Dell Chassis Management Controller version 3.3 pour Dell EMC PowerEdge VRTX

Guide de l'utilisateur

July 2020
Rév. A00

DELL EMC

Remarques, précautions et avertissements

REMARQUE : Une REMARQUE indique des informations importantes qui peuvent vous aider à mieux utiliser votre produit.

PRÉCAUTION : ATTENTION vous avertit d'un risque de dommage matériel ou de perte de données et vous indique comment éviter le problème.

AVERTISSEMENT : un AVERTISSEMENT signale un risque d'endommagement du matériel, de blessure corporelle, voire de décès.

Table des matières

1

Présentation

Le Dell Chassis Management Controller (CMC) pour Dell EMC PowerEdge VRTX est une solution logicielle et matérielle de gestion de systèmes conçue pour gérer le châssis **PowerEdge VRTX**. Le CMC dispose de son propre microprocesseur et de sa propre mémoire, et il est alimenté par le châssis modulaire auquel il est branché.

Le CMC permet à l'administrateur informatique de réaliser les opérations suivantes :

- Affichage de l'inventaire
- Exécution de tâches de configuration et de surveillance
- Mise sous tension ou hors tension à distance du châssis et des serveurs
- Activation d'alertes pour les événements des serveurs et des composants du module serveur
- Affichage et gestion du contrôleur de stockage et des disques dans le châssis VRTX
- Gestion du sous-système PCIe dans le châssis VRTX
- Fourniture d'une interface de gestion un à plusieurs avec les modules iDRAC et les modules E/S du châssis

Vous pouvez configurer le châssis PowerEdge VRTX à l'aide d'un CMC unique, ou des CMC redondants. Dans les configurations avec CMC redondants, si le CMC principal perd la communication avec le châssis ou le réseau de gestion, le CMC de secours se charge de la gestion des châssis.

Le CMC fournit des fonctions de gestion de système pour les serveurs. La gestion de l'alimentation et la gestion thermique constituent les principales des fonctions du CMC énumérées ci-dessous :

- Gestion automatique des températures et de la consommation au niveau du châssis et en temps réel.
  - Le CMC surveille les conditions d'alimentation du système et prend en charge le mode DPSE (Dynamic Power Supply Engagement) facultatif. Ce mode permet au CMC d'améliorer l'efficacité énergétique en configurant les blocs d'alimentation lorsque le serveur est en veille et en gérant de façon dynamique les exigences en termes de charge et de redondance.
  - CMC donne des informations en temps réel sur la consommation, avec une consignation des limites haute et basse accompagnée d'un horodatage.
  - Le contrôleur CMC permet de définir une limite de puissance maximale de boîtier facultative (limitation de la puissance d'entrée du système) qui envoie des alertes et exécute des actions, telle que limiter la consommation électrique des serveurs et bloquer la mise sous tension des nouveaux serveurs, pour maintenir le boîtier dans la limite de puissance maximale définie.
  - Le contrôleur CMC surveille et contrôle automatiquement les fonctions des ventilateurs selon les mesures de température ambiante et interne.
  - CMC comporte des fonctions complètes d'inventaire et de consignation des erreurs ou des états.
- Le contrôleur CMC permet de centraliser la configuration des paramètres et éléments suivants :
  - Réseau et sécurité du boîtier Dell PowerEdge VRTX
  - Redondance de l'alimentation et définition de seuils
  - Réseau des commutateurs d'E/S et du module iDRAC
  - Premier périphérique d'amorçage du module serveur
  - Vérifications de cohérence de la structure d'E/S entre le module d'E/S et les serveurs. Le CMC désactive également les composants, si nécessaire, afin de protéger le matériel du système.
  - Sécurité des accès utilisateur
  - Les composants de stockage, y compris le mode de tolérance des pannes pour les contrôleurs de stockage.
  - Logements PCIe

Vous pouvez configurer le contrôleur CMC pour qu'il envoie des alertes ou des alertes par interruption SNMP ou des erreurs telles que température, configuration matérielle incorrecte, panne de courant, vitesse de ventilateur et ventilateurs.

Sujets :

Nouveautés de cette version

Cette version de CMC pour Dell EMC PowerEdge VRTX prend en charge :

- Amélioration du profil de châssis pour configurer les paramètres réseau iDRAC.
- Application de profils de serveur à l'aide de l'interface racadm.
- Gestion des failles de sécurité open source.

Principales fonctions

Les fonctions CMC peuvent être des fonctions de gestion ou des fonctions de sécurité.

Fonctions de gestion

Le contrôleur CMC offre les fonctionnalités de gestion suivantes :

- Environnement CMC redondant
- Enregistrement DDNS (Système de noms de domaine dynamique) pour IPv4 et IPv6
- Gestion des connexions et configuration des utilisateurs locaux, Active Directory et LDAP.
- Les options de refroidissement avancé, telles que ECM (Enhanced Cooling Mode) et Compensation de ventilation peuvent être activées pour augmenter la capacité de refroidissement afin d'améliorer les performances.
- Gestion et surveillance à distance du système à l'aide de SNMP, d'une interface Web, d'une console KVM ou d'une connexion Telnet/SSH
- Surveillance : permet d'accéder aux informations sur le système et à l'état des composants
- Accès aux journaux des événements système : accès au journal du matériel et au journal du châssis
- Mises à jour micrologicielles des divers composants du châssis : permet de mettre à jour le micrologiciel du contrôleur CMC, d'iDRAC sur les serveurs, de l'infrastructure de châssis et du stockage dans le châssis.
- Mise à jour micrologicielle des composants des serveurs, tels que le BIOS, les contrôleurs de réseau, les contrôleurs de stockage, etc. sur plusieurs serveurs dans le châssis à l'aide du Lifecycle Controller.
- Intégration du logiciel Dell OpenManage : permet de lancer l'interface Web CMC à partir de Dell OpenManage Server Administrator ou d'OpenManage Essentials (OME) 1.2.
- Alertes CMC : signale les problèmes potentiels du nœud géré au moyen d'un message e-mail syslog distant ou d'une interruption SNMP.
- Gestion de l'alimentation à distance : offre des fonctionnalités de gestion de l'alimentation à distance, telles que la mise hors tension et la réinitialisation des composants du châssis, à partir d'une console de gestion.
- Rapport sur l'alimentation
- Cryptage SSL (Secure Sockets Layer) : permet une gestion sécurisée du système distant via l'interface Web.
- Point de lancement de l'interface Web iDRAC (Integrated Dell Remote Access Controller).
- Prise en charge de la gestion WS
- Fonctionnalité FlexAddress : remplace les adresses WWN/MAC (World Wide Name/Media Access Control) définies en usine par les adresses WWN/MAC attribuées par le châssis pour un logement spécifique.
- Prise en charge de la fonctionnalité iDRAC I/O Identity pour l'inventaire d'adresses WWN/MAC.
- Affichage graphique de l'état et de l'intégrité des composants de châssis
- Prise en charge des serveurs à connecteur unique ou multiple
- L'Assistant Configuration iDRAC LCD prend en charge la configuration réseau iDRAC
- Connexion unique iDRAC
- Prise en charge du protocole NTP
- Pages de résumé du serveur, de rapports de l'alimentation et de contrôle de l'alimentation optimisées
- Basculement CMC forcé et réattribution de sièges virtuelle de serveurs
- Gestion de plusieurs châssis. Celle-ci permet à jusqu'à huit autres châssis d'être visibles depuis le châssis maître.

- Configuration des composants de stockage dans le châssis.
- Association des logements PCIe aux serveurs et à leur identification.

Fonctionnalités de sécurité

CMC dispose des fonctionnalités de sécurité suivantes :

- Gestion de la sécurité au niveau des mots de passe : empêche tout accès non autorisé à un système distant.
- Authentification utilisateur centralisée via :
  - Active Directory à l'aide d'un schéma standard ou d'un schéma étendu (facultatif).
  - Identifiants et mots de passe utilisateur stockés dans le matériel.
- Autorité basée sur le rôle qui permet à un administrateur de configurer des privilèges spécifiques pour chaque utilisateur
- Définition de l'ID utilisateur et du mot de passe via l'interface Web. L'interface Web prend en charge le cryptage SSL 3.0 128 bits et 40 bits (pour les pays pour lesquels le cryptage 128 bits n'est pas acceptable).

  REMARQUE : Telnet ne prend pas en charge le cryptage SSL.
- Ports IP configurables (si applicable)
- Limites d'échecs d'ouverture de session par adresse IP, avec blocage de l'ouverture de session à partir de l'adresse IP lorsque la limite est dépassée.
- Délai de session configurable, et plus d'une session simultanée
- Plage d'adresses IP limitée pour les clients se connectant au CMC.
- Secure Shell (SSH) qui utilise une couche cryptée pour une sécurité plus élevée
- Connexion directe, authentification bifactorielle et authentification par clé publique

Présentation du châssis

Cette illustration montre une vue des connecteurs CMC.

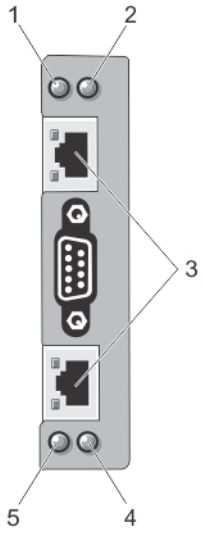


Figure 1. Connecteurs et voyants CMC

Tableau 1. Connecteurs et voyants CMC

Élément	Voyant, bouton ou connecteur
1	Voyant d'état/d'identification (CMC 1)
2	Voyant d'alimentation (CMC 1)
3	Ports des connecteurs CMC (2)
4	Voyant d'alimentation (CMC 2)
5	Voyant d'état/d'identification (CMC 2)

Une vue du panneau arrière du châssis est fournie ici accompagnée d'un tableau qui répertorie les éléments et les périphériques disponibles dans le contrôleur CMC.

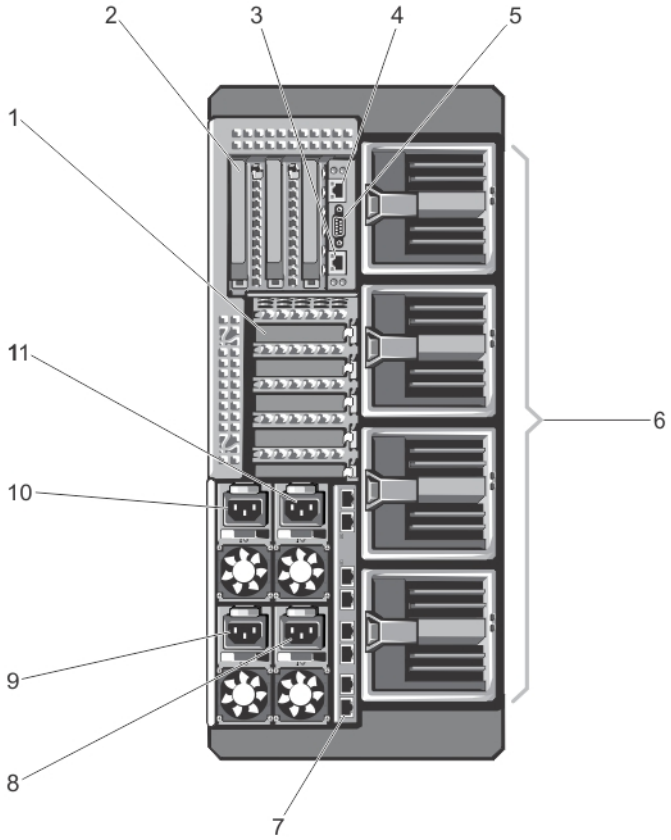


Figure 2. Panneau arrière du CMC

Tableau 2. Panneau arrière du CMC : pièces

Élément	Voyant, bouton ou connecteur
1	Logements de carte d'extension PCIe demi-hauteur (5)
2	Logements pleine hauteur pour carte d'extension PCIe (3)
3	Port Ethernet GB CMC (CMC-2)
4	Port Ethernet GB CMC (CMC-1)
5	Connecteur série
6	Modules de ventilation (4)
7	Ports de module E/S
8	Bloc d'alimentation électrique 4
9	Bloc d'alimentation électrique 3
10	Bloc d'alimentation électrique 1
11	Bloc d'alimentation électrique 2

Une vue du panneau avant du châssis est fournie ici accompagnée d'un tableau qui répertorie les éléments et les périphériques disponibles dans le CMC.

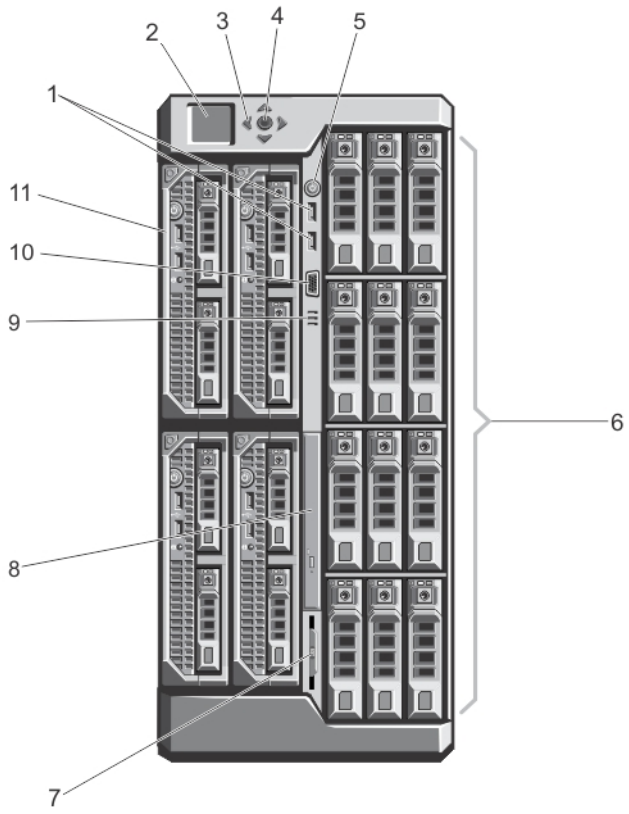


Figure 3. Voyants et fonctions du panneau avant : châssis de disque dur de 3,5 pouces

Tableau 3. Panneau avant : voyants et fonctions

Élément	Voyant, bouton ou connecteur	Description
1	Connecteurs USB (2)	Permettent de connecter un clavier et une souris au système.
2	Écran LCD	Fournit des informations système et des messages d'erreur et d'état qui indiquent si le système fonctionne correctement ou s'il requiert une intervention.
3	Boutons de défilement des menus LCD (4)	Fait avancer le curseur étape par étape.
4	Bouton de sélection (vérification)	Sélectionne et enregistre un élément sur l'écran LCD et passe à l'écran suivant.
5	Voyant de mise sous tension, bouton d'alimentation de boîtier	Le voyant de mise sous tension s'allume lorsque le boîtier est mis sous tension. Le bouton d'alimentation contrôle la sortie du bloc d'alimentation vers le système.
6	Disques durs (HDD)	**Boîtier de disque dur de 2,5 pouces** Jusqu'à vingt-cinq disques durs de 2,5 pouces remplaçables à chaud. **Boîtier de disque dur de 3,5 pouces** Jusqu'à douze disques durs de 3,5 pouces remplaçables à chaud.
7	Plaquette d'information	Panneau d'étiquettes escamotable qui permet d'enregistrer les informations système telles que numéro de service, NIC, adresse MAC, puissance électrique nominale du système et marques Worldwide Regulatory Agency.
8	Lecteur optique (en option)	Un lecteur SATA DVD-ROM ou DVD+/-RW (en option).
9	Entrées d'air	Entrées d'air pour le capteur de température. **REMARQUE : Pour assurer le bon refroidissement, n'obstruez pas les entrées d'air.**
10	Connecteur vidéo	Permet de connecter un écran au système.

Tableau 3. Panneau avant : voyants et fonctions (suite)

Élément	Voyant, bouton ou connecteur	Description
11	Modules serveur	Jusqu'à quatre modules serveur PowerEdge M520, M620, M630 ou M640 ou 2 modules serveur M820 configurés pour le boîtier.

Version CMC minimale

Le tableau suivant répertorie la version CMC minimale requise pour prendre en charge les modules serveur indiqués.

Tableau 4. Version CMC minimale pour les modules serveurs

Serveurs	Version minimale de CMC
PowerEdge M520	CMC 1.36
PowerEdge M620	CMC 1.36
PowerEdge M820	CMC 1.36
PowerEdge M630	CMC 2.00
PowerEdge M830	CMC 2.00
PowerEdge M640	CMC 3.00

Le tableau suivant répertorie la version CMC minimale requise pour prendre en charge les module IO indiqués.

Tableau 5. Version CMC minimale pour les modules IO

Commutateurs IOM	Version minimale de CMC
Transfert R1 VRTX 1Gb	CMC 1.20
Commutateur R1-2401 VRTX 1 GbE	CMC 1.20
Commutateur R1-2210 VRTX 10Gb	CMC 2.00

Connexions d'accès à distance prises en charge

Le tableau suivant répertorie les RAC (Remote Access Controllers - Contrôleurs d'accès à distance) pris en charge.

Tableau 6. Connexions d'accès à distance prises en charge

Connexion	Fonctions
Ports d'interface réseau CMC	· Port GB : interface réseau dédiée pour l'interface Web CMC · Prise en charge de DHCP · Interruptions SNMP et notifications des événements par e-mail · Interface réseau pour le micrologiciel iDRAC et les modules d'E/S · Prise en charge de la console de commande Telnet/SSH et des commandes CLI RACADM, y compris les commandes de démarrage du système, de réinitialisation, de mise sous tension et d'arrêt
Port série	· Prise en charge de la console série et des commandes CLI RACADM, y compris les commandes d'amorçage, de réinitialisation, de mise sous et hors tension des systèmes. · Prise en charge des échanges binaires pour les applications conçues pour communiquer avec un protocole binaire avec un type particulier de module d'E/S. · Le port série peut être connecté en interne à la console série d'un serveur ou à un module d'E/S (IOM) à l'aide de la commande connect (ou racadm connect). · Permet d'accéder uniquement au contrôleur CMC actif.

Plates-formes prises en charge

Le CMC prend en charge les serveurs modulaires conçus pour la plate-forme PowerEdge VRTX. Pour plus d'informations sur la compatibilité avec le CMC, voir la documentation de votre périphérique.

Pour connaître les dernières plateformes prises en charge, voir les *notes de mise à jour de Dell Chassis Management Controller (CMC) version 3.3 pour Dell PowerEdge VRTX* disponibles sur **dell.com/support/manuals**.

Navigateurs Web pris en charge

Les navigateurs Web suivants sont pris en charge par Dell PowerEdge VRTX :

- Microsoft Internet Explorer 11
- Microsoft EDGE
- Safari version 10.1.2
- Safari version 11.1.2
- Mozilla Firefox 61
- Mozilla Firefox 62
- Google Chrome 68
- Google Chrome 69

REMARQUE : Par défaut, TLS 1.1 et TLS 1.2 sont pris en charge dans cette version. Cependant, pour activer TLS 1.0 utilisez la commande racadm suivante :

```
$ racadm config -g cfgRacTuning -o cfgRacTuneTLSProtocolVersionEnable TLSv1.0+
```

Gestion des licences

Les fonctions CMC sont disponibles selon la licence (CMC Express ou CMC Enterprise) achetée. Seules les fonctions sous licence sont disponibles dans les interfaces qui permettent de configurer ou d'utiliser le contrôleur CMC, telles que l'interface Web CMC, RACADM, WS-MAN, etc. La fonction de gestion des licences CMC et de mise à jour du micrologiciel est toujours disponible via l'interface Web CMC et RACADM.

Types de licences

Les types de licences proprosés sont les suivants :

- Évaluation de 30 jours et extension : la licence expire au bout de 30 jours. La période d'évaluation peut être prolongée de 30 jours. Les licences d'évaluation reposent sur la durée et le décompte du temps démarre lorsque le système est mis sous tension.
- Perpétuelle : la licence est liée au numéro de service et elle est prermanente.

Obtention de licences

Pour obtenir des licences, procédez de l'une des manières suivantes :

- E-mail : la licence est jointe à un e-mail envoyé après sa demande auprès du centre d'assistance technique.
- Portail en libre-service : un lien d'accès au portail en libre-service est disponible depuis le contrôleur CMC. Cliquez sur ce lien pour ouvrir le portail en libre-service d'octroi de licences sur Internet pour acheter des licences. Pour plus d'informations, consultez l'aide en ligne de la page du portail en libre-service.
- Point de vente : la licence est acquise lors de la commande d'un système.

Opérations de licence

Avant d'exécuter les tâches de gestion des licences, veillez à obtenir les licences. Pour plus d'informations, voir le document Overview and Feature Guide disponible sur le site support.dell.com.

Vous pouvez exécuter les opérations de licences suivantes à l'aide du CMC, RACADM et WS-MAN pour la gestion des licences une-à-une et Dell License Manager pour la gestion des licences une-à-plusieurs :

REMARQUE : Si vous avez acheté un système avec toutes les licences préinstallées, la gestion des licences n'est pas nécessaire.

- Afficher : affichage des informations de la licence en cours.
- Importer : après l'acquisition d'une licence, stockez la licence dans un emplacement de stockage local et importez-la vers le contrôleur CMC en utilisant l'une des interfaces prises en charge. La licence est importée si les vérifications de validation auxquelles elle est soumise aboutissent.

  REMARQUE : Pour un nombre limité de fonctions, il peut être nécessaire de redémarrer le contrôleur CMC pour activer les fonctions.
- Exporter : exportez la licence installée vers un périphérique de stockage externe pour disposer d'une sauvegarde ou la réinstaller après le remplacement d'un composant de service. Le nom de fichier et le format d'une licence exportée sont <EntitlementID>.xml.
- Supprimer : supprimez la licence affectée à un composant si le composant manque. Une fois la licence supprimée, elle n'est plus stockée dans le contrôleur CMC et les fonctions de base du produit sont activées.
- Remplacer : remplacement de la licence pour prolonger la période d'évaluation d'une licence, changer le type de licence (remplacement d'une licence d'évaluation par une licence achetée) ou étendre une licence expiré.
- Une licence d'évaluation peut être remplacée par une licence d'évaluation mise à niveau ou une licence achetée.
- Une licence achetée peut être remplacée par une licence mise à niveau ou mise à jour. Pour plus d'informations sur la licence, cliquez sur le portail de gestion de licences du logiciel Dell .
- En savoir plus : en savoir plus sur une licence installée ou les licences disponibles pour un composant installé sur le serveur.

  REMARQUE : Pour que l'option En savoir plus affiche la page correcte, veillez à ajouter *.dell.com à la liste des sites de confiance dans les paramètres de sécurité. Pour plus d'informations, voir la documentation d'aide d'Internet Explorer.

État ou condition de composant de licence et opérations disponibles

Le tableau suivant répertorie les opérations de licence disponibles en fonction de l'état ou de la condition d'une licence.

Tableau 7. Opérations de licence en fonction de l'état et de la condition

État/Condition ou état du composant	Importer	Exportation	Supprimer	Remplacer	En savoir plus
Connexion non-administrateur	Non	Oui	Non	Non	Oui
Licence active	Oui	Oui	Oui	Oui	Oui
Licence expirée	Non	Oui	Oui	Oui	Oui
License installée, mais composant manquant	Non	Oui	Oui	Non	Oui

Gestion des licences à l'aide de l'interface Web CMC

Pour gérer les licences à l'aide de l'interface Web CMC, accédez à **Présentation du châssis** > **Configurer** > **Licences** .

Avant d'importer une licence, veillez à enregistrer un fichier de licence valide sur votre système local ou sur un partage réseau accessible depuis le contrôleur CMC. La licence est incorporée ou envoyée par e-mail depuis le **Portail Web en libre-service** ou à l'aide de l'outil de gestion des clés de licence.

La page **Gestion des licences** affiche les licences associées aux périphériques ou les licences installées des périphériques absents du système. Pour plus d'informations sur l'importation, l'exportation, la suppression ou le remplacement d'une licence, voir l'*Aide en ligne*.

Gestion des licences à l'aide de l'interface RACADM

Pour gérer les licences à l'aide des commandes RACADM, utilisez la sous-commande de licence suivante.

```
racadm license <type de commande de licence>
```

Pour plus d'informations sur les commandes RACADM, voir le document *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX) sur le site dell.com/support/Manuals.

Fonctions pouvant faire l'objet d'une licence dans le CMC

Vous trouverez dans le tableau suivant la liste des fonctions CMC qui sont activées en fonction de votre licence.

Tableau 8. Fonctions pouvant faire l'objet d'une licence

Fonction	Express	Enterprise	Remarques
Réseau CMC	Oui	Oui	
Port série CMC	Oui	Oui	
RACADM (SSH, local et distant)	Oui	Oui	
Sauvegarde de la configuration du CMC	Non	Oui	
Restauration de la configuration du CMC	Oui	Oui	
WS-MAN	Oui	Oui	
SNMP	Oui	Oui	
Telnet	Oui	Oui	
SSH	Oui	Oui	
Interface Web	Oui	Oui	
Alertes par e-mail	Oui	Oui	
Déploiement LCD	Oui	Oui	
Gestion d'iDRAC étendue	Oui	Oui	
Syslog distant	Non	Oui	
Services d'annuaire	Non*	Oui	*Pour le paramétrage du service d'annuaire autre que par défaut, seule est autorisée l'option Réinitialiser les services d'annuaire avec la licence Express. Cette option rétablit les paramètres par défaut des services d'annuaire.
Connexion unique iDRAC	Non	Oui	
Authentification bifactorielle	Non	Oui	
Authentification PK	Non	Oui	
Partage de fichier à distance	Oui	Oui	

Tableau 8. Fonctions pouvant faire l'objet d'une licence (suite)

Fonction	Express	Enterprise	Remarques
Gestion des ressources de logement	Non	Oui	
Seuil maximal de puissance au niveau de l'enceinte	Non*	Oui	*Pour le paramétrage du seuil maximal de puissance autre que par défaut, seule l'option de restauration du seuil maximal de puissance est autorisée avec la licence Express. Cette option rétablit les paramètres par défaut définis en usine du seuil de puissance.
Enclenchement dynamique des blocs l'alimentation	Non*	Oui	*Pour les paramètres DPSE autres que par défaut, seule l'option Restaurer DPSE est autorisée avec la licence Express. Cette option rétablit les paramètres DPSE par défaut définis en usine.
Gestion de plusieurs châssis :	Non	Oui	
Configuration avancée	Non	Oui	
Sauvegarde au niveau de l'enceinte	Non	Oui	
Activation de FlexAddress	Non*	Oui	*Pour les paramètres FlexAddress autres que par défaut, seule l'option Restaurer les valeurs par défaut est autorisée avec la licence Express. Cette option rétablit les paramètres FlexAddress par défaut définis en usine.
Mappage de l'adaptateur PCIe	Oui*	Oui	*Au maximum, deux adaptateurs PCIe peuvent être affectés par serveur avec la licence Express.
Mappage Adaptateur virtuel à logement	Non*	Oui	*Pour le mappage autre que par défaut d'adaptateur virtuel, seul le mappage par défaut est autorisé avec la licence Express. L'option Restaurer les valeurs par défaut rétablit les valeurs par défaut de mappage d'adaptateur virtuel définies en usine
Mappage Adaptateur virtuel à logement	Oui	Oui	
Clonage de serveur	Non	Oui	
Mise à jour de micrologiciel de serveur un à plusieurs	Non	Oui	
Configuration un-à-plusieurs d'iDRAC	Non	Oui	
Identité de démarrage	Non	Oui	
Profil du châssis	Non	Oui	
Déploiement rapide	Non	Oui	

Affichage des versions traduites de l'interface Web CMC

Pour afficher les versions traduites de l'interface Web du contrôleur CMC, lisez la documentation de votre navigateur Web.

Applications de console de gestion prises en charge

Le contrôleur CMC peut être intégré à Dell OpenManage Console. Pour plus d'informations, voir la documentation de la console OpenManage sur le site **dell.com/support/manuals**.

Comment utiliser ce guide

Le contenu de ce Guide de l'utilisateur permet d'exécuter les tâches en utilisant :

- L'interface Web : seules les informations liées aux tâches sont indiquées ici. Pour plus d'informations sur les champs et les options, voir l'*Aide en ligne CMC pour Dell PowerEdge VRTX* à laquelle vous pouvez accéder depuis l'interface Web.
- Les commandes RACADM : la commande ou l'objet RACADM que vous devez utiliser est indiqué ici. Pour plus d'informations sur une commande RACADM, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX* sur le site **dell.com/cmcmanuals**.

Autres documents utiles

Pour accéder aux documents à partir du site de support Dell. En complément de ce guide de référence, vous pouvez accéder aux guides suivants disponibles sur **dell.com/support/manuals**.

