinum de XClarity Controller 2
Niveau standard de XClarity Controller 2
nouvelles fonctions 1
options de configuration 17
passerelle ipmi 74
redirection série 113
XClarity Provisioning Manager
Setup utility 10

Lenovo

Numéro de page : SP47A30085

Printed in China

(1P) P/N: SP47A30085