- L'*aide en ligne CMC pour VRTX* fournit des informations sur l'utilisation de l'interface Web. Pour accéder à l'aide en ligne, cliquez sur **Aide** dans l'interface Web du CMC.
- Le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller version 3.3 pour Dell PowerEdge VRTX* explique comment utiliser les fonctionnalités RACADM de VRTX.
- Les *notes de mise à jour de Dell Chassis Management Controller (CMC) pour Dell PowerEdge VRTX version 3.3*, disponibles à l'adresse **dell.com/cmcmanuals**, contiennent les mises à jour de dernière minute du système ou de la documentation, ou les informations de référence technique avancée destinées aux utilisateurs et techniciens expérimentés.
- Le *Guide de l'utilisateur de l'Integrated Dell Remote Access Controller (iDRAC)* explique comment installer, configurer et entretenir l'iDRAC sur des systèmes gérés.
- La *Matrice de compatibilité du sous-système de stockage Dell PowerEdge VRTX* fournit des informations sur les versions de base du sous-système de stockage PowerEdge VRTX. Ce document est disponible en ligne sur **dell.com/support/manuals**.
- Le *Guide de l'utilisateur Dell OpenManage Server Administrator* donne des informations sur l'installation et l'utilisation de Server Administrator.
- *Guide de référence SNMP de Dell OpenManage pour iDRAC et Chassis Management Controller* fournit des informations à propos des SNMP de MIB.
- Le manuel *Guide de l'utilisateur des progiciels Dell Update Package*s fournit des informations sur l'obtention et l'utilisation des progiciels DUP dans le cadre de la stratégie de mise à jour de votre système.
- Le *Guide de l'utilisateur Dell Shared PowerEdge RAID Controller (PERC) 8* fournit des informations sur le déploiement de la carte PERC 8 partagée et la gestion du sous-système de stockage. Ce document est disponible en ligne sur **dell.com/storagecontrollermanuals**.
- La documentation relative aux applications de gestion des systèmes Dell fournit des informations sur l'installation et l'utilisation du logiciel de gestion des systèmes.

La documentation système suivante fournit des informations supplémentaires sur le système sur lequel CMC est installé :

- Les Consignes de sécurité fournies avec votre système contiennent des informations importantes sur la sécurité et réglementaires en vigueur. Pour plus d'informations réglementaires, voir la page d'accueil « Conformité aux normes » sur le site Web **www.dell.com/regulatory_compliance**. Les informations de garantie peuvent être incluses dans ce document ou dans un document distinct.
- Le *Guide de démarrage de Dell PowerEdge VRTX* fourni avec le système présente les fonctionnalités, la configuration et les caractéristiques techniques du système.
- Le document d'installation fourni avec le système contient des informations sur l'installation et la configuration initiale du système.
- Le *Manuel du propriétaire* du module serveur contient des informations sur les fonctions du module serveur et explique comment résoudre les problèmes associés au module et installer ou remplacer les composants du module. Ce document est accessible sur le site **dell.com/poweredgemanuals**.
- La documentation fournie avec le rack indique comment installer le système dans un rack, le cas échéant.
- Pour obtenir le nom complet d'une abréviation ou connaître la signification d'un sigle utilisé dans ce tableau, voir le Glossaire sur **dell.com/support/manuals**.
- La documentation relative aux logiciels de gestion de systèmes décrit les fonctionnalités, la configuration requise, l'installation et l'utilisation de base du logiciel.

- La documentation fournie avec les composants achetés séparément indique comment configurer et installer ces options.
- Tous les supports fournis avec le système contiennent de la documentation et des outils permettant de configurer et de gérer le système, notamment les supports du système d'exploitation, du logiciel de gestion des systèmes, des mises à jour système et des composants système que vous avez achetés avec le système. Pour plus d'informations sur le système, analysez le Quick Resource Locator (QRL) disponible sur votre système et sur la fiche de configuration livrée avec votre système. Téléchargez l'application QRL de votre plateforme mobile pour activer l'application sur votre appareil mobile.

Accès aux documents à partir du site de support Dell EMC

Vous pouvez accéder aux documents requis de l'une des façons suivantes :

- À l'aide des liens suivants :
  - Pour les documents sur la gestion des systèmes Enterprise Dell EMC, la gestion à distance des systèmes Enterprise Dell EMC et les solutions de virtualisation Dell EMC : https://www.dell.com/esmmanuals
  - Pour les documents Dell EMC OpenManage : https://www.dell.com/openmanagemanuals
  - Pour les documents sur l'iDRAC : https://www.dell.com/idracmanuals
  - Pour les documents de gestion des systèmes Dell EMC OpenManage Connections Enterprise : https://www.dell.com/OMConnectionsEnterpriseSystemsManagement
  - Pour les documents relatifs aux outils facilitant la maintenance Dell EMC : https://www.dell.com/serviceabilitytools
- Sur le site de support Dell EMC :
  1. Rendez-vous sur https://www.dell.com/support.
  2. Cliquez sur **Parcourir tous les produits**.
  3. Sur la page **Tous les produits**, cliquez sur **Logiciel** et cliquez sur le lien requis parmi les suivants :
     - **Analytiques**
     - **Gestion des systèmes Client**
     - **Applications d'entreprise**
     - **Gestion des systèmes Enterprise**
     - **Mainframe**
     - **Systèmes d'exploitation**
     - **Solutions du secteur public**
     - **Outils de facilité de la gestion**
     - **Compatibilité**
     - **Utilitaires**
     - **Solutions de virtualisation**
  4. Pour afficher un document, cliquez sur le produit requis, puis sur la version requise.
- Avec les moteurs de recherche :
  - Saisissez le nom et la version du document dans la zone de recherche.

2

Installation et configuration de CMC

Cette section fournit des informations indiquant comment installer votre matériel CMC, établir l'accès au contrôleur CMC et configurer l'environnement de gestion en vue d'utiliser le contrôleur CMC. Elle vous guide dans les étapes suivantes de configuration d'un contrôleur CMC :

- Configuration de l'accès initial à CMC
- Accès à CMC via un réseau
- Ajout et configuration d'utilisateurs CMC
- Mise à jour du micrologiciel de CMC.

Pour plus d'informations sur l'installation et la configuration d'un environnement CMC redondant, voir « Fonctionnement de l'environnement CMC redondant ».

Sujets :

Avant de commencer

Avant de configurer l'environnement, téléchargez la dernière version du micrologiciel CMC de PowerEdge VRTX depuis le site **dell.com/support/**.

En outre, assurez-vous que vous disposez du DVD *Dell Systems Management Tools and Documentation*, fourni avec votre système.

Installation du matériel CMC

CMC est préinstallé sur votre châssis, si bien qu'aucune installation n'est requise. Vous pouvez installer un deuxième CMC pour servir de dispositif de secours au CMC actif.

Check-list pour la configuration du châssis

Les tâches suivantes permettent de configurer le châssis avec précision :

1. Le contrôleur CMC et le poste de gestion sur lequel vous utilisez votre navigateur doivent se trouver sur le même réseau, appelé réseau de gestion. Connectez un câble réseau Ethernet entre le port actif CMC et le réseau de gestion.
2. Installez le module d'E/S dans le châssis et connectez le câble réseau au châssis.
3. Insérez les serveurs dans le châssis.

4. Connectez le châssis à la source d'alimentation.
5. Appuyez sur le bouton d'alimentation ou mettez sous tension le châssis depuis l'interface Web CMC après avoir exécuté la tâche de l'étape 7.

   REMARQUE : Ne mettez pas sous tension les serveurs.
6. À l'aide de l'écran LCD, naviguez vers le Résumé IP et cliquez sur le bouton de vérification pour sélectionner. Utilisez l'adresse IP du contrôleur CMC dans le navigateur du système de gestion (IE, Chrome ou Mozilla). Pour configurer DHCP pour le contrôleur CMC, utilisez l'écran LCD et cliquez sur **Menu principal** > **Paramètres** > **Paramètres réseau**.
7. Connectez-vous à l'adresse IP CMC en utilisant un navigateur Web en entrant le nom d'utilisateur par défaut (root) et le mot de passe par défaut (calvin).
8. Attribuez une adresse IP à chaque iDRAC dans l'interface Web CMC, puis activez le LAN et l'interface IPMI.

   REMARQUE : L'interface LAN iDRAC de certains serveurs est désactivée par défaut. Ces informations peuvent être trouvées dans l'interface Web CMC sous Présentation du serveur > Configuration. Il peut s'agir d'une option de licence avancée, dans quel cas vous devez utiliser la fonction Configuration de chaque serveur).
9. Fournissez l'IO module avec une adresse IP dans l'interface Web du CMC. Vous pouvez obtenir l'adresse IP en cliquant sur **Présentation du module d'E/S**, puis sur **Configuration**.
10. Connectez-vous à chaque iDRAC par l'intermédiaire du navigateur Web et fournissez la configuration finale de l'IDRAC. Par défaut, le nom d'utilisateur est `root` et le mot de passe est `calvin`.
11. Connectez le module d'E/S en utilisant le navigateur Web et fournissez la configuration finale du module d'E/S.
12. Mettez sous tension les serveurs et installez le système d'exploitation.

REMARQUE : Le CMC redémarre, si le panneau de configuration est mal installé sur le châssis.

Connexion réseau CMC de base

Pour une redondance maximale, connectez chaque contrôleur CMC disponible à votre réseau de gestion.

Installation du logiciel d'accès à distance sur une station de gestion

Vous pouvez accéder au contrôleur CMC à partir d'une station de gestion à l'aide d'un logiciel d'accès à distance, tel que les utilitaires Telnet, Secure Shell (SSH) ou de console série, de votre système d'exploitation ou via l'interface Web.

Pour utiliser RACADM à distance à partir de votre station de gestion, installez le module RACADM distant à partir du DVD *Dell Systems Management Tools and Documentation* fourni avec votre système. Ce DVD comprend les composants Dell OpenManage suivants :

- Racine du DVD : contient l'utilitaire d'installation et de mise à jour des systèmes Dell.
- SYSMGMT : contient les produits Systems Management Software, dont Dell OpenManage Server Administrator.
- Docs : contient la documentation des systèmes, produits logiciels Systems Management, périphériques et contrôleurs RAID.
- SERVICE : contient les outils dont vous avez besoin pour configurer votre système ainsi que les derniers diagnostics et pilotes optimisés par Dell pour votre système.

Pour plus d'informations sur l'installation des composants logiciels Dell OpenManage, voir le manuel *Dell OpenManage Installation and Security User's Guide* (Guide d'utilisation Installation et sécurité de Dell OpenManage) disponible sur le DVD ou sur le site **dell.com/support/manuals**. Vous pouvez également télécharger la dernière version des outils Dell DRAC depuis le site **dell.com/support**.

Installation de RACADM sur une station de gestion Linux

1. Ouvrez une session en tant que « root » sur le système fonctionnant sous le système d'exploitation Red Hat Enterprise Linux ou SUSE Linux Enterprise Server sur lequel vous souhaitez installer les composants du système géré.
2. Insérez le DVD *Dell Systems Management Tools and Documentation* dans le lecteur de DVD.
3. Pour monter le DVD à l'emplacement requis, utilisez la commande mount ou une commande similaire.

   REMARQUE : Sous le système d'exploitation Red Hat Enterprise Linux 5, les DVD sont montés automatiquement avec l'option de montage `-noexec mount`. Cette option ne permet pas d'exécuter des fichiers exécutables à partir du DVD. Vous devez monter le DVD-ROM manuellement, puis exécuter les commandes.
4. Naviguez vers le répertoire **SYSMGMT/ManagementStation/linux/rac**. Pour installer le logiciel RAC, entrez la commande suivante :

```
rpm -ivh *.rpm
```

5. Pour obtenir des informations sur la commande RACADM, entrez `racadm help` après avoir entré les commandes précédentes. Pour plus d'informations sur RACADM, voir le document *Chassis Management Controller for Dell PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX).

   REMARQUE : Lors de l'utilisation de la fonctionnalité distante RACADM, vous devez disposer d'un droit d'accès en écriture sur les dossiers où vous utilisez les sous-commandes RACADM impliquant des opérations sur des fichiers, par exemple : `racadm getconfig -f <file name>`.

Désinstallation de l'utilitaire RACADM sur une station de gestion Linux

1. Connectez-vous comme utilisateur `root` au système sur lequel vous souhaitez désinstaller les fonctions de station de gestion.
2. Utilisez la commande de requête rpm suivante pour identifier la version installée des outils DRAC :

   ```
   rpm -qa | grep mgmtst-racadm
   ```

3. Vérifiez la version du progiciel à désinstaller et désinstallez la fonction à l'aide de la commande rpm `-e rpm -qa | grep mgmtst-racadm`.

Configuration d'un navigateur Web

Vous pouvez utiliser un navigateur Web pour configurer et gérer le contrôleur CMC, les serveurs et les modules installés dans le châssis. Reportez-vous à la section relative aux navigateurs pris en charge dans la *Matrice de support logiciel des systèmes Dell* sur le site **dell.com/support/manuals**.

Le contrôleur CMC et le poste de gestion sur lequel vous utilisez votre navigateur doivent se trouver sur le même réseau, appelé *réseau de gestion*. En fonction de vos besoins en matière de sécurité, le réseau de gestion peut être un réseau isolé et hautement sécurisé.

REMARQUE : Veillez à ce que les mesures de sécurité du réseau de gestion, comme les pare-feu et les serveurs proxy, n'empêchent pas le navigateur Web d'accéder au contrôleur CMC.

Certaines fonctions du navigateur peuvent interférer avec les connexions ou les performances, en particulier si le réseau de gestion n'a pas d'accès à Internet. Si votre poste de gestion utilise un système d'exploitation Windows, certains paramètres Internet Explorer peuvent interférer avec les connexions, même si vous utilisez une interface de ligne de commande (CLI) pour accéder au réseau de gestion.

REMARQUE : Pour traiter les problèmes de sécurité, Microsoft Internet Explorer surveille de façon stricte l'heure de la gestion des cookies. Pour que cela soit pris en charge, l'heure de votre ordinateur exécutant Internet Explorer doit être synchronisée avec l'heure du CMC.

Serveur proxy

Pour naviguer via un serveur proxy qui n'a pas accès au réseau de gestion, vous pouvez ajouter les adresses du réseau de gestion à la liste d'exceptions du navigateur. Vous indiquez ainsi au navigateur d'ignorer le serveur proxy lors de l'accès au réseau de gestion.

Internet Explorer

Pour modifier la liste des exceptions dans Internet Explorer :

1. Démarrez Internet Explorer.
2. Cliquez sur **Outils** > **Options Internet** > **Connexions**.
3. Dans la section **Paramètres de réseau local**, cliquez sur **Paramètres réseau**.
4. Dans la section **Serveur proxy**, sélectionnez l'option **Utiliser un serveur proxy pour le LAN (Ces paramètres ne s'appliquent pas aux connexions d'accès à distance et VPN)** et cliquez sur **Avancé**.
5. Dans la section **Exceptions**, ajoutez les adresses des CMC et des iDRAC du réseau de gestion, sous forme de liste séparée par le caractère point-virgule. Vous pouvez utiliser des noms DNS et des caractères génériques.

Mozilla FireFox

Pour modifier la liste des exceptions dans Mozilla Firefox 19.0 :

1. Lancez Mozilla Firefox.
2. Cliquez sur **Outils** > **Options** (pour les systèmes Windows) ou sur **Modifier** > **Préférences**(pour les systèmes Linux).
3. Cliquez sur **Avancé**, puis sur l'onglet **Réseau**.
4. Cliquez sur **Paramètres**.
5. Sélectionnez l'option **Configuration manuelle du proxy**.
6. Dans le champ **Pas de proxy pour**, entrez les adresses des CMC et des iDRAC du réseau de gestion sous forme de liste séparée par des virgules. Vous pouvez utiliser des noms DNS et des caractères génériques.

Filtre anti-hameçonnage de Microsoft

Si vous activez le filtre anti-hameçonnage Microsoft dans Internet Explorer sur le système de gestion et que le contrôleur CMC n'a pas d'accès à Internet, l'accès au contrôleur CMC peut être retardé de quelques secondes. Ce retard se produit lorsque vous utilisez le navigateur ou une autre interface telle que RACADM distant. Procédez comme suit pour désactiver le filtre anti-hameçonnage :

1. Démarrez Internet Explorer.
2. Cliquez sur **Outils** > **Filtre anti-hameçonnage**, puis cliquez sur **Paramètres du filtre anti-hameçonnage**.
3. Cochez la case **Désactiver le filtre anti-hameçonnage**, puis cliquez sur **OK**.

Récupération de la liste de révocation des certificats

Si votre CMC n'a pas accès à Internet, désactivez la fonction de récupération de la liste de révocation des certificats (CRL, Certificate Revocation List) dans Internet Explorer. Cette fonction vérifie si un serveur, comme le serveur Web CMC, utilise un certificat figurant sur une liste de certificats révoqués récupérés sur Internet. Si Internet est inaccessible, cette fonctionnalité peut provoquer des retards de plusieurs secondes lorsque vous accédez au CMC à l'aide du navigateur ou d'une interface de ligne de commande telle que l'interface RACADM distante.

Pour désactiver la récupération de la liste de révocation des certificats :

1. Démarrez Internet Explorer.
2. Cliquez sur **Outils** > **Options Internet**, puis cliquez sur **Avancé**.
3. Accédez à la section Sécurité, décochez la case **Vérifier la révocation des certificats de l'éditeur**, puis cliquez sur **OK**.

Téléchargement de fichiers à partir de CMC dans Internet Explorer

Lorsque vous utilisez Internet Explorer pour télécharger des fichiers à partir du contrôleur CMC, vous risquez de rencontrer des problèmes lorsque l'option **Ne pas enregistrer les pages cryptées sur le disque** n'est pas activée.

Procédez comme suit pour activer l'option **Ne pas enregistrer les pages cryptées sur le disque** :

1. Démarrez Internet Explorer.
2. Cliquez sur **Outils** > **Options Internet Avancé**.
3. Dans la section **Sécurité**, sélectionnez **Ne pas enregistrer les pages cryptées sur le disque**.

Activation des animations dans Internet Explorer

Lors du transfert de fichiers vers et depuis l'interface Web, une icône de transfert de fichier tourne pour indiquer l'activité de transfert. Lorsque vous utilisez Internet Explorer, vous devez configurer le navigateur pour qu'il lise les animations.

Pour configurer Internet Explorer pour la lecture d'animations :

1. Démarrez Internet Explorer.
2. Cliquez sur **Outils** > **Options Internet Avancé**.
3. Accédez à la section **Multimédia** et sélectionnez l'option **Lire les animations dans les pages Web**.

Configuration de l'accès initial à CMC

Pour gérer à distance le contrôleur CMC, connectez-le au réseau de gestion, puis configurez les paramètres réseau CMC.

REMARQUE : Pour pouvoir gérer la solution PowerEdge, vous devez la connecter au réseau de gestion.

Pour en savoir plus sur la définition des paramètres réseau CMC, voir Configuration de réseau initiale pour CMC. Cette configuration initiale définit les paramètres réseau TCP/IP qui permettent l'accès au contrôleur CMC.

Le contrôleur CMC et l'interface iDRAC de chaque serveur, ainsi que les ports de gestion de réseau des module d'E/S du commutateur sont connectés à un réseau intégré commun dans le châssis PowerEdge VRTX. Cela permet d'isoler le réseau de gestion du réseau de données serveur. Il est important de séparer ce trafic pour garantir l'accès ininterrompu à la gestion du châssis.

Le contrôleur CMC est connecté au réseau de gestion. Tout accès externe au contrôleur CMC et aux interfaces iDRAC s'effectue via le contrôleur CMC. En revanche, l'accès aux serveurs gérés passe par des connexions réseau au module d'E/S (IOM). Cela permet d'isoler le réseau d'applications du réseau de gestion.

Il est recommandé d'isoler la gestion du châssis et le réseau de données. En raison du trafic potentiel sur le réseau de données, les interfaces de gestion du réseau de gestion interne peuvent être saturées par le trafic destiné aux serveurs. Cela provoque des retards dans les communications CMC et iDRAC. Ces retards provoquent un comportement imprévisible du châssis : le contrôleur CMC peut, par exemple, indiquer que l'interface iDRAC est hors ligne alors qu'elle est en ligne et fonctionne. Ce problème peut, à son tour, générer un comportement indésirable. S'il n'est pas possible d'isoler physiquement le réseau de gestion, l'autre solution consiste à séparer le trafic CMC et iDRAC sur un VLAN distinct. Le contrôleur CMC et les différentes interfaces réseau iDRAC peuvent être configurés pour utiliser un VLAN.

Configuration du réseau CMC initial

REMARQUE : Si vous modifiez les paramètres réseau de votre CMC, la connexion réseau en cours risque d'être coupée.

Vous pouvez réaliser la configuration réseau initiale de CMC avant ou pendant l'attribution d'une adresse IP au CMC. Si vous configurez les paramètres réseau initiaux de CMC avant d'avoir une adresse IP, vous pouvez utiliser l'une des interfaces suivantes :

- L'écran LCD du panneau avant du châssis
- La console série CMC Dell

Si vous configurez les paramètres réseau initiaux de CMC après avoir obtenu une adresse IP, vous pouvez utiliser l'une des interfaces suivantes :

- Interfaces de ligne de commande (CLI), telles que la console série, Telnet, SSH ou CMC Dell
- Interface RACADM distante
- Interface Web CMC
- Interface de l'écran LCD

Le contrôleur CMC prend en charge les modes d'adressage IPv4 et IPv6. Les paramètres de configuration d'IPv4 sont indépendants des paramètres IPv6.

Configuration du réseau CMC à l'aide de l'interface de panneau LCD

Vous pouvez utiliser l'interface de l'écran LCD pour configurer le réseau CMC.

REMARQUE : Vous pouvez personnaliser l'orientation d'un écran LCD (mode rack ou tour) en gardant les flèches directionnelles haut et bas enfoncées pendant deux secondes. Sinon, vous pouvez également utiliser celles droite et gauche. Pour plus d'informations sur les boutons disponibles sur un panneau LCD du CMC, consultez Navigation LCD.

1. Pour démarrer la configuration CMC :
   - Dans le cas d'un châssis n'ayant pas été configuré précédemment, le panneau **Langue de l'écran LCD** s'affiche. Dans le panneau **Langue de l'écran LCD**, accédez à la langue voulue à l'aide des flèches directionnelles. Lorsque la langue souhaitée est mise en surbrillance, sélectionnez la langue en appuyant sur le bouton central. Le panneau **Paramètres de réseau** s'affiche.
   - Dans le cas d'un châssis n'ayant pas été configuré précédemment, le panneau **Menu principal** s'affiche. Dans le **Menu principal**, sélectionnez **Paramètres**, puis **Paramètres de réseau**.
2. Dans le panneau **Paramètres de réseau**, sélectionnez le mode de configuration requis :
   - **Configuration rapide (DHCP)** : sélectionnez ce mode pour configurer rapidement le CMC à l'aide d'adresses DHCP. Pour plus d'informations sur la configuration du contrôleur CMC à l'aide de ce mode, consultez **Configurer le CMC à l'aide de la configuration rapide (DHCP)**.

- **Configuration avancée** : sélectionnez ce mode pour paramétrer le contrôleur CMC pour des configurations avancées. Pour plus d'informations sur la configuration du contrôleur CMC à l'aide de ce mode, consultez **Configurer le CMC à l'aide de la configuration avancée**.

Configuration du contrôleur CMC à l'aide de la configuration rapide (DHCP)

Pour configurer le réseau à l'aide de l'interface de panneau LCD :

1. Dans le panneau **Paramètres de réseau**, sélectionnez **Configuration rapide (DHCP)**. Le panneau affiche le message suivant.

   ```
   About to get DHCP addresses. Ensure CMC network cable is connected.
   ```

2. Appuyez sur le bouton central pour mettre en surbrillance le bouton Accepter. Appuyez de nouveau sur le bouton central pour accepter les paramètres ou naviguez vers la flèche retour et appuyez sur le bouton central pour revenir en arrière et modifier les paramètres.

Configuration du contrôleur CMC à l'aide de la configuration avancée

1. Dans le volet **Paramètres réseau** , si vous sélectionnez l'option **Configuration avancée**, le message suivant s'affiche pour confirmer si voulez configurer CMC :

   ```
   Configure CMC?
   ```

2. Pour configurer le CMC à l'aide des propriétés de configuration avancée, cliquez sur le bouton central en sélectionnant l'icône de coche.

   REMARQUE : Pour ignorer la configuration CMC, naviguez vers l'icône « X », puis appuyez sur le bouton central.

3. Si un message vous demande de sélectionner une vitesse de réseau appropriée, sélectionnez une vitesse de réseau (**Auto (1 Gb)**, **10 Mb** ou **100 Mb**) en utilisant les boutons appropriés.

   Pour un débit réseau efficace, le paramètre de vitesse réseau doit correspondre à votre configuration réseau. La définition d'une vitesse réseau inférieure à celle de votre configuration réseau augmente la consommation de bande passante et ralentit les communications sur le réseau. Vous devez déterminer si votre réseau prend en charge les vitesses réseau ci-dessus et le configurer en conséquence. Si votre configuration réseau ne correspond à aucune de ces valeurs, il est recommandé de sélectionner l'option **Auto (1 Go)** ou de consulter la documentation utilisateur du fabricant de votre équipement réseau.

4. Effectuez l'une des opérations suivantes :

   - Sélectionnez **Auto (1 Go)**, en appuyant sur le bouton central, puis en appuyant à nouveau sur ce dernier. Le panneau **Protocole** s'affiche. Passez à l'étape 6.
   - Sélectionnez **10 Mo** ou **100 Mo**. Le panneau **Duplex**

     s'affiche. Passez à l'étape 5.

   Sinon, si vous

5. Dans le panneau **Duplex**, pour sélectionner le mode Duplex (**Duplex intégral** ou **Semi-duplex**) qui correspond à l'environnement réseau, appuyez une première fois sur le bouton central, puis une seconde fois. Le panneau **Protocole** s'affiche.

   REMARQUE : Les paramètres de la vitesse réseau et du mode duplex ne sont pas disponibles lorsque l'option Négociation automatique est définie sur Activée ou qu'une vitesse de 1 000 Mo (1 Gbit/s) est sélectionnée. Si la négociation automatique est activée pour un appareil mais pas pour l'autre, l'appareil qui utilise la négociation automatique peut déterminer la vitesse réseau de l'autre périphérique, mais pas son mode duplex. Dans ce cas, le mode duplex Semi duplex est sélectionné lors de la négociation automatique. Une telle incohérence du mode duplex ralentit la connexion réseau.

6. Dans le panneau **Protocole**, sélectionnez le protocole Internet (**IPv4 uniquement**, **IPv6 uniquement** ou **Les deux**) à utiliser pour le contrôleur CMC, puis appuyez une première sur le bouton central, puis une deuxième fois.
7. - Si vous sélectionnez **IPv4** ou **Les deux**, sélectionnez le mode **DHCP** ou **Statique**. Passez à l'étape 8.
   - Sinon, si vous sélectionnez **IPv6**, le panneau **Configurer l'iDRAC** s'affiche. Passez à l'étape 11 intervenant ultérieurement dans cette procédure.
8. Dans le panneau **Mode**, sélectionnez le mode dans lequel CMC doit obtenir les adresses IP des cartes réseau (NIC). Si vous sélectionnez DHCP, le CMC récupère automatiquement la configuration IP (adresse IP, masque et passerelle) auprès d'un serveur DHCP sur votre réseau. Une adresse IP unique allouée à votre réseau est attribuée au CMC. Si vous sélectionnez **DHCP**, appuyez une première fois sur le bouton central, puis une seconde fois. Le panneau **Configurer l'iDRAC** s'affiche. Passez à l'étape 11 intervenant ultérieurement dans cette procédure.
9. Si vous sélectionnez **Statique**, entrez l'adresse IP, la passerelle et le masque de sous-réseau en suivant les instructions de l'écran LCD.

   Les informations IP que vous avez saisies s'affichent. Appuyez une première fois sur le bouton central, puis une seconde fois. L'écran **Configuration du CMC** répertorie les paramètres d'**Adresse IP statique**, de **Masque de sous-réseau** et de **Passerelle** que vous

avez saisis. Vérifiez l'exactitude des paramètres. Pour corriger un paramètre, appuyez sur les boutons appropriés. Appuyez une première fois sur le bouton central, puis une seconde fois. Le panneau **Enregistrer DNS ?** s'affiche.

10. Pour l'enregistrer, sélectionnez l'icône de coche, puis appuyez sur le bouton central. Définissez l'adresse IP DNS, sélectionnez l'icône de coche, puis appuyez sur le bouton central. Si l'enregistrement DNS n'est pas obligatoire, sélectionnez l'icône « X » et appuyez sur le bouton central.
11. Indiquez si vous souhaitez configurer un iDRAC :
    - **Non** : sélectionnez l'icône « X », puis appuyez sur le bouton central. Passez à l'étape 17 intervenant ultérieurement dans cette procédure.
    - **Oui** : sélectionnez l'icône de coche, puis appuyez sur le bouton central.

    Vous pouvez également configurer l'iDRAC depuis l'interface Web CMC.
12. Dans le panneau **Protocole** , sélectionnez le type de l'adresse IP que vous souhaitez utiliser pour les serveurs :
    - **IPv4** : les options **DHCP** ou **Statique** s'affichent.
    - **Les deux**

      - Les options **DHCP** ou **Statique** sont affichées.
    - **IPv6**

      - Le panneau **Configuration iDRAC** s'affiche. Passez à l'étape 15.
13. Sélectionnez **DHCP** ou **Statique**.

Tableau 9. Mode Réseau

Mode Réseau	Description
DHCP (Dynamic Host Configuration Protocol - Protocole de configuration dynamique des hôtes)	L'iDRAC récupère automatiquement la configuration IP (adresse IP, masque de sous-réseau et passerelle) auprès d'un serveur DHCP sur votre réseau. Une adresse IP unique allouée sur votre réseau est attribuée à l'iDRAC. Appuyez sur le bouton central. Le panneau **IPMI sur le LAN** s'affiche.

Statique	Si vous sélectionnez **Statique**, entrez manuellement l'adresse IP, la passerelle et le masque de sous-réseau en suivant les instructions de l'écran LCD.
	Si vous avez sélectionné l'option **Statique**, appuyez sur le bouton central, puis procédez comme suit :
	a. le message suivant demande si vous voulez incrémenter automatiquement en utilisant l'adresse IP du logement 1.
	`IPs will auto-increment by slot number.`
	Cliquez sur le bouton central. Le message suivant demande de saisir le numéro IP du logement 1.
	`Enter slot 1 (starting) IP`
	Entrez le numéro de l'adresse IP du logement 1 et appuyez sur le bouton central.
	b. Définissez le masque de sous-réseau, puis appuyez sur le bouton central.
	c. Définissez la passerelle, puis appuyez sur le bouton central.
	d. L'écran **Récapitulatif du réseau** répertorie les paramètres d'**Adresse IP statique**, de **Masque de sous-réseau** et de **Passerelle** que vous avez saisis. Vérifiez l'exactitude des paramètres. Pour corriger un paramètre, appuyez sur les boutons appropriés, puis sur le bouton central.
	e. Une fois les paramètres vérifiés, passez à l'étape 10.
	Le panneau **IPMI sur le LAN** s'affiche.

14. Dans le panneau **IPMI sur LAN**, sélectionnez **Activer** ou **Désactiver** pour activer ou désactiver l'interface IPMI sur le LAN. Appuyez sur le bouton central pour continuer.
15. Dans le panneau **Configuration iDRAC**, le message suivant s'affiche.

```
Apply settings to installed servers?
```

Pour appliquer tous les paramètres réseau iDRAC aux serveurs installés, sélectionnez l'icône de coche, puis appuyez sur le bouton central. Sinon, sélectionnez l'icône « X », puis appuyez sur le bouton central.

16. Dans le panneau **Configuration d'iDRAC** suivant, le message suivant s'affiche.

```
Auto-Apply settings to newly-inserted servers?
```

Pour appliquer tous les paramètres réseau iDRAC aux serveurs récemment installés, sélectionnez l'icône de coche, puis appuyez sur le bouton central. Lorsqu'un nouveau serveur est inséré dans le châssis, le LCD vous demande si vous souhaitez ou non déployer automatiquement le serveur à l'aide des règles de paramètres réseau précédemment configurées. Si vous ne souhaitez pas appliquer les paramètres réseau iDRAC aux serveurs récemment installés, sélectionnez l'icône « X » et appuyez sur le bouton central. Lorsqu'un nouveau serveur est inséré dans le châssis, les paramètres réseau iDRAC ne sont pas configurés.

17. Dans le panneau **Configuration iDRAC**, le message suivant s'affiche.

```
Apply All Enclosure Settings?
```

Pour appliquer tous les paramètres de boîtier, sélectionnez l'icône de coche et appuyez sur le bouton central. Sinon, sélectionnez l'icône « X », puis appuyez sur le bouton central.

18. Dans le panneau **Récapitulatif IP**, après le panneau d'attente de 30 secondes, passez en revue les adresses IP que vous avez fournies pour vous assurer de leur exactitude. Pour corriger un paramètre, appuyez sur la flèche directionnelle gauche, puis appuyez sur le bouton central pour revenir à l'écran de ce paramètre. Une fois une adresse IP corrigée, appuyez sur le bouton central.

Après avoir vérifié que les paramètres que vous avez saisis sont corrects, appuyez une première fois sur le bouton central, puis une seconde fois. Le panneau **Menu principal** s'affiche.

Le CMC et les iDRAC sont désormais disponibles sur le réseau. Vous pouvez accéder au CMC à l'adresse IP attribuée à l'aide de l'interface Web, ou avec une interface de ligne de commande (CLI) comme une console série, Telnet ou SSH.

Interfaces et protocoles d'accès à CMC

Après avoir configuré les paramètres réseau CMC, vous pouvez accéder au contrôleur CMC à distance à l'aide de différentes interfaces. Le tableau suivant répertorie les interfaces que vous pouvez utiliser pour accéder à distance au contrôleur CMC.

REMARQUE : Comme Telnet n'est pas aussi sécurisé que les autres interfaces, il est désactivé par défaut. Activez Telnet en utilisant l'interface Web, SSH ou l'interface RACADM distante.

REMARQUE : L'utilisation simultanée de plusieurs interfaces de configuration peut générer des résultats inattendus.

Tableau 10. Interfaces CMC

Interface	Description
Interface web	Fournit un accès distant à CMC à l'aide d'une interface utilisateur graphique. L'interface Web est intégrée au micrologiciel CMC et accessible via l'interface de carte réseau (NIC) depuis un navigateur Web pris en charge sur la station de gestion. Pour obtenir la liste des navigateurs Web pris en charge, consultez la section Navigateurs pris en charge de la *Matrice de prise en charge des logiciels des systèmes Dell* sur le site Web **dell.com/support/manuals**.
Interface de ligne de commande RACADM à distance	Employez cet utilitaire de ligne de commande pour gérer CMC et ses composants. Vous pouvez utiliser l'interface RACADM du micrologiciel ou l'interface distante : · L'interface distante RACADM est un utilitaire client exécuté sur une station de gestion. Elle utilise l'interface réseau hors bande pour exécuter des commandes RACADM sur le système géré et le canal HTTPs. L'option `-r` exécute la commande RACADM sur un réseau. · Le RACADM du micrologiciel est accessible en se connectant à l'iDRAC à l'aide de SSH ou Telnet. Vous pouvez exécuter les commandes RACADM du micrologiciel sans spécifier le CMC, l'adresse IP, le nom d'utilisateur ou le mot de passe. Une fois dans l'invite RACADM, vous pouvez directement exécuter les commandes sans le préfixe racadm.
Écran LCD du châssis	Utilisez l'écran LCD du panneau avant pour réaliser les opérations suivantes : · Afficher les alertes et IP CMC. · Définir DHCP. · Configuration des paramètres d'adresse IP statique CMC · Afficher l'adresse MAC de CMC pour le contrôleur CMC actif.

Tableau 10. Interfaces CMC (suite)

Interface	Description
	• Afficher l'ID de VLAN de CMC ajoutée à la fin de l'IP CMC, si le VLAN est déjà configuré.
Telnet	Fournit un accès par ligne de commande à CMC via le réseau. L'interface de ligne de commande (CLI) RACADM et la commande `connect`, qui sert à se connecter à la console série d'un serveur ou module d'E/S, sont disponibles depuis la ligne de commande CMC. **REMARQUE : Telnet n'est pas un protocole sécurisé et il est désactivé par défaut. Telnet transmet toutes les données, y compris les mots de passe en texte clair. Pour transmettre des données sensibles utilisez l'interface SSH**
SSH	Utilisez SSH pour exécuter les commandes RACADM. Vous obtenez les mêmes fonctionnalités qu'avec la console Telnet, mais avec une couche de transport cryptée qui renforce la sécurité. Le service SSH est activé par défaut dans CMC et peut être désactivé.
WSMan	Les services WSMAN reposent sur le protocole de gestion WSMAN (Web Services for Management) pour exécuter des tâches de gestion des systèmes un à plusieurs. Vous devez utiliser un client WS-MAN, tel que WinRM (Windows) ou le client OpenWSMAN (Linux) pour pouvoir utiliser la fonctionnalité CMC Services functionality. Vous pouvez également utiliser Power Shell et Python pour exécuter des scripts vers l'interface WSMan. WSMAN est un protocole SOAP (Simple Object Access Protocol) utilisé pour la gestion des systèmes. CMC utilise WS–Management pour la transmission des informations de gestion DMTF (Distributed Management Task Force) basées sur CIM (Common Information Model). Les informations CIM définissent la sémantique et les types d'informations qui peuvent être modifiés dans un système géré. L'implémentation CMC WSMan utilise SSL sur le port 443 pour la sécurité du transport, et prend en charge l'authentification de base. Les données disponibles via WS-Management sont fournies par l'interface d'instrumentation CMC adressée sur les profils DMTF et les profils d'extension. Pour de plus amples informations, consultez : • fichiers MOF et profils : **delltechcenter.com/page/DCIM.Library** • site Web DTMF : **dmtf.org/standards/profiles/** • Fichier des notes de mise à jour WSMan. • **www.wbemsolutions.com/ws_management.html** • Spécifications DMTF WSManagement : **www.dmtf.org/standards/wbem/wsman** Vous pouvez utiliser les interfaces de services Web en exploitant l'infrastructure client existante, comme Windows WinRM et l'interface de ligne de commande (CLI) Powershell, les utilitaires source libre comme WSManCLI et les environnements de programmation d'applications comme Microsoft .NET. L'outil WinRM définit un délai d'expiration de réponse par défaut de 60 secondes pour toutes les commandes WSMan qu'il envoie. WinRM n'autorise pas de variation d'intervalle d'expiration du délai. Utiliser la commande « “winrm set winrm/config @{MaxTimeoutms ="80000"} » ne modifie pas le délai d'expiration en raison d'un bug dans l'outil WinRM. Par conséquent, il est recommandé que WinRM ne soit pas utilisé pour les commandes qui peut durer plus d'une minute pour terminer l'exécution. L'utilisation de bibliothèques qui créent des paquets SOAP-XML est recommandée, car les utilisateurs peuvent configurer la durée du délai d'expiration grâce à elles. Pour la connexion client avec Microsoft WinRM, la version minimale requise est la version 2.0. Pour plus d'informations, voir l'article Microsoft <**support.microsoft.com/kb/968929**>.

REMARQUE : Le nom d'utilisateur et le mot de passe par défaut CMC sont respectivement `root` et `calvin`.

Lancement de CMC à l'aide d'autres outils de gestion des systèmes

Vous pouvez également lancer le contrôleur CMC depuis Dell Server Administrator ou Dell OpenManage Essentials.

Pour accéder à l'interface CMC avec Dell Server Administrator, lancez Server Administrator sur la station de gestion. Dans le volet de gauche de la page d'accueil Server Administrator, cliquez sur **Système** > **Châssis principal du système** > **Contrôleur d'accès distant**. Pour plus d'informations, voir le *Dell Server Administrator User's Guide* (Guide d'utilisation de Dell Server Administrator) sur le site **dell.com/support/manuals**.

Téléchargement et mise à jour du micrologiciel CMC

Pour télécharger le micrologiciel CMC, voir « Téléchargement du micrologiciel CMC ».

Pour mettre à jour le micrologiciel CMC, voir « Mise à jour du micrologiciel CMC ».

Définition de l'emplacement physique et du nom du châssis

Vous pouvez définir l'emplacement du châssis dans un centre de données, ainsi que le nom du châssis pour l'identifier sur le réseau (le nom par défaut est **Dell Rack System**). Par exemple, une requête SNMP sur le nom de châssis retourne le nom que vous avez défini.

Définition de l'emplacement physique et du nom du châssis avec l'interface Web

Pour définir l'emplacement et le nom du châssis avec l'interface Web CMC :

1. Dans le volet de gauche, accédez à **Présentation du châssis**, puis cliquez sur **Configurer**.
2. Sur la page **Paramètres généraux du châssis**, saisissez les propriétés d'emplacement et le nom du châssis. Pour plus d'informations sur la configuration des propriétés du châssis, consultez l'*Aide en ligne du CMC*.

   Vous pouvez afficher le nom du châssis en vous connectant au CMC à l'aide de SSH, en sélectionnant **Afficher le nom du châssis dans l'invite SSH**. Par défaut, l'option **Afficher le nom du châssis dans l'invite SSH** est désélectionnée.

   REMARQUE : Le champ Emplacement du châssis est facultatif. Utilisez les champs Datacenter, Allée, Rack et Logement de rack pour spécifier l'emplacement physique du châssis.
3. Cliquez sur **Appliquer**. Les paramètres sont enregistrés.

Définition de l'emplacement physique et du nom du châssis avec RACADM

Pour définir le nom, l'emplacement, la date et l'heure du châssis en utilisant l'interface de ligne de commande, voir les commandes **setsysinfo** et **setchassisname**. Pour plus d'informations, voir le document *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX).

Définition de la date et de l'heure sur le CMC

Vous pouvez définir manuellement la date et l'heure ou synchroniser la date et l'heure avec un serveur NTP (Network Time Protocol).

Définition de la date et de l'heure du CMC à l'aide de l'interface Web CMC

Pour définir la date et l'heure sur le contrôleur CMC :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Configurer** > **Date/Heure**.
2. Pour synchroniser la date et l'heure avec le serveur NTP (Network Time Protocol), sur la page **Date/Heure**, sélectionnez **Activer NTP** et définissez jusqu'à trois serveurs NTP. Pour définir manuellement la date et l'heure, désélectionnez l'option **Activer NTP** et modifiez les champs **Date** et **Heure**.
3. Sélectionnez le **fuseau horaire** dans le menu déroulant et cliquez sur **Appliquer**.

Définition de la date et de l'heure du CMC avec RACADM

Pour définir la date et l'heure en utilisant l'interface de ligne de commande, voir la commande **config** et les sections sur les groupes de propriétés de base de données `cfgRemoteHosts` dans le document *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX) sur le site **dell.com/support/manuals**.

Configuration des LED pour l'identification des composants du châssis

Vous pouvez activer les voyants des composants (châssis, serveurs, disques physiques, disques virtuels et module d'E/S) pour qu'ils clignotent et vous permettent d'identifier les composants sur le châssis.

REMARQUE : Vous devez disposer du privilège Administrateur de configuration du châssis pour pouvoir modifier ces paramètres.

Configuration du clignotement des LED avec l'interface Web CMC

Pour activer le clignotement d'un, de plusieurs ou de tous les voyants des composants :

- Dans le volet de gauche, accédez aux pages suivantes :
  - **Présentation du châssis** > **Dépannage**.
  - **Présentation du châssis** > **Contrôleur de châssis** > **Dépannage**.
  - **Présentation du châssis** > **Présentation du serveur** > **Dépannage**.

    REMARQUE : Sur cette page, vous pouvez uniquement sélectionner des serveurs.
  - **Présentation du châssis** > **Présentation du module d'E/S** > **Dépannage**.
  - **Stockage** > **Dépannage** > **Identifier**.

    REMARQUE : Les options Disque physique par enceintes, Disques virtuels par enceinte et le voyant de composant de stockage externe peuvent être sélectionnés sur cette page.

Pour activer le clignotement du voyant d'un composant, sélectionnez l'option **Sélectionner/Désélectionner tout** correspondant au lecteur de disque physique ou au disque virtuel ou encore aux enceintes, puis cliquez sur **Activer le clignotement**. Pour désactiver le clignotement du voyant d'un composant, désélectionnez l'option **Sélectionner/Désélectionner tout** correspondant au voyant, puis cliquez sur **Désactiver le clignotement**.

Configuration du clignotement des LED avec RACADM

Ouvrez une console texte série/Telnet/SSH d'accès à CMC, ouvrez une session et entrez :

`racadm setled -m <module> [-l <ledState>]`, où *<module>* spécifie le module dont vous voulez configurer le voyant. Options de configuration :

- `server-n`, où *n* = 1-4
- `switch-1`

- `cmc-active`

et *<letdState>* indique si le voyant doit clignoter. Options de configuration :

- 0 : aucun clignotement (par défaut)
- 1 : clignotement

`racadm raid <opération> <nom complet du composant>`, où la valeur *opération* est `blink` ou `unblink` et où le nom complet est celui du lecteur de disque physique du composant, du disque virtuel et des enceintes.

Configuration des propriétés de CMC

Vous pouvez définir les propriétés du contrôleur CMC, telles que le bilan de puissance, les paramètres réseau, les utilisateurs et les alertes SNMP et par e-mail à l'aide de l'interface Web ou des commandes RACADM.

Configuration de la méthode de lancement d'iDRAC à l'aide de l'interface Web CMC

Pour configurer la méthode de lancement de l'iDRAC depuis la page **Paramètres généraux du châssis** :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Configuration**.
   La page **Paramètres généraux du châssis** s'affiche.
2. Dans le menu déroulant de la propriété **Méthode de lancement d'iDRAC**, sélectionnez **Adresse IP** ou **DNS**.
3. Cliquez sur **Appliquer**.

   REMARQUE : Un lancement basé sur DNS est utilisé pour un iDRAC spécifique uniquement si :

   - **Le paramètre du châssis est DNS.**
   - **CMC a détecté que l'iDRAC spécifié est configuré avec un nom DNS.**

Configuration de la méthode de lancement d'iDRAC à l'aide de RACADM

Pour mettre à jour le micrologiciel CMC à l'aide de RACADM, utilisez la sous-commande `cfgRacTuneIdracDNSLaunchEnable`. Pour plus d'informations, voir le *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX), disponible à l'adresse **dell.com/support/manuals**.

Configuration des attributs de stratégie de verrouillage de la connexion à l'aide de l'interface Web CMC

REMARQUE : Pour effectuer les étapes suivantes, vous devez disposer du privilège d' Administrateur de configuration du châssis.

L'option **Sécurité de connexion** vous permet de configurer les attributs de la plage d'IP pour vous connecter à CMC à l'aide de l'interface Web CMC. Pour configurer les attributs de la plage IP à l'aide de l'interface Web CMC :

1. Dans le volet gauche, accédez à **Présentation du châssis**, puis cliquez sur **Réseau** > **Réseau**.
   La page **Configuration réseau** s'affiche.
2. Dans la section Paramètres IPv4, cliquez sur **Paramètres avancés**. Alternativement, pour accéder à la page **Sécurité de connexion**, dans le volet gauche, accédez à **Présentation du châssis**, cliquez sur **Sécurité** > **Connexion**.
   La page **Sécurité de connexion** s'affiche.
3. Pour activer la fonction de blocage d'utilisateur et d'adresse IP, dans la section **Stratégie de verrouillage de la connexion**, sélectionnez l'option **Verrouillage par nom d'utilisateur** ou **Verrouillage par adresse IP (IPV4)** .

Les options de définition des attributs de la stratégie de verrouillage de la connexion sont activées.

4. Entrez les valeurs requises pour les attributs de stratégie de verrouillage de la connexion dans les champs activés **Nombre d'échecs de verrouillage**, **Fenêtre d'échec de verrouillage** et **Période de pénalité de verrouillage**. Pour plus d'informations, voir l'*Aide en ligne CMC*.
5. Pour enregistrer ces paramètres, cliquez sur **Appliquer**.

Configuration des attributs de stratégie de verrouillage de la connexion à l'aide de RACADM

Vous pouvez utiliser RACADM pour configurer les attributs de stratégie de verrouillage de la connexion pour les fonctions suivantes :

- Blocage d'un utilisateur
- Blocage d'une adresse IP
- Nombre de tentatives de connexion autorisées
- Délai de nombre d'échecs de connexion avant verrouillage
- Temps de pénalité de verrouillage
- Pour activer la fonction de blocage d'un utilisateur, utilisez :

```
racadm config -g cfgRacTuning -o cfgRacTuneUserBlkEnable <0|1>
```

- Pour activer la fonction de blocage d'une adresse IP, utilisez :

```
racadm config -g cfgRacTuning -o cfgRacTuneIPBlkEnable <0|1>
```

- Pour spécifier le nombre de tentatives de connexion, utilisez la commande suivante :

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailCount
```

- Pour spécifier la période pendant laquelle les échecs de connexion avant verrouillage doivent se produire, utilisez la commande suivante :

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkFailWindow
```

- Pour spécifier la valeur de la période de pénalité de verrouillage, utilisez la commande suivante :

```
racadm config -g cfgRacTuning -o cfgRacTuneIpBlkPenaltyTime
```

Pour plus d'informations sur ces objets, voir le *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX) disponible sur le site **dell.com/support/manuals**.

Fonctionnement de l'environnement CMC redondant

Vous pouvez installer un contrôleur CMC de secours qui prendra le relais si le contrôleur CMC actif ne fonctionne plus. Le CMC redondant peut être préinstallé ou être installé ultérieurement. Pour garantir une redondance totale ou des performances optimales, il est important que le réseau CMC soit correctement câblé.

Le basculement peut survenir dans les cas suivants :

- Vous exécutez la commande RACADM `cmcchangeover`. Voir la section de la commande `cmcchangeover` dans le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX* accessible sur le site dell.com/support/manuals.
- Vous exécutez la commande RACADM `racreset` sur le contrôleur CMC actif. Voir la section de la commande `racreset` dans le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX* accessible sur le site dell.com/support/manuals.
- Réinitialisez le contrôleur CMC actif à partir de l'interface Web. Reportez-vous à l'option `Reset CMC` pour connaître les **Opérations de contrôle de l'alimentation** décrites dans la section Exécution des opérations de contrôle de l'alimentation.
- Retrait du câble réseau du CMC actif.
- Retrait du CMC actif du châssis.

- Lancement d'un vidage Flash du firmware CMC sur le CMC actif.
- Utilisation d'un CMC actif qui n'est plus fonctionnel.

REMARQUE : En cas de basculement du CMC, toutes les connexions iDRAC et toutes les sessions CMC actives seront déconnectées. Les utilisateurs dont les sessions sont déconnectées doivent alors se reconnecter au nouveau contrôleur CMC actif.

À propos du contrôleur CMC de secours

Le contrôleur CMC de secours est identique au contrôleur CMC actif et géré comme miroir de ce dernier. La même version de micrologiciel doit être installée sur les deux contrôleurs CMC, actif et de secours. Si les micrologiciels diffèrent, le système signale une dégradation de la redondance.

Le contrôleur CMC de secours utilise les mêmes paramètres et propriétés que le contrôleur CMC actif. Vous devez utiliser la même version du micrologiciel sur les deux contrôleurs CMC, mais il n'est pas nécessaire de dupliquer les paramètres de configuration sur le contrôleur CMC de secours.

REMARQUE : Pour plus d'informations sur l'installation d'un contrôleur CMC, voir le *Manuel du propriétaire RTX*. Pour les instructions sur l'installation du micrologiciel sur le contrôleur CMC de secours voir Mise à niveau du micrologiciel.

Mode anti-défaillance du contrôleur CMC

Le boîtier PowerEdge VRTX active le mode de sécurité en vue de protéger les serveurs et le module d'E/S contre les pannes. Le mode de sécurité est activé lorsqu'une console CMC ne contrôle pas le châssis. Au cours du basculement CMC ou lors de la perte de gestion d'une seule console CMC :

- Vous ne pouvez pas mettre sous tension les nouveaux serveurs installés.
- Vous ne pouvez pas accéder à distance aux serveurs existants.
- Jusqu'à la restauration de la gestion du contrôleur CMC, les performances des serveurs sont réduites afin de limiter la consommation d'énergie.

La liste suivante répertorie quelques conditions qui peuvent résulter de la perte de gestion d'un module CMC :

- Retrait de module CMC : la gestion du châssis reprend après le remplacement du module CMC ou après la reprise (basculement) sur le module CMC de secours.
- Retrait du câble réseau du module CMC ou perte de connexion réseau : la gestion du châssis reprend après la défaillance du châssis et la reprise sur le module CMC de secours. La reprise réseau n'est activée qu'en mode de CMC redondant.
- Réinitialisation du CMC : la gestion du châssis est rétablie après le redémarrage du CMC ou après le basculement du châssis vers le CMC de secours.
- Émission de la commande de reprise du module CMC : la gestion du châssis reprend lorsque le châssis est défaillant et que le module CMC de secours prend la relève.
- Mise à jour du micrologiciel CMC : la gestion du châssis reprend après le redémarrage du CMC ou le châssis bascule vers le CMC de secours. Il est recommandé de mettre à jour le CMC de secours en premier, afin de ne créer qu'un seul événement de basculement.
- Détection et correction d'erreurs du CMC : la gestion du châssis reprend après la réinitialisation du CMC ou le basculement du châssis vers le CMC de secours.

REMARQUE : Vous pouvez configurer le boîtier à l'aide d'un seul contrôleur CMC ou des contrôleurs CMC redondants. Dans les configurations de contrôleurs CMC redondants, si le contrôleur CMC principal perd la communication avec le boîtier ou le réseau de gestion, le contrôleur CMC de secours se charge de la gestion des châssis.

Processus de sélection du CMC actif

Il n'existe aucune différence entre les deux logements CMC : le logement ne détermine pas l'ordre de priorité. C'est plutôt le CMC installé ou démarré en premier qui devient le CMC actif. Si vous activez l'alimentation CA après avoir installé deux CMC, le contrôleur CMC installé dans le logement CMC 1 (à gauche) assume normalement le rôle de CMC actif. Le voyant bleu indique le CMC actif.

Si vous insérez deux CMC dans un châssis sous tension, la négociation automatique entre le contrôleur actif et le contrôleur de secours peut prendre jusqu'à deux minutes. Le châssis revient à son fonctionnement normal lorsque la négociation est terminée.

Obtention de la condition d'intégrité du contrôleur CMC redondant

Vous pouvez afficher l'état d'intégrité du contrôleur CMC de secours dans l'interface Web. Pour plus d'informations sur l'accès à l'état d'intégrité du contrôleur CMC dans l'interface Web, voir Affichage des informations de châssis et surveillance de l'intégrité des châssis et des composants.

Configuration du panneau avant

Vous pouvez configurer les paramètres suivants :

- Bouton d'alimentation
- Écran LCD
- Lecteur de DVD

Configuration du bouton d'alimentation

Pour configurer le bouton d'alimentation du châssis :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Panneau avant** > **Configurer**.
2. Sur la page **Configuration du panneau avant**, dans la section **Configuration du bouton d'alimentation**, sélectionnez l'option **Désactiver le bouton d'alimentation du châssis** et cliquez sur **Appliquer**.
   Le bouton d'alimentation du châssis est désactivé.

Configuration de l'écran LCD

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Panneau avant** > **Configurer** .
2. Sur la page **Configuration**, dans la section **Configuration de l'écran CD** :
   - Sélectionnez l'option **Verrouiller l'écran LCD du panneau de commande** pour désactiver les configurations que vous pouvez exécuter en utilisant l'interface LCD.
   - Dans le menu déroulant **Langue de l'écran LCD**, sélectionnez la langue voulue.
   - Dans le menu déroulant **Orientation de l'écran LCD**, sélectionnez **Mode Tour** ou **Mode Rack**.

   REMARQUE : Lorsque vous configurez le châssis en utilisant l'Assistant de l'écran LCD et que vous sélectionnez Appliquer automatiquement les paramètres aux nouveaux serveurs insérés, vous ne pouvez pas désactiver la fonction Appliquer automatiquement les paramètres aux nouveaux serveurs insérés en utilisant une licence de base. Si vous ne voulez pas utiliser cette fonction, ignorez le message sur l'écran LCD (il disparaît automatiquement) ou appuyez sur le bouton Ne pas accepter sur l'écran LCD et appuyez sur le bouton central.

3. Cliquez sur **Appliquer**.

Accès au serveur à l'aide de l'interface KVM

Pour associer le serveur à la console KVM et activer l'accès à la console distante de serveur via l'interface KVM, vous pouvez utiliser l'interface Web CMC, RACADM ou l'interface LCD.

Association d'un serveur à une console KVM à l'aide de l'interface Web CMC

Vérifiez que la console KVM est connectée au châssis.

Pour associer un serveur à une console KVM :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Panneau frontal** > **Configuration** .
2. Sur la page **Configuration du panneau frontal**, dans la section **Configuration KVM**, dans la liste **Console VM associée**, sélectionnez le logement à associer à une console KVM et cliquez sur **Appliquer**.

REMARQUE : Le module KVM permet l'adressage à tous les logements de serveur. L'insertion d'un serveur pleine hauteur ou le remplacement d'un serveur mi-hauteur par un serveur pleine hauteur ne modifie pas le comportement de l'adressage. Toutefois, si le KVM est adressé à un logement inférieur et que le logement contient un serveur pleine hauteur, le KVM est disponible uniquement par l'intermédiaire du logement supérieur. Vous devez réadresser le commutateur KVM aux logements supérieurs.

Assocation du serveur à l'interface KVM à l'aide de l'écran LCD

Vérifiez que la console KVM est connectée au châssis.

Pour associer le serveur à la console KVM en utilisant l'écran LCD, depuis l'écran **Menu principal** de l'écran LCD, accédez à **Association KVM**, sélectionnez le serveur à associer et appuyez sur OK.

Association d'un server à un lecteur de DVD

Pour associer un serveur à un lecteur de DVD du châssis :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Panneau frontal** > **Configuration** .
2. Sur la page **Configuration du panneau frontal**, sous la section **Configuration du lecteur de DVD** :

   dans le menu déroulant **Lecteur de DVD associé**, sélectionnez l'un des serveurs pour lequel l'accès au lecteur de DVD du châssis est nécessaire.
3. Cliquez sur **Appliquer**.

Le DVD permet l'adressage à tous les logements de serveur. L'insertion d'un serveur pleine hauteur ou le remplacement d'un serveur mi-hauteur par un serveur pleine hauteur ne modifie pas le comportement de l'adressage. Toutefois, si le DVD est adressé à un emplacement inférieur et que le logement contient un serveur pleine hauteur, le DVD est disponible uniquement via le logement supérieur. Vous devez réadresser le DVD aux logements supérieurs.

3

Connexion au contrôleur CMC

Vous pouvez vous connecter au contrôleur CMC en tant qu'utilisateur CMC local, utilisateur Microsoft Active Directory ou utilisateur LDAP. Le nom d'utilisateur et le mot de passe par défaut sont respectivement `root` et `calvin`. Vous pouvez également vous connecter par connexion directe (SSO) ou avec une connexion par carte à puce.

REMARQUE : Le contrôleur CMC ne prend pas en charge les caractères spéciaux suivants pour la création de nom d'utilisateur ou mot de passe du profil de châssis en langage XML :

" , ! , #, $, %, ^, &, *, (,), -, _, +, =, ?, {, }, +, &, >, |, ., ', [

Sujets :

Accès à l'interface Web CMC

Avant de vous connecter au contrôleur CMC avec l'interface Web, vérifiez que vous avez configuré un navigateur Web pris en charge (Internet Explorer ou Firefox) et que le compte utilisateur a été créé avec les privilèges nécessaires.

REMARQUE : Si vous utilisez Microsoft Internet Explorer pour vous connecter via un proxy et que l'erreur `The XML page cannot be displayed` s'affiche, vous devez désactiver le proxy pour continuer.

Pour accéder à l'interface Web CMC :

1. Ouvrez un navigateur Web pris en charge sur le système.

   Pour obtenir les dernières informations relatives aux navigateurs Web pris en charge, consultez le document *Dell Systems Software Support Matrix* sur le site **dell.com/support/manuals**.

2. Dans le champ **Adresse**, entrez l'URL suivante et appuyez sur <Entrée> :

   - Pour accéder à CMC avec l'adresse IPv4 : `https://<CMC IP address>`

     Si vous avez modifié le numéro de port HTTPS par défaut (port 443), entrez : `https://<CMC IP address>:<port number>`
   - Pour accéder à CMC avec l'adresse IPv6 : `https://[<CMC IP address>]`

     Si le numéro de port HTTPS par défaut (443) a été changé, tapez `https://[<CMC IP address>]:<port number>`, où *<CMC IP address>* est l'adresse IP du contrôleur CMC et *<port number>*, le numéro de port HTTPS.

     La page **Connexion à CMC** s'affiche.

   REMARQUE : Lorsque vous utilisez IPv6, vous devez placer l'adresse IP CMC entre crochets ([ ]).

Connexion au contrôleur CMC en tant qu'utilisateur local, utilisateur Active Directory ou utilisateur LDAP

Pour pouvoir vous connecter au contrôleur CMC, vous devez disposer d'un compte CMC doté du privilège **Connexion au contrôleur CMC**. Le nom d'utilisateur CMC par défaut est root et le mot de passe par défaut est calvin. Le compte root est le compte d'administration par défaut fourni avec le contrôleur CMC.

REMARQUE :

- **Pour plus de sécurité, Dell vous recommande vivement de modifier le mot de passe par défaut du compte root lors de la procédure de configuration initiale.**
- **Lorsque la validation des certificats est activée, vous devez fournir le nom de domaine complet (FQDN) du système. Si la validation de certificat est activée et que l'adresse IP est fournie pour le contrôleur de domaine, la connexion échoue.**

Le contrôleur CMC ne prend pas en charge les caractères ASCII étendus (ß, å, é, ü, etc.), ni les caractères utilisés dans des langues autres que l'anglais.

Pour vous connecter comme utilisateur local, utilisateur Active Directory ou utilisateur LDAP.

1. Dans le champ **Nom d'utilisateur**, entrez votre nom d'utilisateur :
   - Nom d'utilisateur du contrôleur CMC : <nom d'utilisateur>
   - Nom d'utilisateur Active Directory : <domaine>\<nom d'utilisateur>, <domaine>/<nom d'utilisateur> ou <utilisateur>@<domaine>.
   - Nom d'utilisateur LDAP : <nom d'utilisateur>

   REMARQUE : Ce champ est sensible à la casse.
2. Dans le champ **Mot de passe**, entrez le mot de passe de l'utilisateur.

   REMARQUE : Pour l'utilisateur Active Directory, le champ Nom d'utilisateur tient compte de la casse.
3. Dans le menu déroulant du champ **Domaine**, sélectionnez le domaine requis.
4. (Facultatif) Sélectionnez un délai d'expiration de session. Il s'agit de la période pendant laquelle vous pouvez rester connecté sans aucune activité avant d'être automatiquement déconnecté. La valeur par défaut est le **délai d'attente d'inactivité du service Web**.
5. Cliquez sur **OK**.

   Vous êtes connecté à CMC avec les privilèges utilisateur requis.

   Vous ne pouvez pas vous connecter à l'interface Web avec différents noms d'utilisateur dans plusieurs fenêtres du navigateur sur une seule station de travail.

REMARQUE : Si l'authentification LDAP est activée et que vous tentez de vous connecter au CMC à l'aide des informations d'identification locales, les informations d'identification sont d'abord vérifiées sur le serveur LDAP, puis dans le CMC.

Connexion au contrôleur CMC avec une carte à puce

Pour utiliser cette fonction, vous devez disposer d'une licence d'entreprise. Vous pouvez vous connecter au contrôleur CMC en utilisant une carte à puce. Une carte à puce fournit une authentification à deux facteurs qui offre une double sécurité :

- Périphérique de carte à puce physique.
- Code secret, tel qu'un mot de passe ou un code NIP.

Les utilisateurs doivent vérifier leurs données d'identification à l'aide de la carte à puce et du code PIN.

REMARQUE : Vous ne pouvez pas utiliser l'adresse IP pour vous connecter au contrôleur CMC avec une carte à puce. Kerberos valide vos références par rapport au nom de domaine qualifié.

Avant de vous connecter comme utilisateur Active Directory en utilisant une carte à puce :

- Téléversez un certificat d'autorité de certification (CA) de confiance, c'est-à-dire un certificat Active Directory signé par une autorité de certification, dans CMC.
- Configurez le serveur DNS.
- Activez la connexion Active Directory.
- Activez l'ouverture de session par carte à puce

Pour vous connecter au contrôleur CMC en tant qu'utilisateur Active Directory en utilisant une carte à puce :

1. Connectez-vous à CMC à l'aide du lien `https://<cmcname.domain-name>`.
   La page **Connexion à CMC** qui s'affiche vous invite à insérer une carte à puce.
   REMARQUE : Si vous avez changé le numéro de port HTTPS par défaut (port 80), accédez à la page Web CMC en utilisant `<cmcname.domain-name>:<port number>`, où cmcname est le nom d'hôte CMC du contrôleur CMC, *domain-name* est le nom du domaine et *port number* est le numéro du port HTTPS.
2. Introduisez la carte à puce, puis cliquez sur **Ouverture de session**.
   La boîte de dialogue PIN s'affiche.
3. Saisissez le code PIN, puis cliquez sur **Envoyer**.
   REMARQUE : Si l'utilisateur de la carte à puce est présent dans Active Directory, aucun mot de passe Active Directory n'est nécessaire. Autrement, vous devez vous connecter en utilisant un nom d'utilisateur et un mot de passe appropriés.

   Vous êtes connecté à CMC avec vos références Active Directory.

Connexion au CMC par connexion directe

Lorsque la connexion directe est activée, vous pouvez vous connecter au contrôleur CMC sans entrer les données de référence d'authentification utilisateur du domaine telles que le nom d'utilisateur et le mot de passe. Pour utiliser cette fonction, vous devez disposer d'une licence d'entreprise.

REMARQUE : Vous ne pouvez pas utiliser l'adresse IP pour vous connecter par connexion directe (SSO). Kerberos valide vos références par rapport au nom de domaine qualifié (FQDN).

Avant de vous connecter au contrôleur CMC en utilisant la connexion directe, vérifiez que :

- Vous vous êtes connecté au système en utilisant un compte utilisateur Active Directory.
- L'option de connexion directe est activée pendant la configuration Active Directory.

Pour vous connecter au contrôleur CMC en utilisant la connexion directe :

1. Connectez-vous au système client avec votre compte réseau.
2. Accédez à l'interface Web CMC en utilisant `https://<cmcname.domain-name>`
   Par exemple, `cmc-6G2WXF1.cmcad.lab`, où `cmc-6G2WXF1` est le nom du contrôleur CMC et `cmcad.lab`, le nom du domaine.
   REMARQUE : Si vous avez changé le numéro de port HTTPS par défaut (port 80), accédez à l'interface Web CMC en utilisant `<cmcname.domain-name>:<port number>`, où *cmacname* est le nom d'hôte CMC du contrôleur CMC, domain-name est le nom du domaine et port number est le numéro du port HTTPS.

   Le contrôleur CMC vous connecte en utilisant les références Kerberos mises en cache par votre navigateur lorsque vous vous êtes connecté avec votre compte Active Directory valide. Si la connexion échoue, le navigateur est redirigé vers la page de connexion CMC normale.
   REMARQUE : Si vous n'êtes pas connecté au domaine Active Directory et que vous n'utilisez pas le navigateur Internet Explorer, la connexion échoue et le navigateur affiche une page vierge.

Connexion au contrôleur CMC à l'aide de la console série, Telnet ou SSH

Vous pouvez vous connecter au contrôleur CMC via une connexion série, Telnet ou SSH.

Une fois le logiciel d'émulation de terminal de la station de gestion et le BIOS du nœud géré configurés, effectuez les étapes suivantes pour vous connecter au contrôleur CMC :

1. Connectez-vous au contrôleur CMC à l'aide du logiciel d'émulation de terminal de votre station de gestion.
2. Entrez votre nom d'utilisateur et votre mot de passe CMC, puis appuyez sur <Entrée>.
   Vous êtes connecté au contrôleur CMC.

Accès à CMC avec RACADM

RACADM fournit un ensemble de commandes qui vous permettent de configurer et de gérer le contrôleur CMC via une interface de type texte. Vous pouvez accéder à RACADM soit en utilisant une connexion Telnet/SSH ou série à l'aide de la console Dell CMC sur le KVM, soit ou à distance à l'aide de l'interface de ligne de commande RACADM installée sur une station de gestion.

L'interface RACADM est classée comme suit :

- RACADM distant : permet l'exécution de commandes RACADM sur une station de gestion avec l'option -r, et le nom DNS ou l'adresse IP du CMC.
  REMARQUE : RACADM distant est disponible sur le *DVD Dell Systems Management Tools and Documentation*, et il est installé sur une station de gestion.
- RACADM du firmware : vous permet de vous connecter au CMC à l'aide d'une connexion Telnet, SSH ou série. L'interface RACADM du firmware vous permet d'utiliser l'implémentation RACADM qui fait partie du firmware CMC.

Vous pouvez utiliser les commandes de l'interface RACADM distante dans des scripts pour configurer plusieurs CMC. Vous ne pouvez pas exécuter les scripts directement sur l'interface Web du CMC, car le contrôleur CMC ne prend pas en charge cette fonctionnalité.

Pour plus d'informations sur RACADM, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX*.

Pour plus d'informations sur la configuration de plusieurs CMC, voir « Configuration de plusieurs CMC avec RACADM ».

Connexion à CMC à l'aide de l'authentification par clé publique

Vous pouvez vous connecter au contrôleur CMC sur SSH sans entrer de mot de passe. Vous pouvez également envoyer une seule commande RACADM comme argument de ligne de commande à l'application SSH. Les options de ligne de commande fonctionnent pratiquement comme RACADM distant, car la session prend fin après l'exécution de la commande.

Avant de vous connecter au contrôleur CMC sur SSH, vérifiez que les clés publiques sont chargées. Pour utiliser cette fonction, vous devez disposer d'une licence d'entreprise.

Par exemple :

- **Connexion** : `ssh service@<domain>` ou `ssh service@<IP_address>`, où IP_address est l'adresse IP du contrôleur CMC.
- **Envoi de commandes RACADM** : `ssh service@<domain> racadm getversion` et `ssh service@<domain> racadm getsel`

Lorsque vous vous connectez en utilisant le compte de service et qu'une expression de passe a été définie lors de la création de la paire de clés publiques ou privées, un message vous invite à entrer de nouveau l'expression de passe. Si cette dernière est utilisée avec les clés, les systèmes client qui exécutent Windows et Linux permettent d'automatiser la méthode. Sur les systèmes client exécutant Windows, vous pouvez utiliser l'application Pageant. Cette application s'exécute en arrière-plan et rend transparente l'entrée de l'expression de passe. Pour les systèmes client exécutant Linux, vous pouvez utiliser l'agent ssh. Pour configurer et utiliser ces applications, voir la documentation du produit.

Sessions CMC multiples

La liste des sessions CMC possibles en utilisant les diverses interfaces est fournie ici.

Tableau 11. Sessions CMC multiples

Interface	Nombre de sessions
Interface web CMC	4
RACADM	4
Telnet	4
SSH	4

Modification du mot de passe d'ouverture de session par défaut

Le message d'avertissement qui vous permet de modifier le mot de passe par défaut s'affiche si :

- Vous vous connectez au CMC avec le privilège **Configurer les utilisateurs**.
- La fonction d'avertissement de mot de passe par défaut est activée.
- Le nom d'utilisateur et le mot de passe par défaut pour tous les comptes actuellement activés sont respectivement `root` et `calvin`.

Le même message d'avertissement s'affiche si vous vous connectez à l'aide de Active Directory ou LDAP. Les comptes Active Directory et LDAP ne sont pas pris en compte lorsque vous tentez de déterminer si un compte (local) possède les coordonnées `root` et `calvin`. Un message d'avertissement s'affiche également lorsque vous vous connectez au CMC à l'aide de SSH, Telnet, l'interface RACADM distante, ou de l'interface Web. Pour l'interface Web, SSH et Telnet, un message d'avertissement unique s'affiche pour chaque session. Dans le cas de l'interface RACADM distante, le message d'avertissement s'affiche pour chaque commande.

Pour modifier les coordonnées, vous devez disposer du privilège **Configurer les utilisateurs**.

REMARQUE : Un message de connexion au CMC est généré si l'option Ne plus afficher ce message d'avertissement est sélectionnée sur la page Connexion de CMC.

Modification du mot de passe d'ouverture de session par défaut à l'aide de l'interface Web

Lorsque vous ouvrez une session sur l'interface Web CMC, si la page **Avertissement de mot de passe par défaut** s'ouvre, cela signifie que vous pouvez changer le mot de passe. Pour ce faire :

1. Sélectionnez l'option **Modifier le mot de passe par défaut**.
2. Dans le champ **Nouveau mot de passe**, saisissez le nouveau mot de passe.

   Le mot de passe peut contenir un maximum de 20 caractères. Les caractères sont masqués. Les caractères suivants sont pris en charge :

   - 0-9
   - A-Z
   - a-z
   - Caractères spéciaux : +, &, ?, >, -, }, |, ., !, (, ', ,, _,[, ", @, #,), *, ;, $,], /, §, %, =, <, :, {, l, \

   Le contrôleur CMC ne prend pas en charge les caractères ASCII étendus (ß, å, é, ü, etc.), ni les caractères utilisés dans des langues autres que l'anglais. La définition de valeurs à l'aide de ces caractères entraîne un comportement imprévisible.
3. Dans le champ **Confirmer le mot de passe**, saisissez de nouveau le mot de passe.
4. Cliquez sur **Continuer**. Le nouveau mot de passe est configuré et vous êtes connecté(e) au CMC.

   REMARQUE : Le champ Continuer est activé uniquement si les mots de passe saisis dans les champs Nouveau mot de passe et Confirmer le mot de passe correspondent.

   Pour plus d'informations sur les autres champs, voir l'*Aide en ligne*.

Modification du mot de passe d'ouverture de session par défaut à l'aide de RACADM

Pour modifier le mot de passe, exécutez la commande RACADM suivante :

```
racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i <index> <newpassword>
```

où, `<index>` est une valeur comprise entre 1 et 16 (correspond au compte utilisateur) et `<newpassword>` est le nouveau mot de passe défini par l'utilisateur.

Pour plus d'informations, voir le document *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX) sur le site **dell.com/support/manuals**.

Activation ou désactivation du message d'avertissement du mot de passe par défaut

Vous pouvez activer ou désactiver l'affichage du message d'avertissement du mot de passe par défaut. Pour ce faire, vous devez disposer du privilège de **configuration des utilisateurs**.

Activation ou désactivation du message d'avertissement de mot de passe par défaut à l'aide de l'interface Web

Pour activer ou désactiver l'affichage du message d'avertissement de mot de passe par défaut suite à l'ouverture d'une session sur iDRAC :

1. Accédez à **Contrôleur de châssis** > **Authentification de l'utilisateur** > **Utilisateurs locaux** .
   La page **Utilisateurs** s'affiche.
2. Dans la section **Avertissement de mot de passe par défaut**, sélectionnez **Activer**, puis cliquez sur **Appliquer** pour activer l'affichage de la page **Avertissement de mot de passe par défaut** lorsque vous ouvrez une session sur CMC. Sinon, sélectionnez **Désactiver**.

   En variante, si cette fonction est activée et que vous ne souhaitez pas que le message d'avertissement s'affiche pour les ouvertures de session suivantes, à la page **Avertissement de mot de passe par défaut**, sélectionnez l'option **Ne plus afficher cet avertissement**, puis cliquez sur **Appliquer**.

Activation ou désactivation du message d'avertissement pour modifier le mot de passe d'ouverture de session par défaut à l'aide de RACADM

Pour activer l'affichage du message d'avertissement pour modifier le mot de passe d'ouverture de session par défaut à l'aide de RACADM, utilisez l'objet `racadm config -g cfgRacTuning -o cfgRacTuneDefCredentialWarningEnable<0> or <1>`. Pour plus d'informations, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de ligne de commande RACADM pour iDRAC7 et CMC), disponible à l'adresse **dell.com/support/manuals**.

Modification forcée du mot de passe à l'aide de l'interface Web

Vous pouvez modifier le mot de passe par défaut lorsque vous accédez à l'interface CMC pour la première fois. Cette fonctionnalité s'applique aux environnements accessibles sur le réseau et exige l'authentification du nom d'utilisateur et du mot de passe. Vous pouvez configurer et réinitialiser la fonctionnalité de **Modification forcée du mot de passe** à tout moment. Il est obligatoire de modifier votre mot de passe pour vous connecter et accéder à l'interface Web CMC. Le nom d'utilisateur est « root », par défaut.

1. Entrez le **Nouveau mot de passe**.

   Le mot de passe peut contenir un maximum de 20 caractères. Les caractères sont masqués. Les caractères suivants sont pris en charge :

   - 0-9
   - A-Z
   - a-z
   - Caractères spéciaux : +, &, ?, >, -, }, |, ., !, (, ', ,, _, [, ", @, #,), *, ;, $,], /, §, %, =, <, :, {, l, ~ et \

   Le contrôleur CMC ne prend pas en charge les caractères ASCII étendus (ß, å, é, ü, etc.), ni les caractères utilisés dans des langues autres que l'anglais. La définition de valeurs à l'aide de ces caractères entraîne un comportement imprévisible.
2. Saisissez une fois de plus le nouveau mot de passe dans la zone de texte **Confirmer le mot de passe**.
3. Cliquez sur **Continuer** pour appliquer le nouveau mot de passe à la connexion à l'interface Web CMC.

Scénarios de cas d'utilisation

Cette section décrit les cas d'utilisation et les tâches typiques que vous pouvez effectuer avec le CMC (Chassis Management Controller) version 3.3 pour Dell PowerEdge VRTX.

Conversion de la carte Shared PERC 8 externe du mode haute disponibilité (HA) au mode faible disponibilité à l'aide de l'interface Web

Deux cartes Shared PERC 8 externes doivent être présentes dans les logements PCI 5 et PCI 6 du châssis Dell PowerEdge VRTX en mode HA.

Flux de travail

1. Mettez hors tension le châssis. Déconnectez tous les câbles SAS allant des cartes Shared PERC 8 externes aux enceintes MD12x0.
2. Mettez sous tension le châssis.
3. Connectez-vous à l'interface Web CMC, puis rendez-vous sur **stockage→ Contrôleurs→ Dépannage** et activez la **Tolérance de panne** dans le menu déroulant pour la carte Shared PERC 8 externe dans le logement 5, cliquez sur **Appliquer** et sélectionnez désactiver pour le logement 6, puis cliquez sur **Appliquer**.
4. La réinitialisation des deux contrôleurs PERC peut prendre deux minutes. Au bout de deux minutes, le mode du PERC apparaît comme Haute disponibilité (HA).
5. Mettez hors tension le châssis et connectez les enceintes en mode autre que HA.
6. Mettez sous tension le châssis.
7. La carte Shared PERC 8 externe n'est pas en mode Haute disponibilité (HA), rendez-vous sur**Stockage→ Dépannage → Dépannage de la configuration** pour afficher l'état autre que HA.

Conversion du mode Faible disponibilité au mode Haute disponibilité d'une carte Shared PERC 8 externe à l'aide de l'interface Web

Deux cartes Shared PERC 8 externes doivent être présentes dans les logements PCI 5 et PCI 6 du châssis Dell PowerEdge VRTX.

Flux de travail

1. Mettez hors tension le châssis. Déconnectez tous les câbles SAS allant des cartes Shared PERC 8 externes aux enceintes MD12x0.
2. Mettez sous tension le châssis.
3. Connectez-vous à l'interface CMC Web puis rendez-vous sur **Stockage→ Contrôleurs→ Dépannage** et activez la **Tolérance de panne** dans le menu déroulant pour la carte Shared PERC 8 externe dans le logement 5, cliquez sur **Appliquer** et sélectionnez désactiver pour le logement 6, puis cliquez sur **Appliquer**.
4. La réinitialisation des deux contrôleurs PERC peut prendre deux minutes. Au bout de deux minutes, le mode du PERC apparaît comme Haute disponibilité (HA).
5. Mettez le châssis hors tension et connectez les enceintes en mode HA.
6. Mettez sous tension le châssis.
7. La carte Shared PERC 8 externe est en mode Haute disponibilité ; rendez-vous sur**Stockage→ Dépannage → Dépannage de la configuration** pour afficher l'état HA.

Conversion de la carte Shared PERC 8 externe du mode haute disponibilité (HA) au mode faible disponibilité à l'aide de RACADM

Deux cartes Shared PERC 8 externes doivent être présentes dans les logements PCI 5 et PCI 6 du châssis Dell PowerEdge VRTX et doivent être en mode HA.

Flux de travail

1. Mettez hors tension le châssis. Déconnectez tous les câbles SAS allant des cartes Shared PERC 8 externes aux enceintes MD12x0.
2. Mettez sous tension le châssis.
3. Connectez-vous au CMC racadm et exécutez la commande suivante quand les serveurs sont hors tension :

```
racadm  raid set controllers:RAID.ChassisSlot.5-1 -p HighAvailabilityMode None
```

4. Exécutez la commande `racadm raid set controllers:RAID.ChassisSlot.6-1 -p HighAvailabilityMode None` sur la carte Shared PERC 8 externe dans le logement 6.
5. La réinitialisation des deux contrôleurs PERC peut prendre deux minutes avant d'apparaître en mode Haute disponibilité/HA (High Availability).
6. Mettre le châssis hors tension et connectez les enceintes en mode autre que HA.
7. Mettez sous tension le châssis.
8. La carte Shared PERC 8 externe ne se trouve pas en mode HA (HighAvailabiltiy) et la commande suivante est utilisée pour afficher la condition :

```
racadm raid get controllers -o -p HighAvailabilityMode
```

Conversion du mode Faible disponibilité au mode Haute disponibilité d'une carte Shared PERC 8 externe à l'aide de RACADM

Des cartes Shared PERC 8 externes doivent être présentes dans les logements PCI 5 et PCI 6 du châssis Dell PowerEdge VRTX.

Flux de travail

1. Mettez hors tension le châssis. Déconnectez tous les câbles SAS allant des cartes Shared PERC 8 externes aux enceintes MD12x0.
2. Mettez sous tension le châssis.
3. Connectez-vous au Racadm CMC et exécutez la commande suivante quand les serveurs sont hors tension :

```
racadm raid set controllers:RAID.ChassisSlot.5-1 -p HighAvailabilityMode ha
```

4. Exécutez la commande `racadm raid set controllers:RAID.ChassisSlot.6-1 -p HighAvailabilityMode ha` sur la carte Shared PERC 8 externe dans le logement 6.
5. La réinitialisation des deux contrôleurs PERC peut prendre deux minutes. Au bout de deux minutes, le mode du PERC apparaît comme Haute disponibilité (HA).
6. Mettez hors tension le châssis et connectez les enceintes en mode HA.
7. Mettez sous tension le châssis.
8. La carte Shared PERC 8 externe est en mode Haute disponibilité et l'état HA est visible à l'aide de la commande suivante :

```
racadm raid get controllers -o -p HighAvailabilityMode
```

.

4

Mise à jour du micrologiciel

Vous pouvez mettre à jour le micrologiciel de :

- CMC
- Infrastructure du châssis
- Module d'extension VRTX ou Micrologiciel du module d'extension du fond de panier de stockage d'enceintes intégrées ou externes
- Disques physiques (HDD) par enceinte

REMARQUE : Vous pouvez mettre à jour le micrologiciel de disque dur uniquement si nécessaire.

Vous pouvez mettre à jour le micrologiciel des E/S et des composants du serveur suivants :

- Module d'E/S
- BIOS
- iDRAC
- Lifecycle Controller
- Diagnostics 32 bits
- Pack de pilotes de système d'exploitation
- Contrôleurs d'interface réseau (NIC)
- Contrôleurs RAID sur le module de serveur

REMARQUE : La mise à jour du micrologiciel peut prendre plusieurs minutes à s'effectuer.

Sujets :

Téléchargement du firmware du contrôleur CMC

Avant de procéder à la mise à jour du firmware, téléchargez la dernière version du firmware à partir du site **support.dell.com** et enregistrez-la sur le système local.

Lors de la mise à jour du firmware du châssis VRTX, il est recommandé de mettre à jour les versions firmwareles des composants du châssis dans l'ordre suivant :

1. firmware des composants du serveur lame
2. firmware du contrôleur Chassis Management Controller (CMC)
3. firmware de l'infrastructure du châssis
4. firmware du Shared PERC 8 (intégré et externe)
5. Firmware du fond de panier de stockage interne et modules d'extension du boîtier externe
6. Firmware de disque dur (boîtiers intégrés et externes)

Pour plus d'informations sur la séquence de mise à jour pour le châssis VRTX, reportez-vous aux *notes de mise à jour de la version 3.3 du firmware CMC* disponibles sur **dell.com/cmcmanuals**.

Affichage des versions de micrologiciel actuellement installées

Vous pouvez afficher les versions installées du micrologiciel avec l'interface Web CMC ou RACADM.

Affichage des versions du micrologiciel actuellement installées avec l'interface Web CMC

Dans l'interface Web CMC, accédez à l'une des pages suivantes pour afficher les versions actuelles du micrologiciel :

- **Présentation du châssis** > **Mise à jour**
- **Présentation du châssis** > **Contrôleur de châssis** > **Mise à jour**
- **Présentation du châssis** > **Présentation du serveur** > **Mise à jour des composants serveur**
- **Présentation du châssis** > **Présentation du module d'E/S** > **Mise à jour**
- **Présentation du châssis** > **Stockage** > **Mise à jour des composants de stockage**

La page **Mise à jour du micrologiciel** affiche la version actuelle du micrologiciel de chaque composant répertorié et permet de mettre à jour le micrologiciel vers la dernière version.

Si le châssis contient un serveur d'une génération antérieure dont l'iDRAC est en mode Restauration ou que le contrôleur CMC détecte que le micrologiciel iDRAC est endommagé, l'iDRAC de génération antérieure est également répertorié dans la page **Mise à jour du micrologiciel**.

Affichage des versions du micrologiciel actuellement installées à l'aide de RACADM

Pour afficher les informations IP d'iDRAC et du contrôleur CMC et le numéro de service ou d'inventaire CMC à l'aide de RACADM, exécutez la sous-commande `racadm getsysinfo`. Pour plus d'informations sur les autres commandes RACADM, voir le document *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX).

Mise à jour du firmware du contrôleur CMC

Vous pouvez mettre à jour le firmware du CMC dans l'interface Web ou avec RACADM. Par défaut, la mise à jour du firmware conserve les paramètres actuels du CMC. Au cours du processus de mise à jour, vous avez la possibilité de rétablir les paramètres de configuration par défaut du CMC.

REMARQUE : Pour pouvoir mettre à jour le firmware du contrôleur CMC, vous devez disposer du privilège d'administration de configuration du châssis.

Si une session de l'interface utilisateur Web est utilisée pour mettre à jour le firmware d'un composant système, le paramètre **Délai d'inactivité (0, 60–10800)** doit avoir une valeur suffisamment élevée pour gérer la durée du transfert. Parfois, le transfert de fichiers de firmware peut prendre jusqu'à 30 minutes. Pour définir le délai d'inactivité, voir Configuration des services.

Lors des mises à jour du firmware CMC, une partie ou l'ensemble des ventilateurs du châssis tourne à 100 %.

Si vous avez installé des contrôleurs CMC redondants dans le châssis, il est recommandé de mettre à jour simultanément les deux contrôleurs CMC vers la même version du firmware. Si les firmwares des CMC sont différents, des résultats inattendus peuvent survenir en cas de basculement.

REMARQUE :

- **Le firmware CMC ne peut pas être mis à jour vers une version antérieure autre que la version 2.0 pour un châssis qui est configuré avec une alimentation de 1 600 W.**

- **La mise à jour ou la restauration du firmware du CMC est prise en charge uniquement pour les versions du firmware 1.2, 1.25, 1.3, 1.31, 1.35, 1.36, 2.0, 2.01, 2.04 et ultérieures. Pour toute autre version, commencez par effectuer une mise à jour vers l'une de ces versions, puis effectuez une mise à jour vers la version requise.**

Après le chargement du firmware, le CMC actif est réinitialisé et devient temporairement indisponible. S'il existe un CMC de secours, les rôles « actif » et « de secours » s'inversent. Le contrôleur CMC de secours devient le contrôleur CMC actif. Si une mise à jour est appliquée uniquement au contrôleur CMC actif, le contrôleur CMC actif n'exécute pas l'image mise à jour une fois la réinitialisation terminée : seul le contrôleur CMC de secours exécute cette image. En général, il est vivement recommandé de conserver des versions de firmware identiques pour le contrôleur CMC actif et le contrôleur CMC de secours.

Une fois le CMC de secours mis à jour, inversez les rôles des CMC de sorte que le CMC qui vient d'être mis à jour devienne le CMC actif et que le CMC dont le firmware est plus ancien devienne celui de secours. Pour plus d'informations sur l'inversion des rôles, voir la section sur la commande `cmcchangeover` dans le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX*. Vous pouvez ainsi vérifier que la mise à jour a réussi et que le nouveau firmware fonctionne correctement avant d'appliquer la mise à jour au deuxième CMC. Une fois les deux CMC mis à jour, vous pouvez rétablir les rôles précédents des CMC à l'aide de la commande `cmcchangeover`. La révision 2.x du firmware du CMC met à jour le contrôleur CMC principal et le contrôleur CMC redondant sans exécuter la commande `cmcchangeover`.

Pendant les phases finales du processus de mise à jour du firmware dans le CMC, la session dans le navigateur et la connexion au contrôleur CMC sont temporairement perdues lorsque le CMC n'est pas connecté au réseau. Le CMC indique que l'intégrité générale du châssis est critique du fait de la perte temporaire du réseau. Lorsque le contrôleur CMC redémarre après quelques minutes, ouvrez une session dans celui-ci. Le CMC indique ensuite que l'intégrité générale du châssis est intègre et la liaison réseau du CMC est établie. Après la réinitialisation du contrôleur CMC, la nouvelle version du firmware s'affiche sur la page **Mise à jour du firmware**.

Pour éviter de déconnecter d'autres utilisateurs pendant une réinitialisation, informez les utilisateurs autorisés susceptibles de se connecter au CMC, et vérifiez si des sessions actives existent dans la page **Sessions**. Pour ouvrir la page **Sessions**, cliquez sur **Présentation du châssis** dans le volet de gauche, cliquez sur **Réseau**, puis sur **Sessions**.

Lorsque vous transférez des fichiers vers et depuis le CMC, l'icône de transfert de fichiers tourne pendant le transfert. Si votre icône est inactive, vérifiez que votre navigateur est configuré pour permettre les animations. Pour plus d'informations sur les animations dans le navigateur, voir Autoriser les animations dans Internet Explorer.

REMARQUE : Si vous avez configuré la longueur du nom de logement à plus de 15 caractères dans la version actuelle de CMC, la mise à niveau du firmware CMC tronque sa longueur à 15 caractères.

Image de micrologiciel CMC signé.

Pour CMC M1000e version 2.0 et les versions ultérieures, le micrologiciel contient une signature. Le micrologiciel CMC vérifie la signature afin de vérifier l'authenticité du micrologiciel téléversé. La mise à jour du micrologiciel aboutit uniquement si l'image du micrologiciel est authentifiée par CMC comme image valide auprès du fournisseur de service et qu'elle n'a pas été modifiée. La mise à jour du micrologiciel est interrompue si CMC ne peut pas vérifier la signature de l'image de micrologiciel téléversée. Un événement d'avertissement est consigné et le message d'erreur approprié s'affiche.

La vérification de la signature peut être exécutée sur VRTX firmware versions 1.2 et les versions suivantes. Pour les régressions de micrologiciel vers des versions antérieures à 1.1, vous devez d'abord mettre à jour le micrologiciel vers une version VRTX CMC postérieure ou égale à la version 1.2, mais antérieure à 2.0. Après cette mise à jour (régression de micrologiciel vers une version antérieure), les versions VRTX non signées peuvent être exécutées.

Mise à jour du firmware du CMC et de la carte principale.

Les fonctions partagées de la carte Shared PERC 8 externe ne sont pas disponibles tant que le firmware CMC et la carte principale n'ont pas été mis à jour.

REMARQUE :

- **Pour afficher le schéma de câblage MD12x0, reportez-vous au *Guide de l'utilisateur de la mise à niveau de PowerEdge VRTX pour la prise en charge d'extension de stockage partagé* ou au *Guide de l'utilisateur des cartes du contrôleur Dell PowerEdge RAID (PERC) 8 pour les systèmes Dell PowerEdge VRTX* disponibles à l'adresse dell.com/support/manuals.**
- **La carte de stockage externe partagé exige que vous mettiez à jour le CMC à la version 2.20 ou une version ultérieure et la carte principale à la version 2.21 ou une version ultérieure pour prendre en charge la carte Shared PERC 8 externe.**
- **Vous ne pouvez pas rétrograder le firmware CMC à une version antérieure à 2.2 avec les cartes partagées externes.**

Pour mettre à jour le firmware CMC et celui de la carte principale :

1. Mise à jour du firmware de CMC.
2. Mise à jour du firmware de la carte principale.
3. Mettez le châssis hors tension et installez les cartes de stockage partagé dans les logements PCIe 5 et 6.
4. Mise sous tension du châssis.
5. Après la mise sous tension du châssis, mettez à jour les cartes de stockage partagé externe.

REMARQUE : Par défaut, la carte de stockage Shared PERC 8 externe n'est pas en mode Tolérance de panne. Vous devez la passer en mode Tolérance de panne après l'avoir correctement raccordée. Pour plus d'informations, reportez-vous à *Mise à niveau de PowerEdge VRTX pour la prise en charge d'extension de stockage partagé*.

Dans un événement, si vous voulez restaurer le firmware CMC ou MPC/de la carte principale ou la version firmwarele de CMC et de MPC, effectuez les tâches suivantes :

Pour restaurer le firmware CMC et de la carte principale :

1. Mettez le châssis hors tension.
2. Retirez des logements PCI toutes les cartes de stockage externe.
3. Mettez sous tension le châssis.
4. Restaurez le firmware CMC et/ou de la carte principale.

Vous ne pouvez pas rétrograder le CMC, si une carte de stockage partagé externe est détectée.

Si les processus ne sont pas exécutés dans l'ordre indiqué, le comportement du système devient aléatoire et le système peut devenir partiellement instable. Le CMC consigne des messages IOV ou de contrôleur RAID. Seuls les adressages VA du stockage partagé pour PERC 1 et PERC 2 sont visibles dans l'ancienne version du CMC. La version précédente du CMC ne contient pas tous les adressages VA du stockage partagé externe. Si une carte de stockage partagé externe PERC 8 est insérée après la restauration, le CMC la traite comme une carte non partagée. Cela peut être dû au fait que le pilote PERC hôte ne prend pas en charge la carte de stockage Shared PERC 8 externe.

Mise à jour du firmware CMC à l'aide de l'interface Web

REMARQUE :

- **Avant d'appliquer la mise à jour du module CMC, assurez-vous que le châssis est sous tension. Si les lames sont sous tension, il n'est pas nécessaire de les mettre hors tension pour effectuer la mise à jour du CMC.**
- **Le processus de rétrogradation du firmware CMC à une version antérieure à 2.1 avec des adaptateurs externes partagés est bloqué.**

Pour mettre à jour le firmware du contrôleur CMC en utilisant l'interface Web CMC :

1. Dans le volet de gauche, accédez aux pages suivantes :
   - **Présentation du châssis** > **Mise à jour**
   - **Présentation du châssis** > **Contrôleur de châssis** > **Mise à jour**
2. Sur la page **Mise à jour du firmware**, dans la section **Firmware CMC**, sélectionnez les composants requis dans la colonne **Mettre à jour les cibles** du ou des contrôleurs CMC (si un contrôleur CMC de secours existe) à mettre à jour, puis cliquez sur **Appliquer la mise à jour CMC**.
3. Dans le champ **Image de firmware**, cliquez sur **Parcourir** (Internet Explorer ou Firefox) ou **Sélectionner un fichier** (Google Chrome) pour naviguer vers l'emplacement de fichier. Le nom par défaut du fichier image du firmware CMC est `vrtx_cmc.bin`.
4. Cliquez sur **Commencer la mise à jour du firmware**. La section **Avancement de la mise à jour du firmware** fournit des informations sur l'état de mise à jour du firmware. Un indicateur d'état s'affiche sur la page pendant le chargement du fichier d'image. La durée du transfert de fichiers varie en fonction du débit de la connexion. Lorsque le processus de mise à jour interne démarre, la page est automatiquement actualisée et l'horloge de mise à jour du firmware s'affiche.
5. Pour un CMC en veille, une fois la mise à jour terminée, le champ **État de la mise à jour** affiche **Terminé**. Pour un CMC actif, pendant les phases finales du processus de mise à jour du firmware, la session de navigateur et la connexion au contrôleur CMC sont temporairement perdues car le contrôleur CMC actif n'est pas connecté au réseau. Vous devez vous connecter au bout de quelques minutes, une fois que le contrôleur CMC actif a redémarré. Après la réinitialisation du CMC, le nouveau firmware s'affiche sur la page **Mise à jour du firmware**.

   REMARQUE : Après la mise à jour du firmware, supprimez les fichiers de la mémoire cache du navigateur Web. Pour savoir comment vider la mémoire cache du navigateur Web, consultez l'aide en ligne du navigateur.

Instructions supplémentaires :

- Au cours d'un transfert de fichiers, ne cliquez pas sur l'icône **Actualiser** ou ne changez pas de page.
- Pour annuler le processus, sélectionnez l'option **Annuler le transfert de fichiers et la mise à jour**. Cette option n'est disponible que pendant le transfert de fichiers.
- Le champ **État de la mise à jour** affiche l'état de mise à jour du firmware.

  REMARQUE : La mise à jour du contrôleur CMC peut prendre plusieurs minutes.

Mise à jour du firmware CMC via RACADM

Pour mettre à jour le firmware du CMC à l'aide de RACADM, utilisez la sous-commande `fwupdate`. Pour plus d'informations sur les commandes RACADM, reportez-vous au *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX*.

REMARQUE : Exécutez la commande de mise à jour du firmware via une seule session racadm à distance à la fois.

Mise à jour du micrologiciel de l'infrastructure du châssis

La mise à jour de l'infrastructure du châssis met à jour les composants, tels que le micrologiciel de la carte principale et celui de la gestion du sous-système PCIe.

REMARQUE : Pour mettre à jour le micrologiciel de l'infrastructure du châssis, assurez-vous que le châssis est sous tension et que les serveurs sont hors tension.

REMARQUE : Lorsque la carte principale est mise à niveau vers une version ultérieure, le châssis et Chassis Management Controller peuvent redémarrer.

Mise à jour du micrologiciel de l'infrastructure du châssis à l'aide de l'interface Web CMC

1. Accédez à l'une des pages suivantes :
   - **Présentation du châssis** > **Mise à jour**.
   - **Présentation du châssis** > **Contrôleur de châssis** > **Mise à jour**.
2. Sur la page **Mise à jour du micrologiciel**, dans la section **Micrologiciel de l'infrastructure du châssis**, dans la colonne **Mettre à jour les cibles**, sélectionnez l'option et cliquez sur **Appliquer le micrologiciel de l'infrastructure du châssis**.
3. Sur la page **Mettre à jour le micrologiciel**, cliquez sur **Parcourir**, puis sélectionnez le micrologiciel d'infrastructure de châssis approprié.
4. Cliquez sur **Lancer la mise à jour du micrologiciel**, puis cliquez sur **Oui** pour continuer.
   La section **Avancement de la mise à jour du micrologiciel** contient des informations sur l'état de la mise à jour du micrologiciel. Pendant le téléversement du fichier image, un indicateur d'état s'affiche sur la page. Le délai de transfert du fichier varie en fonction de la vitesse de la connexion. Lorsque la mise à jour commence, la page s'actualise automatiquement et le chronomètre de mise à jour du micrologiciel s'affiche.

Instructions supplémentaires à suivre :

- Ne cliquez pas sur l'icône **Actualiser** et ne naviguez vers aucune autre page pendant le transfert de fichier.
- Le champ **État de la mise à jour** affiche l'état de mise à jour du micrologiciel.

Une fois la mise à jour terminée, vous perdez brièvement la connexion à la carte mère, car elle se réinitialise ; le nouveau micrologiciel apparaît dans la page **Mise à jour du micrologiciel**.

Mise à jour du micrologiciel de l'infrastructure du châssis à l'aide de RACADM

Pour mettre à jour le micrologiciel de l'infrastructure du châssis en utilisant RACADM, utilisez la sous-commande `fwupdate`. Pour plus d'informations sur l'utilisation des commandes RACADM, voir le document *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX).

Mise à jour du micrologiciel iDRAC du serveur

Vous pouvez mettre à jour le micrologiciel de l'iDRAC à l'aide de l'interface Web CMC ou de RACADM. Pour pouvoir utiliser cette fonction, vous devez disposer d'une licence d'entreprise.

La version du micrologiciel iDRAC doit être 1.40.40 ou ultérieure pour les serveurs avec iDRAC.

L'iDRAC (sur un serveur) se réinitialise et il est temporairement indisponible après une mise à jour de micrologiciel.

REMARQUE : Pour mettre à jour un micrologiciel iDRAC via le contrôleur de gestion du châssis, une carte SD doit être disponible dans le châssis. Cependant, pour mettre à jour le micrologiciel iDRAC via l'interface Web iDRAC, une carte SD n'est pas requise dans CMC. Pour plus d'informations sur le lancement de l'interface Web iDRAC à partir de CMC, voir Lancement d'iDRAC à partir de la page Condition du serveur.

Mise à jour du micrologiciel du contrôleur iDRAC du serveur avec l'interface Web

Pour mettre à jour le micrologiciel iDRAC dans le serveur :

1. Accédez à l'une des pages suivantes :
   - **Présentation du châssis** > **Mise à jour**.
   - **Présentation du serveur** > **Mise à jour** > **Mise à jour des composants du serveur**.

   La page **Mise à jour de micrologiciel** s'affiche.

   REMARQUE :

   Vous pouvez également mettre à jour le micrologiciel iDRAC du serveur avec Présentation du châssis > Présentation du serveur > Mise à jour. Pour en savoir plus, voir Mise à jour du micrologiciel des composants du serveur.
2. Pour mettre à jour le micrologiciel iDRAC7 ou 8, dans la section **Micrologiciel iDRAC7** ou **Micrologiciel iDRAC8**, selon le cas, cliquez sur le lien **Mise à jour** correspondant au serveur dont vous voulez mettre à jour le micrologiciel.
   La page **Mise à jour des composants de serveur** s'affiche. Pour continuer, voir la section Mise à jour du micrologiciel des composants de serveur.
3. Dans le champ **Image de micrologiciel**, entrez le chemin d'un fichier d'image de micrologiciel figurant sur la station de gestion ou sur le réseau partagé, ou cliquez sur **Parcourir** pour naviguer vers le fichier voulu. Le nom par défaut de l'image de micrologiciel iDRAC est `firming.imc`.
4. Cliquez sur **Lancer la mise à jour du micrologiciel**, puis cliquez sur **Oui** pour continuer.
   La section **Avancement de la mise à jour du micrologiciel** contient les informations d'état de la mise à jour du micrologiciel. Une barre d'avancement indique l'état du téléversement. La durée du transfert de fichier varie en fonction de la vitesse de la connexion. Lorsque la mise à jour interne commence, la page s'actualise automatiquement et le chronomètre de la mise à jour du micrologiciel s'affiche.

   REMARQUE : Instructions supplémentaires à suivre :
   - **Ne cliquez pas sur l'icône Actualiser et ne naviguez vers aucune autre page pendant le transfert de fichiers.**
   - **Pour annuler le processus, cliquez sur Annuler le transfert de fichier et la mise à jour. Cette option n'est disponible que pendant le transfert de fichier.**
   - **Le champ État de la mise à jour affiche l'état de mise à jour du micrologiciel.**

   La mise à jour du micrologiciel iDRAC peut prendre jusqu'à 10 minutes.

Mise à jour du firmware des composants de serveur

La fonctionnalité de mise à jour de type un à plusieurs dans le CMC vous permet de mettre à jour le firmware des composants du serveur sur plusieurs serveurs. Vous pouvez mettre à jour les composants du serveur à l'aide des modules de mise à jour Dell (Dell Update Packages) disponibles sur le système local ou en partage réseau. Cette opération est activée à l'aide de la fonction Lifecycle Controller sur le serveur.

Le service Lifecycle Controller est disponible sur chaque serveur et facilité par iDRAC. Vous pouvez gérer le firmware des composants et des périphériques sur les serveurs à l'aide du service Lifecycle Controller. Lifecycle Controller utilise un algorithme d'optimisation pour mettre à jour le firmware afin de réduire le nombre de redémarrages nécessaires.

Lifecycle Controller fournit le support de mise à jour de module pour iDRAC7 et les serveurs ultérieurs.

REMARQUE : Le CMC ne prend pas en charge la mise à jour du firmware de la carte SSD PCIE sur la page de mise à jour du firmware une-à-plusieurs.

REMARQUE : Mettez à jour les versions de firmware des serveurs avant d'utiliser la fonctionnalité de mise à jour basée sur Lifecycle Controller.

REMARQUE : Pour mettre à jour le firmware de composants, vous devez activer l'option CSIOR pour les serveurs.

Pour activer CSIOR :

- Serveurs de 12e génération et ultérieurs : après le redémarrage du serveur, depuis la configuration F2, sélectionnez **Paramètres iDRAC** > **Lifecycle Controller**, puis activez **CSIOR** et enregistrez les changements.
- Serveurs de 13e génération : après avoir redémarré le serveur, lorsque vous y êtes invité, appuyez sur F10 pour accéder au Lifecycle Controller. Accédez à la page **Inventaire du matériel** en sélectionnant **Configuration matérielle** > **Inventaire du matériel**. Sur la page **Inventaire du matériel**, cliquez sur **Collecter l'inventaire système au redémarrage**.

La méthode de **Mise à jour à partir d'un fichier** vous permet de mettre à jour le firmware des composants du système à l'aide des fichiers DUP stockés sur un système local. Vous pouvez sélectionner les composants de serveur individuels pour mettre à jour le firmware à l'aide des fichiers DUP requis. Vous pouvez mettre à jour un grand nombre de composants en même temps à l'aide d'une carte SD afin de stocker un fichier DUP d'une taille de mémoire supérieure à 48 Mo.

REMARQUE : Notez les points suivants :

- **Lors de la sélection des composants de serveur individuels en vue de la mise à jour, assurez-vous qu'il n'existe aucune condition préalable pour les composants sélectionnés. La sélection de certains composants dont la mise à jour dépend de conditions préalables associées à d'autres composants peut provoquer un arrêt brutal du fonctionnement du serveur.**
- **Assurez-vous de mettre à jour les composants de serveur dans l'ordre prescrit. Sinon, le processus de mise à jour du firmware de composants risque d'échouer.**

  Mettez toujours à jour les modules de firmware de composant de serveur dans l'ordre suivant :

  - **BIOS**
  - **Lifecycle Controller**
  - **iDRAC**

La mise à jour toutes lames en un seul clic ou la méthode de **Mise à jour à partir du partage réseau** vous permettent de mettre à jour le firmware des composants du serveur à l'aide des fichiers DUP stockés sur le partage réseau. Vous pouvez utiliser la fonctionnalité de mise à jour basée sur Dell Repository Manager (DRM) pour accéder aux fichiers DUP stockés sur le partage en réseau et mettre à jour les composants du serveur en une seule opération. Vous pouvez définir une logithèque distante personnalisée des fichiers DUP du firmware et des images binaires à l'aide du Dell Repository Manager et la partager sur le partage en réseau. Vous pouvez également utiliser Dell Repository Manager (DRM) pour rechercher les dernières mises à jour firmwareles disponibles. Dell Repository Manager (DRM) permet de s'assurer que les systèmes Dell sont à jour et disposent de la dernière version du BIOS, des pilotes, des firmwares et des logiciels. Vous pouvez rechercher les dernières mises à jour disponibles sur le site de Support (**support.dell.com**) pour les plates-formes prises en charge en fonction de la marque, du modèle ou du numéro de série. Vous pouvez télécharger les mises à jour ou créer une logithèque à partir des résultats de la recherche. Pour plus d'informations sur l'utilisation de DRM pour rechercher les dernières mises à jour du firmware, consultez la section *Utilisation de Dell Repository Manager pour rechercher les dernières mises à jour sur le site de support de Dell* sur https://www.kb.dell.com/. Pour plus d'informations sur l'enregistrement du fichier d'inventaire qu'utilise DRM comme entrée pour créer les référentiels, consultez la section Enregistrement du rapport d'inventaire du châssis à l'aide de l'interface Web CMC.

REMARQUE : La méthode de mise à jour Un seul clic pour toutes les lames présente les avantages suivants :

- **Vous permet de mettre à jour tous les composants sur tous les serveurs lames avec un minimum de clics.**
- **Toutes les mises à jour sont regroupées dans un répertoire. Cela évite d'avoir à télécharger individuellement le firmware de chaque composant.**
- **Méthode plus rapide et cohérente de mise à jour des composants du serveur.**
- **Permet de maintenir une image standard avec les versions de mises à jour requises pour les composants de serveur qui peuvent être utilisés pour mettre à jour plusieurs serveurs en une seule opération.**
- **Vous pouvez copier les répertoires des mises à jour depuis l'utilitaire Dell Server Update (SUU), télécharger le DVD ou créer et personnaliser les versions de mise à jour requises dans Dell Repository Manage DRM. Vous n'avez pas besoin de la version la plus récente de Dell Repository Manager pour créer ce répertoire. Cependant, la version 1.8 de Dell Repository Manager fournit une option permettant de créer une logithèque (répertoire des mises à jour) en fonction de l'inventaire qui a été exporté depuis les serveurs dans le châssis. Pour plus d'informations sur la création d'une logithèque à l'aide de Dell Repository Manager, consultez le *Guide de l'utilisateur du datacenter Dell Repository Manager version 1.8* et le *Guide de l'utilisateur Dell Repository Manager Business Client version 1.8*, disponibles sur dell.com/support/manuals.**

Lifecycle Controller prend en charge la mise à jour de modules via iDRAC. Il vous est recommandé de mettre à jour le firmware du CMC avant de mettre à jour les modules de firmware des composants de serveur. Après la mise à jour du firmware CMC, dans l'interface Web du CMC, vous pouvez mettre à jour le firmware des composants du serveur depuis la page **Tour d'horizon du châssis** > **Tour d'horizon du serveur Mise à jour** > **Mise à jour des composants du serveur**. Il vous est également recommandé de sélectionner tous les modules des composants d'un serveur devant être mis à jour ensemble. Ceci permet au Lifecycle Controller d'utiliser ses algorithmes optimisés pour mettre à jour le firmware, réduisant ainsi le nombre de redémarrages.

Pour mettre à jour le firmware des composants d'un serveur, dans l'interface Web CMC, cliquez sur **Présentation du châssis** > **Présentation du serveur** > **Mettre à jour** > **Mise à jour des composants du serveur**.

Si le serveur ne prend pas en charge le service Lifecycle Controller, la section **Inventaire des firmwares des composants/appareils** affiche **Non pris en charge**. Pour les serveurs nouvelle génération, installez le firmware Lifecycle Controller et mettez à jour le firmware iDRAC afin d'activer le service Lifecycle Controller sur le serveur. Pour les serveurs de génération antérieure, cette mise à niveau est impossible.

Le firmware Lifecycle Controller est installé à l'aide du module d'installation approprié, exécuté dans le système d'exploitation du serveur. Pour les serveurs pris en charge, un module spécial d'installation ou de réparation doté d'une extension de fichier `.usc` est disponible. Ce fichier vous permet d'installer le firmware de Lifecycle Controller via la fonctionnalité de mise à jour du firmware disponible sur l'interface de navigation Web iDRAC.

Vous pouvez aussi installer le firmware de Lifecycle Controller à l'aide d'un module d'installation approprié, exécuté dans le système d'exploitation du serveur. Pour plus d'informations, consultez le *Guide de l'utilisateur Dell Lifecycle Controller*.

Si le service Lifecycle Controller est désactivé sur le serveur, la section **Inventaire des firmwares des composants/périphériques** affiche :

```
Lifecycle Controller may not be enabled.
```

REMARQUE : La méthode « InstallFromURI » peut ne pas fonctionner si l'URI contient des espaces blancs.

Si le firmware est mis à jour à la même version, une erreur d'incompatibilité de firmware EMM non critique s'affiche sur la page **intégrité du châssis**. Pour résoudre ce problème, redémarrez le châssis VRTX après une mise à jour EMM.

REMARQUE : Avec une carte SSD PCIe NVMe de Samsung, la case à cocher pour la mise à jour du firmware ne s'affiche pas dans la page mise à jour du firmware une-à-plusieurs.

Séquence de mise à jour des composants du serveur

En cas de mise à jour de composants individuels, vous devez mettre à jour les versions des micrologiciels des composants de serveur dans l'ordre qui suit :

- iDRAC
- Lifecycle Controller
- Diagnostics (en option)
- Packs de pilotes OS (en option)
- BIOS

- Carte réseau
- RAID
- Autres composants

REMARQUE : Lorsque vous mettez à jour les versions micrologicielles de tous les composants serveur en une fois, la séquence de mise à jour est gérée par le Lifecycle Controller.

Activation de Lifecycle Controller

Vous pouvez activer le service Lifecycle Controller lors de la mise sous tension d'un serveur :

- Pour les serveurs iDRAC, sur la console de démarrage, appuyez sur la touche <F2> pour accéder à **Configuration du système**.
- Sur la page **Menu principal Configuration système**, accédez au menu **Paramètres d'iDRAC** > **Lifecycle Controller**, puis cliquez sur **Activé**. Retournez à la page **Menu principal Configuration système** et cliquez sur **Terminer** pour enregistrer les paramètres.

L'annulation des services système permet d'annuler toutes les tâches planifiées en attente et de les supprimer de la file d'attente.

Pour plus d'informations sur le service Lifecycle Controller, les composants de serveur pris en charge et la gestion du firmware de périphériques, voir le document :

- *Lifecycle Controller-Guide de démarrage rapide des services à distance*.
- **delltechcenter.com/page/Lifecycle+Controller**.

La page **Mise à jour des composants de serveur** vous permet de mettre à jour les différents composants du firmware sur le serveur. Pour utiliser les fonctions et fonctionnalités de cette page, vous devez disposer des éléments suivants :

- Contrôleur CMC : privilège **d'administration du serveur**.
- iDRAC : **Configuration d'iDRAC** et **Connexion à iDRAC**.

Si les droits sont insuffisants, vous ne pouvez afficher que l'inventaire des firmwares des composants et périphériques sur le serveur. Vous ne pouvez pas sélectionner de composants ou de périphériques pour exécuter une quelconque opération Lifecycle Controller sur le serveur.

Sélection du type de mise à jour du micrologiciel des composants du serveur via l'interface Web CMC

Pour sélectionner le type de composant de serveur type de mise à jour :

1. Dans l'arborescence système, accédez à **Présentation du serveur**, puis cliquez sur**Mise à jour** > **Mise à jour des composants de serveur**.
   La page **Mise à jour des composants de serveur** s'affiche.
2. Dans la section **Choisir le type de mise à jour**, sélectionnez la méthode de mise à jour requise :
   - **Mise à jour depuis un fichier**
   - **Mise à jour depuis un partage réseau**

Filtrage des composants pour les mises à jour micrologicielles

Les informations de tous les composants et périphériques de tous les serveurs sont collectées simultanément. Pour gérer cet important volume d'informations, Lifecycle Controller offre différents mécanismes de filtrage :

REMARQUE : Pour utiliser cette fonction, vous devez disposer d'une licence d'entreprise.

La section **Filtre de mise à jour des composants/périphériques** dans la page **Mise à jour des composants de serveur** qui permet de filtrer les informations en fonction du composant, est uniquement disponible pour le mode **Mise à jour par fichier**.

Ces filtres permettent de :

- sélectionner une ou plusieurs catégories de composants ou périphériques pour une visualisation aisée,
- comparer les versions micrologicielles des composants et périphériques répartis sur le serveur,
- Pour limiter la catégorie d'un composant ou d'un périphérique en fonction des types ou des modèles, filtrez automatiquement les composants et les périphériques sélectionnés.

REMARQUE : La fonction de filtrage automatique est importante lorsque vous utilisez un progiciel DUP (Dell Update Package, progiciel de mise à jour Dell). La programmation d'un progiciel DUP peut reposer sur le type ou le modèle d'un composant ou périphérique. Le comportement de filtrage automatique est conçu pour minimiser les décisions de sélection suivantes après la sélection initiale.

Voici quelques exemples où les mécanismes de filtrage sont appliqués :

- Si vous choisissez le filtre BIOS, seul l'inventaire BIOS de tous les serveurs s'affiche. Si l'ensemble de serveurs réunit un certain nombre de modèles de serveurs et que vous sélectionnez un serveur pour la mise à jour du BIOS, la logique de filtrage automatique supprime automatiquement tous les autres serveurs qui ne correspondent pas au modèle du serveur sélectionné. Cela garantit que la sélection de l'image de mise à jour du micrologiciel BIOS (DUP) est compatible avec le modèle de serveur correct.

  Parfois, une même image de mise à jour du micrologiciel BIOS peut être compatible avec plusieurs modèles de serveur. Ce type d'optimisation est ignoré, au cas où cette compatibilité ne serait plus vraie à l'avenir.
- Le filtrage automatiquement est important pour les mises à jour du micrologiciel des cartes d'interface réseau et des contrôleurs RAID. Ces catégories de périphériques regroupent plusieurs types et modèles. De même, les images de mise à jour du micrologiciel (DUP) peuvent être disponibles dans des formats optimisés, où un seul DUP peut être programmé pour mettre à jour plusieurs types ou modèles de périphériques dans une catégorie donnée.

Filtrage des composants pour la mise à jour des micrologiciels avec l'interface Web CMC

Pour filtrer les périphériques :

1. Dans le volet de gauche, accédez à **Présentation du serveur**, puis cliquez sur **Mettre à jour**.
2. Sur la page **Mise à jour des composants du serveur**, dans la section **Filtre de mise à jour de composant/périphérique**, sélectionnez un ou plusieurs des éléments suivants :
   - **BIOS**
   - **iDRAC**
   - **Lifecycle Controller**
   - **Diagnostics 32 bits**
   - **Pack de pilotes du système d'exploitation**
   - **Contrôleur d'interface réseau**
   - **Contrôleur RAID**

   La section **Filtre de mise à jour des composants/périphériques** est affichée uniquement en mode de mise à jour du micrologiciel **Mise à jour par fichier**.

   La section **Inventaire du micrologiciel** contient uniquement les composants ou périphériques associés sur tous les serveurs présents dans le châssis. Lorsque vous sélectionnez un élément dans le menu déroulant, seuls les composants ou périphériques associés à ceux de la liste s'affichent.

   Une fois l'ensemble de composants et de périphériques filtré affiché dans la section d'inventaire, un filtrage supplémentaire peut être appliqué lorsque vous sélectionnez un composant ou périphérique pour la mise à jour. Par exemple, si vous avez activé le filtre BIOS, la section d'inventaire affiche tous les serveurs avec uniquement leur composant BIOS. Si le composant BIOS de l'un des serveurs est sélectionné, l'inventaire est filtré encore davantage pour afficher les serveurs dont le nom de modèle correspond à celui du serveur sélectionné.

   Si aucun filtre n'est sélectionné et que vous effectuez une sélection de mise à jour d'un composant ou de périphérique dans la section d'inventaire, le filtre associé à la sélection est automatiquement activé. Un filtrage supplémentaire peut se produire lorsque la section d'inventaire affiche tous les serveurs possédant une correspondance pour le composant sélectionné en terme de modèle, de type ou d'identification. Par exemple, si vous sélectionnez pour mise à jour le composant BIOS de l'un des serveurs, le filtre BIOS est automatiquement activé et la section d'inventaire affiche les serveurs correspondant au nom de modèle du serveur sélectionné.

Filtrage des composants pour la mise à jour des micrologiciels avec RACADM

Pour filtrer les composants pour les mises à jour de micrologiciel à l'aide de RACADM, exécutez la commande **getversion** :

```
racadm getversion -l [-m <module>] [-f <filtre>]
```

Pour plus d'informations, voir le document *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX) sur le site **dell.com/support/manuals**.

Affichage de l'inventaire des micrologiciels

Vous pouvez afficher le récapitulatif des versions de micrologiciel de tous les composants et périphériques de tous les serveurs actuellement présents dans le châssis, ainsi que leur condition.

REMARQUE : Pour pouvoir utiliser cette fonction, vous devez disposer d'une licence d'entreprise.

Affichage de l'inventaire des micrologiciels dans l'interface Web CMC

Pour afficher l'inventaire des micrologiciels :

1. Dans le volet de gauche, cliquez sur **Présentation du serveur** et sur **Mettre à jour**.
2. Sur la page **Mise à jour des composants du serveur**, consultez les informations d'inventaire des micrologiciels dans la section **Inventaires des micrologiciels des composants/périphériques**. Cette page contient les informations suivantes :
   - Les serveurs qui ne prennent pas en charge le service Lifecycle Controller portent la mention **Non pris en charge**. Vous disposez d'un lien hypertexte d'accès vers une autre page permettant de mettre directement à jour le micrologiciel de l'iDRAC uniquement. Cette page prend en charge la mise à jour du micrologiciel de l'iDRAC, mais pas celle des autres composants et périphériques du serveur. La mise à jour du micrologiciel iDRAC est indépendante du service Lifecycle Controller.
   - Si le serveur est répertorié comme **Pas prêt**, cela implique que, lors de la collecte de l'inventaire des micrologiciels, l'iDRAC du serveur était encore en cours d'initialisation. Attendez que l'iDRAC soit pleinement opérationnel, puis actualisez la page pour récupérer à nouveau l'inventaire des micrologiciels.
   - Si l'inventaire des composants et périphériques ne reflète pas les éléments physiquement installés sur le serveur, exécutez le Lifecycle Controller pendant le processus d'amorçage du serveur. Cela permet d'actualiser les informations concernant les composants intégrés et les périphériques et de vérifier les périphériques et composants actuellement installés. L'inventaire ne reflète pas précisément les informations de composants et de périphériques lorsque :
     - le micrologiciel iDRAC du serveur est mis à jour pour introduire la fonctionnalité Lifecycle Controller à la gestion du serveur,
     - vous insérez de nouveaux périphériques dans le serveur.

     Pour automatiser cette action, l'utilitaire iDRAC Settings fournit une option accessible via la console d'amorçage.

     a. Pour les serveurs iDRAC, dans la console d'amorçage, appuyez sur <F2> pour accéder à la **configuration du système**.
     b. Sur la page du **menu principal de la configuration du système**, cliquez sur **Paramètres iDRAC** > **Collecter l'inventaire du système au redémarrage**, sélectionnez **Activé**, revenez à la page du **menu principal de la configuration du système**, puis cliquez sur **Terminer** pour enregistrer les paramètres.
   - Vous disposez dans cet écran d'options permettant d'exécuter différentes opérations Lifecycle Controller, notamment la mise à jour, la restauration (rollback), la réinstallation et la suppression de tâches. Vous ne pouvez réaliser qu'un seul type de tâche à la fois. Des composants et périphériques non pris en charge peuvent être répertoriés dans l'inventaire, mais vous ne pourrez y effectuer aucune opération Lifecycle Controller.

Le tableau suivant contient des informations sur les composants et périphériques du serveur :

Tableau 12. Informations sur les composants et périphériques

Champ	Description
Emplacement	Indique le logement occupé par le serveur dans le châssis. Les numéros de logement sont des ID séquentiels allant de 1 à 4 (pour les 4 logements disponibles dans le châssis), qui vous aident à identifier l'emplacement du serveur dans le châssis. Si moins de 4 serveurs occupent des logements, seuls les logements contenant un serveur sont affichés.
Nom	Affiche le nom du serveur dans chaque logement.
Modèle	Affiche le modèle du serveur.
Composant/ Périphérique	Affiche la description du composant ou périphérique dans le serveur. Si la colonne est trop étroite, utilisez l'outil de pointage à la souris pour afficher la description.
Version actuelle	Affiche la version actuelle du composant ou du périphérique sur le serveur.
Version de la restauration	Affiche la version de restauration du composant ou du périphérique sur le serveur.

Tableau 12. Informations sur les composants et périphériques (suite)

Champ	Description
Condition de la tâche	Indique l'état des opérations planifiées sur le serveur. L'état des tâches est mis à jour dynamiquement en continu. Si le système détecte l'achèvement d'une tâche, les versions de micrologiciel des composants et périphériques du serveur correspondant sont automatiquement actualisées si la version de micrologiciel sur ces composants/périphériques a changé. Une icône d'information s'affiche également en regard de l'état actuel pour fournir des informations supplémentaires sur l'état actuel de la tâche. Vous affichez ces informations en cliquant ou en pointant sur cette icône.
Mettre à jour	Cliquez pour sélectionner le composant ou le périphérique dont le micrologiciel doit être mis à jour sur le serveur.

Affichage de l'inventaire des micrologiciels avec RACADM

Pour afficher l'inventaire des micrologiciels avec RACADM, utilisez la commande `getversion` :

```
racadm getversion -l [-m <module>] [-f <filtre>]
```

Pour plus d'informations, voir le document *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX) sur le site **dell.com/support/manuals**.

Enregistrement du rapport d'inventaire du châssis à l'aide de l'interface Web CMC

Pour enregistrer le rapport d'inventaire de châssis :

1. Dans l'arborescence système, accédez à **Présentation du serveur**, puis cliquez sur **Mise à jour** > **Mise à jour des composants de serveur**.
   La page **Mise à jour des composants de serveur** s'affiche.
2. Cliquez sur **Enregistrer le rapport d'inventaire**.
   Le fichier *Inventory.xml* est enregistré sur un système externe.

   REMARQUE : Dell Repository Manager Application utilise le fichier *Inventory.xml* comme entrée pour créer un référentiel des mises à jour pour toutes les lames disponibles dans le châssis. Ce référentiel peut être exporté ultérieurement vers un partage réseau. Le mode Mise à jour depuis un partage réseau de mise à jour du micrologiciel utilise ce partage réseau pour mettre à jour les composants de tous les serveurs. Vous devez avoir activé CSIOR sur les serveurs et enregistré le rapport d'inventaire du châssis chaque fois qu'il existe une modification de la configuration matérielle et logicielle du châssis.

Configuration du Partage réseau via l'interface Web du CMC

Pour configurer ou modifier l'emplacement du Partage réseau ou de références :

1. Dans l'interface Web CMC, ouvrez l'arborescence système, accédez à **Présentation du serveur**, puis cliquez sur **Partage réseau**.
   La page **Modifier le partage réseau** s'affiche.

   REMARQUE : Lorsque vous disposez du même dossier pour les profils de châssis, de serveur et d'identité de démarrage et qu'il y a plus de 100 profils, vous risquez de rencontrer des problèmes de performances.
2. Dans la section **Paramètres de partage réseau**, configurez les paramètres suivants de la façon requise :
   - Protocole
   - Adresse IP ou nom d'hôte
   - Nom du partage
   - Dossier de mise à jour
   - Nom de fichier (facultatif)

REMARQUE : La saisie du Nom de fichier est en option uniquement lorsque le nom de fichier du catalogue par défaut est `catalog.xml`. Si le nom de fichier du catalogue est modifié, vous devez saisir le nouveau nom dans ce champ.

- Dossier de profil
- Nom de domaine
- Nom d'utilisateur
- Mot de passe
- Version SMB

REMARQUE : L'option SMB version est uniquement disponible si le type de protocole est CIFS.

REMARQUE : Si vous utilisez CIFS lorsqu'il est enregistré avec un domaine et que vous y accédez en utilisant l'adresse IP avec les informations d'identification de l'utilisateur local CIFS, vous devez saisir le nom d'hôte ou l'adresse IP de l'hôte dans le champ Nom de domaine.

Pour plus d'informations, voir l'*Aide en ligne CMC*.

3. Cliquez sur **Répertoire de test** pour vérifier si les répertoires sont lisibles et inscriptibles.
4. Cliquez sur **Test de la connexion réseau** pour vérifier si l'emplacement de partage réseau est accessible.

   Lorsque vous appliquez une version SMB, le partage de réseau existant n'est ni monté ni démonté de nouveau au moment où vous cliquez sur **Tester la connexion du réseau** ou que vous naviguez vers d'autres pages de l'interface graphique.
5. Cliquez sur **Appliquer** pour appliquer les modifications des propriétés de partage réseau.

   REMARQUE :

   Cliquez sur **Précédent** pour revenir à la page **Mise à jour des composants du serveur**.

Opérations de tâche Lifecycle Controller

REMARQUE : Pour utiliser cette fonction, vous devez disposer d'une licence d'entreprise.

Vous pouvez réaliser les opérations Lifecycle Controller suivantes :

- Réinstallation
- Restauration
- Mettre à jour
- Suppression de tâches

Vous ne pouvez réaliser qu'un seul type d'opération à la fois. Des composants et périphériques non pris en charge peuvent être répertoriés dans l'inventaire, mais vous ne pouvez y effectuer aucune opération Lifecycle Controller.

Pour réaliser des opérations Lifecycle Controller, vous devez disposer des éléments suivants :

- Pour CMC : privilège Server Administrator.
- Pour iDRAC : privilèges Configurer iDRAC et Ouvrir une session iDRAC.

Une opération Lifecycle Controller planifiée sur un serveur peut prendre 10 à 15 minutes. Le processus implique plusieurs redémarrages du serveur, au cours desquels l'installation du micrologiciel est effectuée et qui incluent également une étape de vérification du micrologiciel. Vous pouvez afficher l'avancement de ce processus dans la console du serveur. Si vous avez besoin de mettre à jour plusieurs composants ou périphériques d'un serveur, vous pouvez regrouper toutes les mises à jour en une seule opération planifiée, ce qui minimise le nombre de redémarrages nécessaire.

Une opération peut parfois être tentée alors que vous êtes déjà en train de soumettre une autre opération pour planification dans une autre session ou un autre contexte. Dans ce cas, un message pop-up de confirmation s'affiche, indiquant la situation et signalant que l'opération ne doit pas être soumise. Attendez la fin de l'opération en cours avant de soumettre à nouveau la nouvelle opération.

Ne quittez pas la page affichée après avoir soumis une opération à planifier. Si vous le faites, un message de confirmation s'affiche permettant d'annuler la navigation. Sinon, l'opération est interrompue. Toute interruption, particulièrement pendant une opération de mise à jour, peut provoquer l'arrêt du téléversement du fichier image du micrologiciel avant son achèvement. Une fois que vous avez soumis l'opération à planifier, acceptez le message de confirmation signalant la réussite de la planification de l'opération.

Réinstallation du micrologiciel des composants des serveurs

Vous pouvez réinstaller l'image du micrologiciel déjà installé des composants ou des périphériques sélectionnés sur un ou plusieurs serveurs. L'image du micrologiciel est disponible dans le Lifecycle Controller.

Réinstallation du micrologiciel des composants de serveur à l'aide de l'interface Web

Pour réinstaller le micrologiciel d'un composant d'un serveur :

1. Dans le volet de gauche, cliquez sur **Présentation du serveur** > **Mettre à jour**.
2. La page **Mise à jour des composants du serveur** s'affiche. Dans la section **Choix du type de mise à jour**, sélectionnez **Mettre à jour depuis un fichier**.
3. Dans la colonne **Version actuelle**, cochez la case du composant ou périphérique dont vous voulez réinstaller le micrologiciel.
4. Sélectionnez l'une des options suivantes :
   - **Redémarrer maintenant** : redémarre immédiatement le serveur.
   - **Au prochain redémarrage** : permet de redémarrer manuellement le serveur ultérieurement.
5. Cliquez sur **Réinstaller**. La version du micrologiciel du composant ou du périphérique sélectionné est réinstallée.

Restauration (rollback) du micrologiciel des composants de serveur

Vous pouvez réinstaller une image de micrologiciel précédemment installée pour les composants ou périphériques sélectionnés sur un ou plusieurs serveurs. L'image de micrologiciel est disponible dans le Lifecycle Controller pour l'opération de restauration (rollback). Cette disponibilité dépend de la logique de compatibilité de versions du Lifecycle Controller. Le système part également de l'hypothèque que la mise à jour précédente est passée par le Lifecycle Controller.

REMARQUE : Pour pouvoir utiliser cette fonction, vous devez disposer d'une licence d'entreprise.

Restauration du micrologiciel des composants de serveur à l'aide de l'interface Web CMC

Pour restaurer une version précédente du micrologiciel d'un composant d'un serveur :

1. Dans le volet de gauche, cliquez sur **Présentation du serveur→Mettre à jour**.
2. La page **Mise à jour des composants de serveur** s'affiche. Dans la section **Choisir le type de mise à jour**, sélectionnez **Mettre à jour depuis un fichier**.
3. Dans la colonne **Restaurer la version**, sélectionnez l'option du composant ou du périphérique dont vous voulez restaurer le micrologiciel.
4. Sélectionnez l'une des options suivantes :
   - **Redémarrer maintenant** : redémarre immédiatement le serveur.
   - **Au prochain redémarrage** : permet de redémarrer manuellement le serveur ultérieurement.
5. Cliquez sur **Restaurer**. La version du micrologiciel précédemment installée du composant ou du périphérique sélectionné est réinstallée.

Mise à niveau du micrologiciel des composants de serveur

Vous pouvez installer la nouvelle version de l'image de micrologiciel des composants ou périphériques sélectionnés sur un ou plusieurs serveurs. L'image de micrologiciel est disponible dans le service Lifecycle Controller pour l'opération de restauration. Pour pouvoir utiliser cette fonction, vous devez disposer d'une licence d'entreprise.

REMARQUE : Pour la mise à jour du micrologiciel du contrôleur iDRAC et des packs de pilotes de système d'exploitation, vérifiez que la fonction de stockage étendu est activée.

Il est recommandé d'effacer la file d'attente des travaux avant de lancer la mise à jour du micrologiciel des composants d'un serveur. La liste de toutes les tâches sur les serveurs est disponible dans la page **Tâches Lifecycle Controller**. Cette page permet de supprimer une ou plusieurs tâches ou de purger toutes les tâches sur un serveur.

Les mises à jour du BIOS sont propres au modèle de serveur. Parfois, même si vous sélectionnez une seule carte d'interface réseau pour la mise à niveau du micrologiciel sur un serveur, la mise à jour peut être appliquée à toutes les cartes NIC du serveur. Ce comportement est inhérent à la fonction Lifecycle Controller, en particulier pour le code de programmation inclus dans les mises à jour DUP (Dell Update Package). Actuellement, seuls les DUP inférieurs à 48 Mo sont pris en charge.

Si la taille de l'image de fichier de mise à jour dépasse cette valeur, l'état de la tâche indique que le téléchargement a échoué. Si vous lancez plusieurs mises à jour de composants sur un serveur, la taille combinée de tous les fichiers de mise à jour du micrologiciel peut également dépasser 48 Mo. Dans ce cas, une des mises à jour de composants échoue, car le fichier de mise à jour correspondant est tronqué. Pour mettre à jour plusieurs composants sur un serveur, il est recommandé de commencer par mettre à jour le Lifecycle Controller et les composants Diagnostics 32 bits ensemble. Ils ne nécessitent aucun redémarrage du serveur et leur mise à jour est assez rapide. Vous pouvez ensuite mettre à jour simultanément tous les autres composants.

Toutes les mises à jour du Lifecycle Controller sont planifiées pour exécution immédiate. Toutefois, les services système peuvent parfois retarder cette exécution. Dans ce cas, la mise à jour échoue car le partage distant hébergé par le CMC n'est plus disponible.

Mise à niveau du micrologiciel des composants de serveur d'un fichier utilisant l'interface Web du CMC

Pour mettre à niveau la version du micrologiciel des composants du serveur à la version suivante à l'aide de la méthode **Mettre à jour depuis le fichier** :

1. Dans l'interface Web du CMC, ouvrez l'arborescence système, accédez à **Présentation du serveur**, puis cliquez sur **Mise à jour** > **Mise à jour des composants de serveur**.
   La page **Mise à jour des composants de serveur** s'affiche.
2. Dans la section **Choisir le type de mise à jour** , sélectionnez **Mettre à jour depuis un fichier**. Pour plus d'informations, reportez-vous à la section Choix du type de mise à jour de mocrologiciel de composant de serveur en utilisant l'interface Web CMC.
3. Dans la section **Filtre de mise à jour des composants/périphériques**, filtrez le composant ou le périphérique (en option). Pour plus d'informations, voir Filtrage des composants pour les mises à jour de micrologiciel à l'aide de l'interface Web CMC.
4. Dans la colonne **Mise à jour**, cochez les cases des composants ou périphériques dont vous voulez mettre à jour le micrologiciel vers la nouvelle version. Utilisez la touche de raccourci CRTL pour sélectionner le type de composant ou de périphérique à mettre à jour sur l'ensemble des serveurs applicables. En appuyant sur la touche CRTL et en la maintenant enfoncée, vous mettez tous les composants en surbrillance en jaune. Tout en maintenant la touche CRTL enfoncée, sélectionnez le composant ou périphérique voulu en cochant la case associée dans la colonne **Mise à jour**.

   La deuxième table qui s'affiche répertorie le type de composant ou de périphérique sélectionné, ainsi qu'un sélecteur de fichier d'image de micrologiciel. Pour chaque type de composant, l'écran affiche un seul sélecteur de fichier d'image de micrologiciel.

   Quelques périphériques, comme les cartes d'interface réseau (NIC) et les contrôleurs RAID, contiennent un grand nombre de types et de modèles. La logique de sélection des mises à jour filtre automatiquement le type de périphérique ou le modèle approprié sur la base des périphériques initialement sélectionnés. La cause principale de ce comportement de filtrage automatique est que vous ne pouvez spécifier qu'un seul fichier d'image de micrologiciel pour la catégorie.

   REMARQUE : Vous pouvez ignorer la limite de taille de mise à jour d'un seul progiciel DUP ou de DUP combinés, si la fonction de stockage étendu est installée et activée. Pour plus d'informations sur l'activation du stockage étendu, voir « Configuration de la carte de stockage étendu CMC ».
5. Spécifiez le fichier d'image de micrologiciel du ou des composants ou périphériques sélectionnés. Il s'agit d'un fichier DUP (Dell Update Package, progiciel de mise à jour Dell) Microsoft Windows.
6. Sélectionnez l'une des options suivantes :

- **Redémarrer maintenant** : redémarrez immédiatement. La mise à jour du micrologiciel s'appliquera immédiatement
- **Au prochain redémarrage** : redémarrez le serveur manuellement ultérieurement. La mise à jour du micrologiciel est appliquée au prochain démarrage.

REMARQUE : Cette étape n'est pas valide pour la mise à jour du micrologiciel du Lifecycle Controller et de Diagnostics 32 bits. Un redémarrage du serveur n'est pas nécessaire pour ces périphériques.

7. Cliquez sur **Mise à jour**. La version du micrologiciel est mise à jour pour le composant ou périphérique sélectionné.

Un seul clic de mise à jour des composants de serveur à l'aide de Network Share (partage de réseau)

La mise à jour des composants d'un serveur ou de plusieurs à partir d'un partage réseau à l'aide Dell Repository Manager et de l'intégration de châssis Dell PowerEdge VRTX simplifie la mise à jour en utilisant un micrologiciel de groupe personnalisé, ce qui permet d'effectuer les déploiements plus rapidement et plus facilement. La mise à jour à partir d'un partage réseau permet de mettre à jour tous les serveurs 12G simultanément avec un seul catalogue unique à partir d'un partage CIFS ou NFS.

Cette méthode fournit un moyen simple et rapide de créer un référentiel personnalisé pour vos systèmes Dell en utilisant Dell Repository Manager et le fichier d'inventaire du châssis exporté à l'aide de l'interface Web CMC. DRM permet de créer un référentiel personnalisé qui inclut uniquement les packages de mise à jour pour la configuration spécifique du système. Vous pouvez également créer des référentiels contenant des mises à jour uniquement pour les périphériques qui ne sont pas à jour, ou à un référentiel de base qui contient les mises à jour de tous les périphériques. Vous pouvez également créer des groupes de mises à jour pour Linux ou Windows en fonction du mode de mise à jour requis. DRM permet d'enregistrer le référentiel dans un partage CIFS ou NFS. L'interface Web CMC permet de configurer les informations d'identification et les informations d'emplacement du partage. A l'aide de l'interface Web CMC, vous pouvez effectuer la mise à jour des composants d'un seul serveur ou de plusieurs serveurs.

Configuration requise pour utiliser le mode de mise à jour à partir du partage réseau

Les conditions suivantes doivent exister pour mettre à jour le micrologiciel des composants du serveur à l'aide du mode Partage réseau :

- Les serveurs doivent appartenir à la 12e génération minimum et posséder une licence iDRAC Enterprise.
- La version CMC doit être la version 2.0 ou une version ultérieure.
- Lifecycle Controller doit être activé sur les serveurs.
- iDRAC 1.50 ou version ultérieure doit être disponible sur les serveurs de 12e génération.
- Dell Repository Manager 1.8, ou une version ultérieure, doit être installé sur le système.
- Vous devez détenir les privilèges d'administrateur CMC.

Mise à niveau du firmware des composants de serveur à partir d'un partage réseau à l'aide de l'interface Web du CMC

Pour mettre à niveau la version du firmware de composants de serveur à la version suivante à l'aide du mode **Mettre à jour partir d'un partage réseau** :

1. Dans l'interface Web CMC, ouvrez l'arborescence système, accédez à **Présentation du serveur**, puis cliquez sur **Mise à jour** > **Mise à jour des composants de serveur**.
   La page **Mise à jour des composants de serveur** s'affiche.
2. Dans la section **Choisir le type de mise à jour**, sélectionnez **Mise à jour depuis un partage réseau**. Pour plus d'informations, reportez-vous à la section Sélection du type de mise à jour du firmware des composants de serveur.
3. Si le partage réseau n'est pas connecté, configurez le partage réseau pour le châssis. Pour configurer ou modifier les détails du partage réseau, dans le tableau Propriétés du partage réseau, cliquez sur **Modifier**. Pour plus d'informations, reportez-vous à la section Configuration du partage réseau à l'aide de l'interface Web du CMC.
4. Cliquez sur l'option **Enregistrer le rapport d'inventaire** pour exporter le fichier d'inventaire du châssis qui contient les composants et les informations de firmware.
   Le fichier *Inventory.xml* est enregistré sur un système externe. Dell Repository Manager utilise le fichier *inventory.xml* pour créer des bundles de mises à jour personnalisés. Cet espace de stockage est situé dans le partage CIFS ou NFS configuré par le CMC. Pour plus

d'informations sur la création d'un espace de stockage à l'aide du Dell Repository Manager, voir le *Guide de l'utilisateur du Dell Repository Manager Data Center Version 1.8* et le *Guide de l'utilisateur du Dell Repository Manager Business Client Version 1.8*, disponibles sur **dell.com/support/manuals**.

5. Cliquez sur l'option **Rechercher les mises à jour** pour afficher les mises à jour du firmware disponibles dans le partage réseau. La section **Inventaire du firmware des composants/périphériques** affiche les versions actuelles du firmware des composants et périphériques répartis sur tous les serveurs présents dans le châssis et les versions du firmware des progiciels DUP disponibles dans le Partage réseau.

   REMARQUE : Cliquez sur Réduire en regard d'un logement pour réduire les détails relatifs au firmware des composants et des périphériques pour ce logement spécifique. Sinon, pour afficher de nouveau tous les détails, cliquez sur Développer.

6. Dans la section **Inventaire des firmwares des composants/périphériques**, cochez la case en regard de l'option **Sélectionner/Désélectionner tout** pour sélectionner tous les serveurs pris en charge. Sinon, cochez la case correspondant au serveur pour lequel vous souhaitez mettre à jour le firmware des composants du serveur. Vous ne pouvez pas sélectionner des composants individuels du serveur.
7. Sélectionnez une des options suivantes pour indiquer si un redémarrage de système est requis après la planification des mises à jour :
   - Redémarrer maintenant : les mises à jours sont planifiées et le serveur redémarre, appliquant immédiatement les mises à jour aux composants du serveur.
   - Au prochain redémarrage : les mises à jour sont planifiées mais ne s'appliquent qu'au prochain redémarrage du serveur.
8. Cliquez sur **Mettre à jour** pour planifier les mises à jour du firmware de composants disponibles des serveurs sélectionnés. Un message s'affiche en fonction du type de mises à jour contenues et vous demande de confirmer si vous souhaitez continuer.
9. Cliquez sur **OK** pour poursuivre et terminer la planification de la mise à jour du firmware pour les serveurs sélectionnés. Remarque :

   REMARQUE : La colonne État des tâches affiche l'état de la tâche des opérations planifiées sur le serveur. La condition de la tâche est mise à jour de manière dynamique.

Versions du micrologiciel prises en charge pour la mise à jour des composants du serveur

La section suivante fournit la mise à jour des composants du serveur pour CMC.

Le tableau suivant répertorie les versions de micrologiciel prises en charge pour les composants du serveur dans un scénario où la version du micrologiciel du CMC existante est 3.1 et les composants du serveur sont mis à jour depuis la version N-1 vers la version N.

REMARQUE : La mise à jour du micrologiciel des composants du serveur depuis la version N-1 vers la version N a réussi si le micrologiciel du CMC est de version 2.0 ou ultérieure, pour tous les serveurs de 12e, 13e et 14e génération mentionnés dans le tableau suivant.

Tableau 13. Versions des composants du serveur pris en charge pour la mise à jour des composants du serveur vers la version N

Plate-forme	Composant serveur	Composant de la version précédente (Version N-1)	Version des composants mis à jour (Version N)
M520	iDRAC	2.52.52.52	2.60.60.60
	Lifecycle Controller	2.52.52.52	2.60.60.60
	Diagnostics	4231A0	4247A1
	BIOS	2.4.2	2.6.1
	Carte NIC	19.2.0	20.00.00.13
M620	iDRAC	2.52.52.52	2.60.60.60
	Lifecycle Controller	2.52.52.52	2.60.60.60
	Diagnostics	4231A0	4247A1

Tableau 13. Versions des composants du serveur pris en charge pour la mise à jour des composants du serveur vers la version N (suite)

Plate-forme	Composant serveur	Composant de la version précédente (Version N-1)	Version des composants mis à jour (Version N)
	BIOS	2.5.4	2.6.1
M820	iDRAC	2.52.52.52	2.60.60.60
	Lifecycle Controller	2.52.52.52	2.60.60.60
	Diagnostics	4231A0	4247A1
	BIOS	2.6.1	2.6.1
M630	iDRAC	2.52.52.52	2.60.60.60
	Lifecycle Controller	2.52.52.52	2.60.60.60
	Diagnostics	4239.44	4239A36
	BIOS	2.6.0	2.7.1
M830	iDRAC	2.52.52.52	2.60.60.60
	Lifecycle Controller	2.52.52.52	2.60.60.60
	Diagnostics	4239.44	4239A36
	BIOS	2.5.4	2.7.1
M640	iDRAC	3.15.15.15	3.21.21.21
	Lifecycle Controller	3.15.15.15	3.21.21.21
	Diagnostics	4301A13	4301A13
	BIOS	1.3.7	1.4.8

Suppression de tâches planifiées de micrologiciel de composant de serveur

REMARQUE : Pour utiliser cette fonction, vous devez disposer d'une licence d'entreprise.

Vous pouvez supprimer les tâches planifiées pour les composants et/ou périphériques sélectionnés sur un ou plusieurs serveurs.

Suppression des tâches planifiées de micrologiciel des composants de serveur à l'aide de l'interface Web

Pour supprimer des tâches planifiées concernant le micrologiciel des composants de serveur :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** et sur **Mettre à jour**.
2. Sur la page **Mise à jour des composants du serveur**, filtrez le composant ou le périphérique (facultatif).
3. Dans la colonne **État de la tâche**, si une case à cocher apparaît en regard de l'état de la tâche, cela signifie qu'une tâche Lifecycle Controller est en cours et qu'elle a actuellement l'état indiqué. Vous pouvez la sélectionner pour l'opération de suppression de tâche.
4. Cliquez sur **Supprimer la tâche**. Les tâches sont supprimées des composants ou des périphériques sélectionnés.

Mise à jour des composants de stockage à l'aide de l'interface Web CMC

Vérifiez que vous avez téléchargé les DUP des composants de stockage appropriés.

Pour mettre à jour les composants de stockage :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Stockage** > **Mise à jour**.
2. Sur la page **Mise à jour des composants de stockage** , cliquez sur **Parcourir**.
   La boîte de dialogue **Choisir le fichier à charger** s'affiche
3. Naviguez vers l'emplacement où le fichier DUP requis fichier a été téléchargé et enregistré à partir du site de support Dell et sélectionnez le fichier DUP, puis cliquez sur **Ouvrir**.
   Le nom du fichier et le chemin d'accès du fichier DUP s'affichent dans le champ **Parcourir**.
4. Cliquez sur **Charger**.
   Le fichier DUP est téléchargé sur le CMC. La section **Mise à jour des composants de stockage** affiche uniquement les composants pris en charge par le fichier DUP téléchargé. La version actuelle, la dernière version disponible et la case à cocher **Mettre à jour** s'affichent pour les composants.
5. Sélectionnez les cases à cocher **Mettre à jour** appropriées pour les composants requis.
6. Cliquez sur **Mettre à jour**.
   L'action de mise à jour du firmware est lancée pour les composants sélectionnés. L'état de progression s'affiche dans la colonne **Mise à jour**.

   Lorsque l'action est terminée, un message approprié s'affiche pour indiquer la réalisation ou l'échec de la mise à jour du firmware.

REMARQUE :

- **Les serveurs doivent être mis hors tension avant de mettre à jour le firmware.**
- **Un composant met à jour d'autres composants correspondants du système de la même manière. Par exemple, les SPERC sont mis à jour de la même manière que les SPERC existants et les modules EMM sont mis à jour de la même manière que les modules EMM intégrés.**
- **Cliquez sur le + pour afficher le disque dur de différents boîtiers.**

5

Affichage des informations de châssis et surveillance de l'intégrité du châssis et des composants

Vous pouvez afficher des informations et surveiller l'intégrité des éléments suivants :

- CMC actifs et de secours
- Tous les serveurs, ou chaque serveur séparément
- Module d'ES
- Ventilateurs
- Unité d'alimentation (PSU)
- Capteurs de température
- Disques durs
- Ensemble d'écran LCD
- Contrôleurs de stockage
- Périphériques PCIe

REMARQUE : L'intégrité des composants externes a un impact sur l'intégrité générale du composant de stockage ainsi que sur celle du stockage existant et des composants de stockage intégrés dans VRTX. Cela indique que les composants externes n'ont aucune incidence sur l'intégrité de tout composant du châssis.

Sujets :

Affichage des récapitulatifs de châssis et de composants

Lorsque vous vous connectez à l'interface Web CMC, la page **Intégrité du châssis** affiche l'intégrité du châssis et de ses composants. Elle contient une vue graphique du châssis et de ses composants. Elle est mise à jour dynamiquement. Les superpositions des sous-graphiques des composants, ainsi que les infobulles sont automatiquement modifiées pour refléter l'état actuel.

Pour afficher l'intégrité du châssis, cliquez sur **Tour d'horizon du châssis**. Le système affiche le statut global de l'intégrité du châssis, les contrôleurs CMC actifs et en veille, les modules serveur, l'IO Module (IOM), les ventilateurs, les blocs d'alimentation électrique, l'ensemble LCD, le contrôleur de stockage et les périphériques PCIe. Des informations détaillées sur chaque composant s'affichent lorsque vous cliquez sur le composant. Les derniers événements du log de matériel CMC s'affichent également. Reportez-vous à *l'Aide en ligne* pour plus d'informations.

REMARQUE : Après un cycle d'alimentation du châssis ou une réinitialisation RAC, les alertes d'un lecteur physique, en état « hors ligne », sont supprimées.

Si votre châssis est configuré en tant que maître de groupe, la page **Intégrité du groupe** s'affiche après la connexion. Elle affiche les informations et les alertes au niveau du châssis. Toutes les alertes actives, critiques et non critiques sont affichées.

Graphiques du châssis

Le boîtier est représenté par les vues avant et arrière : respectivement, les images supérieure et inférieure. Les serveurs, les DVD, les disques durs, les KVM et l'écran LCD figurent dans la vue avant, les composants restants se trouvant dans la vue arrière. Une dominante de couleur bleue indique la sélection des composants. Pour la contrôler, cliquez sur l'image du composant requis. Lorsqu'un composant est présent dans le châssis, une icône de type de composant apparaît dans le graphique à l'emplacement (logement) où le composant a été installé. Les positions vides sont représentées par un fond gris anthracite. L'icône de composant indique l'état du composant. Les autres composants affichent des icônes qui représentent les composants physiques. Placez le pointeur de la souris sur un composant pour afficher une infobulle contenant des informations supplémentaires sur le composant.

Tableau 14. États d'icône de serveur dans les systèmes de 13e génération

Icon	Description
	Le serveur est présent, allumé et fonctionne normalement.
	Un serveur est présent, mais hors tension.
	Un serveur est présent, mais signale une erreur non critique.

Tableau 14. États d'icône de serveur dans les systèmes de 13e génération (suite)

Icon	Description
	Un serveur est présent, mais signale une erreur critique.
	Un serveur n'est pas présent.

Tableau 15. États d'icône de serveur dans les systèmes de 14e génération

Icon	Description
	Le serveur est présent, allumé et fonctionne normalement.
	Un serveur est présent, mais hors tension.
	Un serveur est présent, mais signale une erreur non critique.
	Un serveur est présent, mais signale une erreur critique.
	Aucun serveur n'est présent.

REMARQUE : Par défaut, les icônes d'état du serveur pour les systèmes Dell PowerEdge de 13e génération sont affichées si vous insérez un serveur PowerEdge 14e génération lorsque le châssis est hors tension.

Informations sur le composant sélectionné

Les informations pour le composant sélectionné sont affichées dans trois sections indépendantes :

- Intégrité, performances et propriétés : cette section affiche les événements actifs, critiques et non critiques, tels qu'ils figurent dans les journaux du matériel et contient les données de performances qui varient dans le temps.
- Propriétés : indique les propriétés de composant qui ne varient pas dans le temps ou qui changent rarement.
- Liens rapides : fournit des liens permettant d'accéder aux pages les plus fréquemment consultées, ainsi qu'aux actions les plus fréquemment exécutées. Seuls les liens applicables au composant sélectionné s'affichent dans cette section.

Le tableau suivant répertorie les propriétés et les informations des composants affichées sur la page **Intégrité du châssis** dans l'interface Web.

REMARQUE : Dans la gestion multichâssis (MCM), aucun des liens rapides associés aux serveurs ne s'affiche.

Tableau 16. Propriétés des composants

Composant	Propriétés d'intégrité et de performances	Propriétés	Liens rapides
Ensemble d'écran LCD	• Intégrité du panneau LCD • Intégrité du châssis	• Bouton d'alimentation du châssis • Verrouiller l'écran LCD du panneau de configuration • Langue de l'écran LCD • Orientation de l'écran LCD	Configuration du panneau avant
CMC actifs et de secours	• Mode de redondance • Adresse MAC • IPv4 • IPv6	• Micrologiciel • Micrologiciel : • Dernière mise à jour • Matériel	• État du CMC • Mise en réseau • Mise à jour du micrologiciel
Tous les serveurs et les serveurs individuels	• État de l'alimentation • Consommation énergétique • Intégrité • Alimentation allouée • Température	• Nom • Modèle • Numéro de service • Nom d'hôte • iDRAC • CPLD • BIOS • SE • Informations sur l'UC • Total de mémoire système	• État du serveur • Lancer la console distante • Lancer l'interface utilisateur d'iDRAC • Mettre le serveur hors tension • Arrêt normal • Partage de fichier à distance • Déployer le réseau iDRAC • Mise à jour des composants de serveur **REMARQUE : Les liens rapides pour la Mise hors tension et l'Arrêt normal d'un serveur s'affichent uniquement si l'état de l'alimentation du serveur est Sous tension. Si l'état de l'alimentation du serveur est Hors tension, le lien rapide de mise sous tension du serveur s'affiche.**
Logement KVM	Intégrité	• KVM mappé • Logement 1 : USB/Vidéo du panneau avant activé • Logement 2 : USB/Vidéo du panneau avant activé	Configuration du panneau avant

Tableau 16. Propriétés des composants (suite)

Composant	Propriétés d'intégrité et de performances	Propriétés	Liens rapides
		• Logement 3 : USB/Vidéo du panneau avant activé • Logement 4 : USB/Vidéo du panneau avant activé	
Logement DVD	• Intégrité • État de l'alimentation	• Lecteur de DVD mappé • Logement 1 : lecteur DVD activé • Logement 2 : lecteur DVD activé • Logement 3 : lecteur DVD activé • Logement 4 : lecteur DVD activé	Configuration du panneau avant
Logement de disque	• Intégrité • État	• Modèle • Numéro de série • État de l'alimentation • Version du micrologiciel • Taille • Type	• État des disques physiques • Configuration de disque physique • Afficher le contrôleur de ce disque physique • Afficher les disques virtuels pour ce disque physique
Unités de bloc d'alimentation	État de l'alimentation	Capacité	• Condition des blocs d'alimentation • Consommation énergétique • Bilan de puissance du système
Périphériques PCIe	• Installé • Attribué	• Modèle • Mappage des logements du serveur • Numéro/ID fournisseur) • ID de périphérique • Type de logement • Puissance allouée • Structure • État de l'alimentation	• État PCIe • Configuration PCIe
Ventilateurs	• Vitesse • PWM (% du max) • Décalage de ventilateur	• Seuil d'avertissement • Seuil critique	• Condition des ventilateurs • Configuration de ventilateur
Ventilateur	• Vitesse • PWM (% du max) • Mode de refroidissement optimisé	• Seuil d'avertissement • Seuil critique	• Condition des ventilateurs • Configuration de ventilateur
Logement SPERC	• Installé • Attribué	• Modèle • Mappage des logements du serveur • Numéro/ID fournisseur) • ID de périphérique • Type de logement • Puissance allouée • Structure • État de l'alimentation	• État du contrôleur • Configuration du contrôleur

Tableau 16. Propriétés des composants (suite)

Composant	Propriétés d'intégrité et de performances	Propriétés	Liens rapides
Logement de la carte Shared PERC 8 externe	• Installé • Attribué	• Modèle • Mappage des logements du serveur • Numéro/ID fournisseur) • ID de périphérique • Type de logement • Puissance allouée • Structure • État de l'alimentation	• Condition du logement PCIe • Configuration PCIe
Logement IOM	• État de l'alimentation • Rôle	• Modèle • Numéro de service	Condition du module d'E/S Lancer l'IUG du module d'E/S

Affichage du nom du modèle de serveur et du numéro de service

Vous pouvez afficher instantanément le nom du modèle et le numéro de service de chaque serveur en procédant comme suit :

1. Dans le volet de gauche, sous le nœud d'arborescence **Présentation des serveurs**, tous les serveurs (de SLOT-01 à SLOT-04) s'affichent dans la liste de serveurs. Si un serveur ne figure pas dans un logement, l'image correspondante dans l'illustration est grisée. Lorsqu'un serveur de hauteur standard est présent dans les logements 1 et 3, le logement 3 affiche le nom du logement comme **extension de 1**.
2. Placez le pointeur de la souris sur le nom de logement ou le numéro de logement d'un serveur ; une infobulle contenant le nom de modèle et le numéro de service (si disponible) du serveur s'affiche.

Affichage du résumé du châssis

Pour afficher le résumé du châssis, cliquez sur **Présentation du châssis** > **Propriétés** > **Résumé** dans le volet de gauche.
La page **Résumé du châssis** s'affiche. Pour plus d'informations, voir l'*Aide en ligne*.

Affichage des informations et de la condition du contrôleur de châssis

Pour afficher les informations et l'état du contrôleur de châssis, dans l'interface Web CMC, cliquez sur **Présentation du châssis** > **Contrôleur de châssis**.
La page **État du contrôleur de châssis** s'affiche. Pour plus d'informations, voir l'*Aide en ligne*.

Affichage des informations et de la condition d'intégrité de tous les serveurs

Pour afficher la condition d'intégrité de tous les serveurs, effectuez l'une des opérations suivantes :

- Cliquez sur **Présentation du châssis**. La page **Intégrité du châssis** affiche la vue d'ensemble graphique de tous les serveurs installés dans le châssis. La condition d'intégrité du serveur est indiquée par le sous-graphique de serveur. Pour plus d'informations, voir l'*Aide en ligne*.
- Cliquez sur **Présentation du châssis** > **Présentation du serveur**. La page **Condition des serveurs** présente les serveurs dans le châssis. Pour plus d'informations, voir l'*Aide en ligne*.

Affichage de la condition d'intégrité et des informations de chaque serveur

Pour afficher la condition d'intégrité de chaque serveur, effectuez l'une des opérations suivantes :

1. Accédez à **Présentation du châssis** > **Propriétés** > **Intégrité**.
   La page **Intégrité du châssis** affiche une présentation graphique de tous les serveurs installés dans le châssis. L'état d'intégrité du serveur est indiqué par superposition d'une couche sur le sous-graphique de serveur. Déplacez la souris pour pointer sur chaque sous-graphique de serveur. Le texte ou l'info-bulle qui correspond fournit des informations supplémentaires sur ce serveur. Cliquez sur le sous-graphique de serveur pour afficher, à droite, les informations sur le module d'E/S. Pour plus d'informations, voir l'*Aide en ligne*.
2. Accédez à **Présentation du châssis** et développez l'entrée **Présentation du serveur** dans le volet gauche. Tous les serveurs (1 à 4) s'affichent dans la liste étendue. Cliquez sur le serveur (logement) à afficher.
   La page **Condition du serveur** (à ne pas confondre avec la page **Condition des serveurs**) indique l'état d'intégrité du serveur dans le châssis et permet de lancer l'interface Web iDRAC, micrologiciel utilisé pour gérer le serveur. Pour plus d'informations, voir l'*Aide en ligne*.

   REMARQUE : Pour utiliser l'interface Web iDRAC, vous devez disposer d'un nom d'utilisateur et d'un mot de passe iDRAC. Pour plus d'informations sur iDRAC et sur l'utilisation de l'interface Web iDRAC, voir le manuel *Integrated Dell Remote Access Controller User's Guide* (Guide d'utilisation d'Integrated Dell Remote Access Controller (iDRAC)).

Affichage des informations et de la condition d'intégrité du module IOM

Pour afficher la condition d'intégrité des modules d'E/S (IOM), effectuez l'une des opérations suivantes dans l'interface Web CMC :

1. Cliquez sur **Présentation du châssis**.
   La page **Intégrité du châssis** s'affiche. Le graphique dans le volet de gauche affiche les vues arrière, avant et latérale du châssis et contient la condition d'intégrité du module IOM. Cette condition est indiquée par le masque du sous-graphique de module IOM. Placez le pointeur de la souris sur le sous-graphique IOM. L'info-bulle fournit des informations supplémentaires sur l'IOM. Cliquez sur le sous-graphique IOM pour afficher les informations de l'IOM dans le volet de droite.
2. Accédez à **Présentation du châssis** > **Présentation du module d'E/S**.
   La page **État du module d'E/S** affiche la vue d'ensemble de l'IOM associé au châssis. Pour plus d'informations, voir l'*Aide en ligne*.

REMARQUE : Après la mise à jour ou le redémarrage du module IOM/IOA, assurez-vous que le système d'exploitation de l'IOM/IOA est également amorcé correctement. Sinon, l'état du module IOM s'affiche en tant que « Hors ligne ».

Affichage des informations et de la condition d'intégrité des ventilateurs

Le contrôleur CMC contrôle la vitesse du ventilateur du châssis en augmentant ou diminuant la vitesse du ventilateur en fonction des événements système. Le ventilateur peut fonctionner dans trois modes : Faible, Moyen et Élevé. Pour en savoir plus sur la configuration d'un ventilateur, consultez l'*Aide en ligne*.

Pour définir les propriétés des ventilateurs en utilisant les commandes RACADM, entrez la commande suivante dans l'interface CLI.

```
racadm fanoffset [-s <off|low|medium|high>]
```

Pour plus d'informations sur les commandes RACADM, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX* sur le site **dell.com/cmcmanuals**.

REMARQUE : Le contrôleur CMC surveille les capteurs de température du châssis et ajuste automatiquement la vitesse du ventilateur. Vous pouvez cependant ignorer ces ajustements pour maintenir une vitesse de ventilateur minimale à l'aide de la commande racadm fanoffset. Si vous utilisez cette commande pour contourner les réglages, le CMC fera systématiquement fonctionner le ventilateur à la vitesse sélectionnée, même si le châssis n'a pas besoin de cette vitesse de ventilateur.

Le contrôleur CMC génère une alerte et augmente les vitesses des ventilateurs lorsque les événements suivants se produisent :

- Le seuil de température ambiante de CMC est dépassé.
- Un ventilateur ne fonctionne plus.
- Un ventilateur est retiré du châssis.

REMARQUE : Pendant les mises à jour du firmware CMC ou iDRAC sur un serveur, certains ou tous les ventilateurs du châssis tournent à 100 %. Ce phénomène est normal.

Pour afficher la condition d'intégrité des ventilateurs, effectuez l'une des opérations suivantes dans l'interface Web CMC :

1. Accédez à **Présentation du châssis**.
   La page **Intégrité du châssis** s'affiche. La partie inférieure de la représentation graphique du châssis présente la vue de gauche du châssis et indique l'état d'intégrité des ventilateurs. L'état d'intégrité du ventilateur est indiqué par la superposition du sous-graphique du ventilateur. Déplacez le curseur sur le sous-graphique du ventilateur. Le texte d'astuce fournit des informations supplémentaires sur un ventilateur. Cliquez sur le sous-graphique du ventilateur pour afficher des informations sur les ventilateurs dans le volet de droite.
2. Accédez à **Présentation du châssis** > **Ventilateurs**.
   La page **État des ventilateurs** indique l'état, les mesures de vitesse (en tours par minute, ou tr/min) et les valeurs seuils des ventilateurs du châssis. Il peut y avoir un ou plusieurs ventilateurs.

   REMARQUE : En cas de perte des communications entre le contrôleur CMC et un ventilateur, le contrôleur CMC ne peut pas obtenir ni afficher sa condition d'intégrité.

   REMARQUE : Le message suivant s'affiche lorsque les deux ventilateurs sont absents des logements ou qu'un ventilateur est lent :

   ```
   Fan <number> is less than the lower critical threshold.
   ```

   Reportez-vous à *l'Aide en ligne* pour plus d'informations.

Configuration des ventilateurs

Compensation/Décalage de ventilation permet d'augmenter le refroidissement des zones de stockage et PCIe du châssis. Cette fonction permet d'accroître le flux d'air vers les disques durs, les contrôleurs PERC Shared et les logements de cartes PCIe. Par exemple, vous pouvez utiliser la fonction lorsque vous utilisez des cartes PCIe haute puissance ou personnalisées qui nécessitent une ventilation accrue. La fonction dispose des options Désactivé, Bas, Moyen et haut. Ces paramètres correspondent à une compensation de vitesse de ventilation (augmentation) de 20 %, 50 % et 100 % de la vitesse maximale. Il existe également des vitesses minimales pour chaque option, à savoir 35 % pour Bas, 65 % pour Moyen et 100 % pour Haut.

Si, par exemple, vous utilisez la compensation moyenne, vous augmentez la vitesse des ventilateurs 1–6 de 50 % de la vitesse maximale. L'augmentation est supérieure à la vitesse définie par le système pour refroidir en fonction de la configuration matérielle installée.

Lorsque les options de compensation de ventilation sont activées, la consommation électrique augmente. Le système devient plus bruillant avec la compensation Basse, nettement plus bruillant avec la compensation Moyenne et beaucoup plus bruillant avec la compensation haute. Lorsque l'option de compensation de ventilation n'est pas activée, les vitesses de ventilation sont ramenées aux vitesses par défaut de refroidissement du système de la configuration matérielle installée.

Pour définir la fonction de décalage, accédez à **Présentation du châssis** > **Ventilateurs** > **Configuration**. Sur la page **Configurations de ventilation avancées**, dans le tableau **Configuration du ventilateur**, à partir du menu déroulant **Valeur** correspondant à la **Compensation du ventilateur**, sélectionnez une option de manière appropriée.

Pour plus d'informations sur la fonction de compensation de ventilation, voir l'*Aide en ligne*.

Pour définir ces fonctions en utilisant les commandes RACADM, utilisez la commande suivante :

```
racadm fanoffset [-s <off|low|medium|high>]
```

Pour plus d'informations sur les commandes RACADM associées à la compensation de ventilation, voir le document *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX) sur le site dell.com/support/Manuals.

Mode de refroidissement avancé (ECM) : il s'agit d'une fonction du contrôleur CMC qui permet d'augmenter la capacité de refroidissement des serveurs installés dans le châssis PowerEdge VRTX. Vous pouvez utiliser ce mode, par exemple, dans un environnement ambiant ou lorsque vous utilisez des serveurs avec des UC de haute puissance (≥120 W). L'augmentation de la capacité de refroidissement est obtenue en permettant aux modules de ventilation du châssis de fonctionner plus rapidement. Par conséquent, la consommation électrique du système et le niveau de bruit peuvent augmenter lorsque le mode ECM est activé.

Lorsqu'il est activé, le mode ECM augmente uniquement la capacité de refroidissement vers les logements des serveurs dans le châssis. Notez aussi qu'ECM n'est pas conçu pour fournir un refroidissement élevé aux serveurs en permanence. Même lorsqu'ECM est activé, les

vitesses de ventilation élevées ne sont utilisées que lorsqu'un refroidissement élevé est exigé, par exemple lors d'une utilisation ou d'un stress élevé du serveur et de températures ambiantes élevées.

ECM est désactivé par défaut. Lorsque le mode est activé, les ventilateurs peuvent augmenter le flux d'air de 20 % environ par lame.

Pour définir le mode de gestion de contenu d'entreprise ECM, accédez à la page **Présentation du châssis** > **Ventilateurs** > **Configuration**. Sur la page **Configurations de ventilation avancées** , dans le tableau **Configuration de ventilateur**, à partir du menu déroulant **Valeur** correspondant au **Mode de refroidissement optimisé**, sélectionnez une option de manière appropriée.

Pour plus d'informations sur le mode ECM, voir l'*Aide en ligne*.

Affichage des propriétés du panneau avant

Pour afficher les propriétés du panneau avant :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Panneau avant**.
2. Les informations suivantes figurent sur la page **Propriétés** :
   - **Propriétés du bouton d'alimentation**
   - **Propriétés du panneau LCD**
   - **Propriétés du KVM**
   - **Propriétés du lecteur de DVD**

Affichage des informations et de l'état d'intégrité KVM

Pour afficher l'état d'intégrité des consoles KVM associées au châssis, effectuez l'une des opérations suivantes :

1. Cliquez sur **Présentation du châssis**.
   La page **Intégrité du châssis** s'affiche. Le volet de gauche contient la vue avant du châssis et l'état d'intégrité d'une console KVM. Cet état est indiqué par le sous-graphique KVM. Placez le pointeur de la souris sur un sous-graphique KVM pour afficher une info-bulle qui fournit des informations supplémentaires sur la console KVM. Cliquez sur le sous-graphique KVM pour afficher les informations KVM dans le volet de droite.
2. Vous pouvez également cliquer sur **Présentation du châssis** > **Panneau avant**.
   Sur la page **État**, sous **Propriétés KVM**, vous pouvez afficher l'état et les propriétés d'une console KVM associée à un châssis. Pour plus d'informations, voir l'*Aide en ligne*.

Affichage des informations et de l'intégrité de l'écran LCD

Pour afficher l'état d'intégrité d'un écran LCD :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis**.
   La page **Intégrité du châssis** s'affiche. Le volet de gauche contient la vue avant du châssis. L'état d'intégrité de l'écran LCD est indiqué par le sous-graphique LCD.
2. Pointez sur le sous-graphique LCD avec la souris. L'écran de texte ou l'info-bulle qui correspond fournit des informations supplémentaires sur l'écran LCD.
3. Cliquez sur le sous-graphique LCD pour afficher les informations LCD dans le volet de droite. Pour plus d'informations, voir l'*Aide en ligne*.

   Vous pouvez également accéder à **Présentation du châssis** > **Panneau avant** > **Propriétés** > **État**. Sur la page **État**, sous **Propriétés LCD**, vous pouvez identifier l'état de l'écran LCD du châssis. Pour plus d'informations, voir l'*Aide en ligne*.

Affichage des informations et de la condition d'intégrité des capteurs de température

Pour afficher la condition d'intégrité des capteurs de température :

Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Capteurs de température**.

La page **Condition des capteurs de température** affiche l'état et les mesures des capteurs de température de l'ensemble du châssis (châssis et serveurs). Pour plus d'informations, voir l'*Aide en ligne*.

REMARQUE : La valeur des capteurs de température n'est pas modifiable. Tout changement au-delà du seuil génère une alerte provoquant la modification de la vitesse des ventilateurs. Par exemple, si le capteur de température ambiante du contrôleur CMC dépasse le seuil, la vitesse des ventilateurs du châssis augmente.

Affichage de la capacité de stockage et de l'état des composants de stockage

Pour afficher la capacité et l'état de tolérance aux pannes des composants de stockage, effectuez l'une des opérations suivantes :

1. Accédez à **Présentation du châssis**.
   La page **Intégrité du châssis** s'affiche. Des informations détaillées sur la capacité de stockage, le mode de tolérance des pannes (actif/passif) et l'état de tolérance des pannes (Activé) s'affichent dans le volet droit. Ces informations de tolérance des pannes s'affichent uniquement si la fonctionnalité de tolérance des pannes est activée pour les composants de stockage.

   La section inférieure des graphiques du châssis fournit une vue de la gauche du châssis. Déplacez le curseur sur le sous-graphique du composant de stockage. Le champ textuel fournit des informations supplémentaires sur le composant de stockage. Cliquez sur le sous-graphique du composant de stockage pour consulter les informations associées dans le volet de droite.
2. Dans le volet de gauche, vous pouvez également cliquer sur **Présentation du châssis** > **Stockage** > **Propriétés** > **État**.
   La page **Présentation du stockage** qui s'affiche présente les informations suivantes :
   - Afficher le résumé graphique des disques physiques installés dans le châssis et leur état.
   - Afficher le résumé de tous les composants de stockage avec des liens vers leurs pages respectives.
   - Afficher la capacité utilisée et la capacité totale du stockage.
   - Afficher les informations de contrôleur

     REMARQUE : Dans le cas d'un contrôleur à tolérance des pannes, le format de nom est : Shared *PERC numéro*> (Integrated <numéro>). Par exemple, le contrôleur actif est Shared PERC8 (Integrated 1) et le contrôleur homologue est Shared PERC8 (Integrated 2).
   - Afficher les événements de stockage récemment journalisés

   REMARQUE : Reportez-vous à *l'Aide en ligne* pour plus d'informations.

6

Configuration de CMC

Le Chassis Management Controller (Contrôleur de gestion du châssis) permet de définir les propriétés, les utilisateurs et les alertes pour exécuter des tâches de gestion à distance.

Avant de configurer le contrôleur CMC, vous devez définir les paramètres réseau CMC afin de pouvoir gérer le contrôleur CMC à distance. Cette configuration initiale définit les paramètres de mise en réseau TCP/IP qui permettent d'accéder au contrôleur CMC. Pour plus d'informations, voir Configuration de l'accès initial au contrôleur CMC.

Vous pouvez configurer CMC dans l'interface Web ou avec RACADM.

REMARQUE : Lorsque vous configurez CMC pour la première fois, vous devez vous connecter en tant qu'utilisateur root pour exécuter les commandes RACADM sur un système distant. Vous pouvez aussi créer un autre utilisateur avec des privilèges de configuration de CMC.

Une fois le controleur CMC configuré et après avoir effectué la configuration de base, vous pouvez exécuter les opérations suivantes :

- Modifier les paramètres réseau, si nécessaire.
- Définissez les interfaces d'accès à CMC.
- Configurer l'écran LCD.
- Configurer des groupes de châssis, si nécessaire.
- Configurer les serveurs, le module d'E/S ou le panneau de commande.
- Définir les paramètres VLAN.
- Obtenez les certificats nécessaires.
- Ajoutez et configurez des utilisateurs CMC avec les privilèges voulus.
- Configurer et activer des alertes par e-mail et par interruption SNMP.
- Définir la politique de limitation d'alimentation, si nécessaire.

REMARQUE : Vous ne pouvez pas utiliser les caractères suivants dans les chaînes de propriété des deux interfaces CMC (graphiques et CLI) :

- **&#**
- **< et > ensemble**
- **; (point-virgule)**

Sujets :

Affichage et modification des paramètres réseau (LAN) CMC

Les paramètres LAN, comme la chaîne de communauté et l'adresse IP du serveur SMTP, affectent CMC et les paramètres externes du châssis.

Si le châssis contient deux contrôleurs CMC (actif et de secours) connectés au réseau, le contrôleur CMC de secours acquiert automatiquement les paramètres réseau du contrôleur CMC actif en cas de basculement.

Si le protocole IPv6 est activé lors de l'amorçage, trois sollicitations de routage sont envoyées toutes les quatre secondes. Si les commutateurs de réseau externes exécutent STP (Spanning Tree Protocol), les ports des commutateurs externes peuvent être bloqués pendant plus de 12 secondes, au cours desquelles les sollicitations de routage IPv6 sont envoyées. Dans ce cas, il peut exister une période où la connectivité IPv6 est limitée, jusqu'à ce que les annonces de routeur soient envoyées gratuitement par les routeurs IPv6.

REMARQUE : Si vous modifiez les paramètres réseau CMC, vous risquez de couper la connexion réseau en cours.

REMARQUE : Vous devez disposer de privilèges d'Administrateur de configuration du châssis pour configurer les paramètres réseau CMC.

Affichage et modification des paramètres réseau (LAN) CMC dans l'interface Web CMC

Pour afficher et modifier les paramètres réseau LAN CMC dans l'interface Web CMC :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** et sur **Réseau**. La page **Configuration du réseau** affiche les paramètres réseau actuels.
2. Modifiez les paramètres généraux IPv4 ou IPv6 de manière appropriée. Pour plus d'informations, voir l'*Aide en ligne*.
3. Cliquez sur **Appliquer les changements** dans chaque section afin d'appliquer les paramètres.

Affichage et modification des paramètres réseau (LAN) CMC à l'aide de RACADM

Pour afficher les paramètres IPv4, utilisez les objets du groupe **cfgCurrentLanNetworking** avec les sous-commandes suivantes `getconfig` et `getniccfg`.

Pour afficher les paramètres IPv6, utilisez les objets du groupe **cfgIpv6LanNetworking** avec la sous-commande `getconfig` .

Pour afficher les informations d'adresses IPv4 et IPv6 du châssis, utilisez la sous-commande `getsysinfo`.

Pour plus d'informations sur les sous-commandes et les objets, voir le document *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX).

Activation de l'interface réseau CMC

Pour activer ou désactiver l'interface réseau CMC pour IPv4 et IPv6, entrez :

```
racadm config -g cfgLanNetworking -o cfgNicEnable 1
racadm config -g cfgLanNetworking -o cfgNicEnable 0
```

REMARQUE : La NIC de CMC est activée par défaut.

Pour activer ou désactiver l'adressage IPv4 CMC, entrez :

```
racadm config -g cfgLanNetworking -o cfgNicIPv4Enable
1
racadm config -g cfgLanNetworking -o cfgNicIPv4Enable
0
```

REMARQUE : L'adressage IPv4 de CMC est activé par défaut.

Pour activer ou désactiver l'adressage IPv6 CMC, entrez :

```
racadm config -g cfgIpv6LanNetworking -o cfgIPv6Enable
1
racadm config -g cfgIpv6LanNetworking -o cfgIPv6Enable
0
```

REMARQUE : Notez les points suivants :

- **Il y a un délai de 30 secondes entre la modification d'un paramètre de réseau et son application.**
- **L'adressage IPv6 de CMC est désactivé par défaut.**

Par défaut, pour IPv4, le contrôleur CMC demande et obtient automatiquement une adresse IP CMC du serveur DHCP (Dynamic Host Configuration Protocol). Vous pouvez désactiver la fonction DHCP et spécifier une adresse IP CMC statique, une passerelle et un masque de sous-réseau.

Dans le cas d'un réseau iPv4, pour désactiver DHCP et préciser l'adresse IP statique de CMC, la passerelle et le masque de sous-réseau, entrez :

```
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0
racadm config -g cfgLanNetworking -o cfgNicIpAddress <static IP address>
racadm config -g cfgLanNetworking -o cfgNicGateway <static gateway>
racadm config -g cfgLanNetworking -o cfgNicNetmask <static subnet mask>
```

Par défaut, pour IPv6, CMC demande et obtient automatiquement une adresse IP CMC auprès du mécanisme de configuration automatique IPv6.

Dans le cas d'un réseau IPv6, pour désactiver la fonctionnalité Configuration automatique et spécifier une adresse IPv6 CMC statique, une passerelle et une longueur de préfixe, entrez :

```
racadm config -g cfgIPv6LanNetworking -o
cfgIPv6AutoConfig 0
racadm config -g cfgIPv6LanNetworking -o
cfgIPv6Address <IPv6 address>
racadm config -g cfgIPv6LanNetworking -o
cfgIPv6PrefixLength 64
racadm config -g cfgIPv6LanNetworking -o
cfgIPv6Gateway <IPv6 address>
```

Activation ou désactivation de DHCP pour l'adresse d'interface réseau CMC

Lorsqu'elle est activée, la fonctionnalité DHCP d'adresse de carte réseau (NIC) de CMC demande et obtient automatiquement une adresse IP auprès du serveur DHCP (Dynamic Host Configuration Protocol - Protocole de configuration dynamique des hôtes). Cette fonction est activée par défaut.

Vous pouvez désactiver la fonction DHCP d'adresse NIC, et spécifier une adresse IP statique, un masque de sous-réseau et une passerelle. Pour plus d'informations, voir « Configuration de l'accès initial à CMC ».

Activation ou désactivation de la fonction DHCP pour les adresses IP DNS

Par défaut, la fonction DHCP d'adresse DNS du CMC est désactivée. Lorsque vous l'activez, cette fonction permet d'obtenir l'adresse des serveurs DNS principal et secondaire depuis le serveur DHCP. Lorsque vous utilisez cette fonction, vous n'avez pas besoin de configurer les adresses IP statiques des serveurs DNS.

Pour désactiver la fonction d'adresse DHCP pour DNS et spécifier les adresses préférées et alternatives du serveur DNS, entrez :

```
racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0
```

Pour désactiver la fonction d'adresse DHCP pour DNS pour iPv6 et spécifier les adresses préférées et alternatives du serveur DNS, entrez :

```
racadm config -g cfgIPv6LanNetworking -o cfgIPv6DNSServersFromDHCP6 0
```

Définition des adresses IP statiques du DNS

REMARQUE : Les paramètres des adresses IP statiques DNS ne sont pas valides tant que la fonction DHCP d'adresse DNS est désactivée.

Pour IPv4, pour définir les adresses IP préférées principale et secondaire du serveur DNS, entrez :

```
racadm config -g cfgLanNetworking -o cfgDNSServer1 <adresse IP> racadm config -g
cfgLanNetworking -o cfgDNSServer2 <adresse IPv4>
```

Pour IPv6, pour définir les adresses IP préférée et secondaire des serveurs DNS, entrez :

```
racadm config -g cfgIPv6LanNetworking -o cfgIPv6DNSServer1 <adresse IPv6> racadm config -g
cfgIPv6LanNetworking -o cfgIPv6DNSServer2 <adresse IPv6>
```

Configuration des paramètres DNS IPv4 et IPv6

- **Enregistrement de CMC** : pour enregistrer CMC sur le serveur DNS, entrez :

  ```
  racadm config -g cfgLanNetworking -o
  cfgDNSRegisterRac 1
  ```

  REMARQUE : Certains serveurs DNS n'enregistrent que les noms comportant 31 caractères ou moins. Assurez-vous que le nom désigné se trouve dans la limite requise par le DNS.

  REMARQUE : les paramètres suivants ne sont valides que si vous avez enregistré CMC sur le serveur DNS en définissant la variable cfgDNSRegisterRac sur la valeur 1.

- **CMC Name (Nom CMC)** : le nom par défaut du module CMC sur le serveur DNS est cmc-<*numéro de série*>. Pour modifier le nom du CMC sur le serveur DNS, entrez :

  ```
  racadm config -g cfgLanNetworking -o cfgDNSRacName <name>
  ```

  où <*name*> est une chaîne contenant au maximum 63 caractères alphanumériques et tirets. Par exemple : cmc-1, d-345.

  REMARQUE : Si un nom de domaine DNS n'est pas spécifié, le nombre maximum de caractères est 63. Si un nom de domaine est spécifié, le nombre de caractères dans le nom du CMC auquel s'ajoute le nombre de caractères du nom de domaine DNS doit être inférieur ou égal à 63 caractères.

- **DNS Domain Name (Nom de domaine DNS)** : le nom de domaine DNS par défaut est une espace unique. Pour définir un nom de domaine DNS, entrez :

  ```
  racadm config -g cfgLanNetworking -o
  cfgDNSDomainName <name>
  ```

  où <*name*> est une chaîne contenant au maximum 254 caractères alphanumériques et tirets. Par exemple : p45, a-tz-1, r-id-001.

Configuration de la négociation automatique, du mode duplex et de la vitesse réseau pour IPv4 et IPv6

Lorsqu'elle est activée, la fonctionnalité de négociation automatique détermine si le CMC définit automatiquement le mode duplex et la vitesse réseau en communiquant avec le routeur ou le commutateur le plus proche. La fonction de négociation automatique est activée par défaut.

Vous pouvez désactiver la négociation automatique et préciser le mode duplex et la vitesse réseau en tapant :

```
racadm config -g cfgNetTuning -o cfgNetTuningNicAutoneg 0
racadm config -g cfgNetTuning -o cfgNetTuningNicFullDuplex <duplex mode>
```

où :

<*duplex mode*> est égal à 0 (semi duplex) ou 1 (duplex total, valeur par défaut)

```
racadm config -g cfgNetTuning -o cfgNetTuningNicSpeed <speed>
```

où :

<*speed*> est égal à 10 ou 100 (valeur par défaut).

Configuration de l'unité de transmission maximale pour IPv4 et IPv6

La propriété de l'unité de transmission maximale (MTU, Maximum Transmission Unit) vous permet de définir une limite supérieure de taille pour les paquets pouvant être transmis via l'interface. Pour définir la valeur MTU, entrez :

```
racadm config -g cfgNetTuning -o cfgNetTuningMtu <mtu>
```

où <*mtu*> est une valeur comprise entre 576 et 1 500 (inclus). La valeur par défaut est 1 500.

REMARQUE : IPv6 nécessite une valeur MTU minimale de 1 280. Si IPv6 est activé et si `cfgNetTuningMtu` est défini sur une valeur plus faible, le CMC utilise la valeur MTU de 1 280.

Configuration des paramètres de réseau et de sécurité de connexion CMC

Les fonctions de blocage de l'adresse IP et de l'utilisateur dans le CMC vous permettent de prévenir les problèmes de sécurité dus aux tentatives visant à deviner le mot de passe. Cette fonction vous permet de bloquer une plage d'adresses IP et d'utilisateurs pouvant accéder au CMC. Par défaut, la fonction de blocage des adresses IP est activée dans le CMC. Vous pouvez définir les attributs de la plage IP à l'aide de l'interface Web CMC ou de RACADM. Pour utiliser les fonctions de blocage des adresses IP et des utilisateurs, activez les options à l'aide de l'interface Web CMC ou de RACADM. Configurez les paramètres de la stratégie de verrouillage de la connexion pour définir le nombre d'échecs de tentatives de connexion pour un utilisateur particulier ou une adresse IP. Une fois la limite atteinte, l'utilisateur bloqué ne pourra se connecter qu'à la fin de la période de pénalité.

REMARQUE : Le blocage via les adresses IP s'applique uniquement pour les adresses IPV4.

Configuration des attributs de la plage IP à l'aide de l'interface Web CMC

REMARQUE : Pour effectuer les étapes suivantes, vous devez disposer du privilège d' Administrateur de configuration du châssis.

Pour configurer les attributs de la plage IP à l'aide de l'interface Web CMC :

1. Dans le volet gauche, accédez à la section **Présentation du châssis**, puis cliquez sur **Réseau** > **Réseau**. La page **Configuration réseau** s'affiche.
2. Dans la section Paramètres IPv4, cliquez sur **Paramètres avancés**.
   La page **Sécurité de connexion** s'affiche.

   Autrement, pour accéder à la page Sécurité de connexion, dans le volet gauche, accédez à **Présentation du châssis**, cliquez sur **Sécurité** > **Connexion**.
3. Pour activer la fonction de vérification de la plage IP, dans la section **Plage IP** section, sélectionnez l'option **Plage IP activée**.
   Les champs **Plage d'adresses IP** et **Masque de plage IP** sont activés.
4. Dans les champs **Plage d'adresses IP** et **Masque de plage IP** , entrez la plage d'adresses IP et les masques de plage IP pour lesquels vous souhaitez bloquer l'accès au CMC.

   Pour en plus d'informations, voir l'*Aide en ligne*.
5. Cliquez sur **Appliquer** pour enregistrer vos paramètres.

Configuration des attributs de la plage d'adresses IP à l'aide de RACADM

Vous pouvez configurer les attributs de la plage d'adresses IP suivantes pour CMC à l'aide de RACADM :

- Fonction de vérification de la plage d'adresses IP
- La plage d'adresses IP pour lesquelles vous voulez bloquer l'accès au CMC
- Le masque de la plage d'adresses IP pour lesquelles vous voulez bloquer l'accès au CMC

Le filtrage d'adresses IP compare les adresses IP d'une connexion entrante à la plage d'adresses IP spécifiée. Une connexion depuis une adresse IP entrante est autorisée uniquement si les deux propriétés suivantes sont identiques :

- **cfgRacTuneIpRangeMask** au niveau du bit et avec une adresse IP entrante
- **cfgRacTuneIpRangeMask** au niveau du bit et avec **cfgRacTuneIpRangeAddr**
- Pour activer la fonction de vérification de plage d'adresses IP, utilisez la propriété suivante sous le groupe `cfgRacTuning` :

  ```
  cfgRacTuneIpRangeEnable <0/1>
  ```

- Pour spécifier la plage d'adresses IP pour lesquelles vous souhaitez bloquer l'accès au CMC, utilisez la propriété suivante sous le groupe `cfgRacTuning` :

  ```
  cfgRacTuneIpRangeAddr
  ```

- Pour spécifier le masque de la plage d'adresses IP pour lesquelles vous souhaitez bloquer l'accès au CMC, utilisez la propriété suivante sous le groupe `cfgRacTuning` :

  ```
  cfgRacTuneIpRangeMask
  ```

Configuration des propriétés de balise VLAN pour le contrôleur CMC

Virtual LANfunctionality permet à plusieurs VLAN de coexister sur le même câble réseau physique et de diviser le trafic réseau à des fins de sécurité ou de gestion de la charge. Lorsque vous activez la fonctionnalité VLAN, chaque paquet réseau reçoit un numéro VLAN.

Configuration des propriétés de balisage VLAN pour CMC avec RACADM

1. Activez les fonctions VLAN du réseau de gestion du châssis externe :

   ```
   racadm config -g cfgLanNetworking -o cfgNicVLanEnable 1
   ```

2. Spécifiez le N° VLAN pour le réseau de gestion du châssis externe :

   ```
   racadm config -g cfgLanNetworking -o cfgNicVlanID <VLAN id>
   ```

   Les valeurs valides de <*VLAN id*> sont comprises entre 1 et 4 000, et entre 4 021 et 4 094. La valeur par défaut est 1.

   Par exemple :

   ```
   racadm config -g cfgLanNetworking -o cfgNicVlanID 1
   ```

3. Spécifiez ensuite la priorité VLAN du réseau de gestion du châssis externe :

   ```
   racadm config -g cfgLanNetworking -o cfgNicVLanPriority <VLAN priority>
   ```

   Les valeurs valides de <*VLAN priority*> sont comprises entre 0 et 7. La valeur par défaut est 0.

Par exemple :

```
racadm config -g cfgLanNetworking -o cfgNicVLanPriority 7
```

Vous pouvez également spécifier l'ID du VLAN et la priorité VLAN avec une seule commande :

```
racadm setniccfg -v <ID VLAN> <priorité VLAN>
```

Par exemple :

```
racadm setniccfg -v 1 7
```

4. Pour supprimer le VLAN de CMC, désactivez les fonctions VLAN du réseau de gestion du châssis externe :

```
racadm config -g cfgLanNetworking -o cfgNicVLanEnable 0
```

Vous pouvez également supprimer le VLAN de CMC en utilisant la commande suivante :

```
racadm setniccfg -v
```

Configuration des propriétés de balise VLAN virtuel pour le contrôleur CMC à l'aide de l'interface Web

Pour configurer le VLAN CMC avec l'interface Web CMC :

1. Accédez à l'une des pages suivantes :
   - Dans le volet de gauche, cliquez sur **Présentation du châssis** et sur **Réseau** > **VLAN**.
   - Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Présentation du serveur** et sur**Réseau** > **VLAN**.

   La page **Paramètres de balise VLAN** s'affiche. Les balises VLAN sont des propriétés de châssis. Elles demeurent associées au châssis même lorsque vous retirez un composant.
2. Dans la section **CMC**, activez le VLAN pour le contrôleur CMC, définissez la priorité et affectez l'ID approprié. Pour plus d'informations sur les champs, voir l'*Aide en ligne*.
3. Cliquez sur **Appliquer**. Les paramètres de balise VLAN sont enregistrés.

   Vous pouvez également accéder à cette page depuis **Présentation du châssis** > **Serveurs** > **Configurer** > **VLAN**.

Standards FIPS (Federal Information Processing Standards)

Les agences et les sous-traitants du gouvernement fédéral des États-Unis utilisent les normes de sécurité informatique FIPS (Federal Information Processing Standards), qui concernent toutes les applications dotées d'interfaces de communication. La norme 140-2 se compose de quatre niveaux : Niveau 1, Niveau 2, Niveau 3 et Niveau 4. La série de normes FIPS 140-2 stipule que toutes les interfaces de communication doivent disposer des propriétés de sécurité suivantes :

- authentification
- confidentialité
- intégrité du message
- non-répudiation
- disponibilité
- contrôle d'accès

Si l'une des propriétés dépend d'algorithmes cryptographiques, les FIPS doivent approuver ces algorithmes.

Par défaut, le mode FIPS est désactivé. Lorsque FIPS est activé, la taille de clé minimum pour OpenSSL FIPS est SSH-2 RSA 2 048 bits.

REMARQUE : La mise à jour du micrologiciel du bloc d'alimentation n'est pas prise en charge lorsque le mode FIPS est activé dans le châssis.

Pour plus d'informations, voir l'*Aide en ligne CMC*.

Les fonctions/applications suivantes sont conformes aux FIPS.

- GUI Web
- RACADM
- WSMan
- SSH v2
- SMTP
- Kerberos
- Client NTP
- NFS

REMARQUE : SNMP n'est pas compatible avec le mode FIPS. En mode FIPS, toutes les fonctions SNMP fonctionnent, à l'exception de l'authentification à l'aide de l'algorithme Message Digest version 5 (MD5).

Activation du mode FIPS à l'aide de l'interface Web CMC

Pour activer FIPS :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis**.
   La page **Intégrité du châssis** s'affiche.
2. Dans la barre de menus, cliquez sur **Réseau**.
   La page **Configuration réseau** s'affiche.
3. Dans la section **FIPS (Federal Information Processing Standards)**, à partir du menu déroulant **Mode FIPS**, sélectionnez **Activé**.
   Un message s'affiche pour indiquer que l'activation de FIPS réinitialise le CMC aux paramètres par défaut.
4. Cliquez sur **OK** pour continuer.

Définition du mode FIPS à l'aide de RACADM

Pour activer le mode FIPS, exécutez la commande suivante :

```
racadm config -g cfgRacTuning -o cfgRacTuneFipsModeEnable 1
```

.

Désactivation du mode FIPS

Pour désactiver le mode FIPS, réinitialisez le CMC aux paramètres par défaut.

Configuration des services

Vous pouvez configurer et activer les services suivants dans CMC :

- Console série CMC : permet d'accéder au contrôleur CMC en utilisant la console série.
- Serveur Web : permet d'accéder à l'interface Web CMC. La désactivation du serveur Web désactive RACADM distant.
- SSH : permet d'accéder à CMC via le RACADM micrologiciel.
- Telnet : permet d'accéder à CMC via le RACADM micrologiciel.
- RACADM : permet d'accéder à CMC avec RACADM.
- SNMP : permet à CMC d'envoyer des interruptions SNMP pour les événements.
- Journal syslog distant : permet au contrôleur CMC de consigner les événements sur un serveur distant. Pour utiliser cette fonction, vous devez disposer d'une licence d'entreprise.

Le contrôleur CMC inclut un serveur Web configuré pour utiliser le protocole de sécurité standard SSL pour accepter et transférer des données cryptées depuis et vers des clients sur Internet. Le serveur Web inclut un certificat numérique SSL autosigné Dell (ID de serveur). Il est chargé d'accepter les demandes HTTP sécurisées provenant des clients et d'y répondre. Ce service est indispensable à l'interface Web et à l'outil CLI RACADM distant pour communiquer avec le contrôleur CMC.

En cas de réinitialisation du serveur Web, attendez au moins une minute que les services redeviennent disponibles. La réinitialisation du serveur Web intervient généralement à la suite de l'un des événements suivants :

- Vous modifiez les propriétés de configuration réseau ou de sécurité réseau dans l'interface utilisateur Web CMC ou avec RACADM.
- Vous modifiez la configuration de port du serveur Web via l'interface utilisateur Web ou RACADM.

- Vous réinitialisez CMC.
- Un nouveau certificat de serveur SSL est téléchargé.

REMARQUE : Pour modifier les paramètres des services, vous devez disposer des droits d'Administrateur de configuration du châssis.

Le journal syslog distant est une cible supplémentaire de journalisation du contrôleur CMC. Une fois que vous avez configuré le journal syslog distant, toute nouvelle entrée de journal générée par le contrôleur CMC est envoyée vers les destinations correspondantes.

REMARQUE : Comme le transport réseau des entrées de journal transférées est UDP, il n'existe aucune garantie que les entrées de journal soient livrées, pas plus que le contrôleur CMC n'indique si les entrées de journal ont été correctement reçues.

Configuration des services dans l'interface Web CMC

Pour configurer les services CMC à l'aide de l'interface Web CMC :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** et sur **Réseau** > **Services**. La page **Gestion des services** s'affiche.
2. Configurez les services suivants, si nécessaire :
   - Série CMC
   - Web Server
   - SSH
   - Telnet
   - Interface RACADM distante
   - SNMP
   - Syslog distant

   Pour plus d'informations sur les champs, voir l'*Aide en ligne*.
3. Cliquez sur **Appliquer** et mettez à jour toutes les limites d'expiration par défaut et maximales.

Configuration des services à l'aide de l'interface RACADM

Pour activer et configurer les services, utilisez les objets RACADM suivants :

- `cfgRacTuning`
- `cfgRacTuneRemoteRacadmEnable`

Pour plus d'informations sur ces objets, voir le document *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX) accessible sur le site dell.com/support/manuals.

Si le micrologiciel du serveur ne prend pas en charge une fonctionnalité, la configuration d'une propriété liée à cette fonctionnalité affiche une erreur. Par exemple, l'utilisation de RACADM pour activer un journal système (syslog) distant sur un iDRAC non pris en charge génère un message d'erreur.

De même, lors de l'affichage des propriétés iDRAC à l'aide de la commande RACADM `getconfig`, les valeurs des propriétés s'affichent sous la forme S/O pour une fonctionnalité non prise en charge sur le serveur.

Par exemple :

```
$ racadm getconfig -g cfgSessionManagement -m server-1 # cfgSsnMgtWebServerMaxSessions=N/A #
cfgSsnMgtWebServerActiveSessions=N/A # cfgSsnMgtWebServerTimeout=N/A #
cfgSsnMgtSSHMaxSessions=N/A # cfgSsnMgtSSHActiveSessions=N/A # cfgSsnMgtSSHTimeout=N/A #
cfgSsnMgtTelnetMaxSessions=N/A # cfgSsnMgtTelnetActiveSessions=N/A #
cfgSsnMgtTelnetTimeout=N/A
```

Configuration de la carte de stockage étendu CMC

Vous pouvez activer ou réparer le support Flash amovible en option pour l'utiliser comme stockage étendu non volatile. Certaines fonctionnalités CMC ont besoin du stockage étendu non volatile pour fonctionner correctement.

Pour activer ou réparer le support Flash amovible en utilisant l'interface Web CMC :

1. Dans le volet de gauche, accédez à **Présentation du châssis** et cliquez sur **Contrôleur de châssis** > **Support Flash**.
2. Sur la page **Support Flash amovible**, dans le menu déroulant, sélectionnez l'une des options suivantes de manière appropriée :
   - **Réparer le média du contrôleur actif**
   - **Arrêter d'utiliser le média flash pour stocker les données du châssis**

   Pour plus d'informations sur ces options, voir l'*Aide en ligne*.
3. Cliquez sur **Appliquer** pour appliquer l'option sélectionnée.

   Si le châssis contient deux contrôleurs CMC, les deux CMC (actif et de secours) doivent contenir un support Flash. Autrement, les performances de la fonction de stockage étendu seront dégradées.

Configuration d'un groupe de châssis

Le contrôleur CMC permet de surveiller plusieurs châssis à partir d'un châssis maître unique. Lorsque vous activez un groupe de châssis, le contrôleur CMC du châssis maître génère une image graphique de l'état du châssis maître et de tous les châssis membres du groupe de châssis. Pour utiliser cette fonction, vous devez disposer d'une licence d'entreprise.

Les fonctions des groupes de châssis sont les suivantes :

- Affiche les images de la face avant et de la face arrière de chaque châssis, un ensemble pour le maître et un ensemble pour chaque membre.
- Les problèmes d'intégrité du maître et des membres d'un groupe sont signalés par des superpositions rouges ou jaunes, et par un X ou un point d'exclamation (!) sur le composant montrant les symptômes en question. Vous affichez des détails supplémentaires sous l'image en cliquant sur l'image de châssis ou sur **Détails**.
- Des liens de lancement rapide sont disponibles pour ouvrir les pages Web du châssis membre ou du serveur.
- Un inventaire de serveur et des entrées/sorties est disponible pour un groupe.
- Une option sélectionnable est disponible pour synchroniser les propriétés d'un nouveau membre avec celles du chef de groupe lorsqu'un nouveau membre est ajouté à ce dernier.

Un groupe de châssis peut contenir jusqu'à huit membres. De plus, un maître ou un membre ne peut appartenir qu'à un seul groupe. Vous ne pouvez pas placer un châssis, maître ou membre, déjà membre d'un autre groupe. Par contre, vous pouvez supprimer un châssis d'un groupe pour l'ajouter ensuite à un autre groupe.

Pour configurer un groupe de châssis avec l'interface Web CMC :

1. Connectez-vous au châssis maître à l'aide des privilèges d'administrateur.
2. Cliquez sur **Configuration** > **Administration des groupes**.
3. Dans la page **Groupe de châssis**, sous **Rôle**, sélectionnez **Maître**. Un champ permet d'ajouter le nom du groupe.
4. Entrez le nom du groupe dans le champ **Nom du groupe**, puis cliquez sur **Appliquer**.

   REMARQUE : les mêmes règles qui s'appliquent pour un nom de domaine s'appliquent au nom de groupe.

   Une fois le groupe de châssis créé, l'interface utilisateur graphique affiche automatiquement la page **Groupe de châssis**. Le volet de gauche contient le groupe identifié par son nom et le châssis maître, ainsi que les châssis membres non remplis.

Ajout de membres à un groupe de châssis

Une fois le groupe du châssis configuré, pour ajouter des membres au groupe :

1. Connectez-vous au châssis maître en utilisant les privilèges d'administrateur.
2. Sélectionnez le châssis maître dans l'arborescence.
3. Cliquez sur **Configuration** > **Administration des groupes**.
4. Sous **Gestion des groupes**, saisissez l'adresse IP ou le nom DNS du membre dans le champ **Nom d'hôte/Adresse IP**.
5. Dans le champ **Nom de l'utilisateur**, entrez le nom d'utilisateur détenant des privilèges d'administrateur du châssis membre.
6. Entrez le mot de passe correspondant dans le champ **Mot de passe**.
7. Facultatif : sélectionnez **Synchroniser le nouveau membre avec les propriétés du leader/chef** pour pousser les propriétés du chef vers le membre.
8. Cliquez sur **Appliquer**.
9. Pour ajouter jusqu'à huit membre, exécutez les tâches des étapes 4 à 8. Les noms de châssis des nouveaux membres apparaissent dans la boîte de dialogue **Membres**.

REMARQUE : Les références entrées pour un membre sont transmises en mode sécurisé au châssis membre afin d'établir une relation de confiance entre les châssis membres et le châssis maître. Les références ne sont pas conservées dans chaque châssis et ne sont plus jamais échangées après l'établissement de la relation de confiance.

Retrait d'un membre du châssis maître

Vous pouvez supprimer un membre de groupe à partir du châssis maître. Pour supprimer un membre :

1. Connectez-vous au châssis maître en utilisant les privilèges d'administrateur.
2. Dans le volet de gauche, sélectionnez le châssis maître.
3. Cliquez sur **Configuration** > **Administration des groupes**.
4. Dans la liste **Suppression de membres**, sélectionnez le nom du membre à supprimer, puis cliquez sur **Appliquer**.

   Le châssis maître communique avec le ou les membres, si vous en avez sélectionné plusieurs, supprimés du groupe. Le nom de membre est supprimé. Les châssis membres ne reçoivent pas le message si un problème réseau empêche le châssis maître de contacter les membres. Dans ce cas, désactivez le membre à partir du châssis membre pour achever la suppression.

Dissolution d'un groupe de châssis

Pour dissoudre un groupe de châssis depuis le châssis maître :

1. Connectez-vous au châssis maître avec les privilèges d'Administrateur.
2. Sélectionnez le châssis maître dans le volet de gauche.
3. Cliquez sur **Configuration** > **Administration des groupes**.
4. Dans la page **Groupe du châssis**, sous **Rôle**, sélectionnez **Aucun**, puis cliquez sur **Appliquer**.

   Le châssis maître indique alors à tous les membres qu'ils ont tous été supprimés du groupe. Le châssis maître peut être défini comme maître ou membre d'un nouveau groupe.

   Si un problème de réseau empêche le contact entre le maître et le membre, le châssis membre peut ne pas recevoir les message. Dans ce cas, désactivez le membre depuis le châssis membre pour effectuer le retrait.

Désactivation d'un seul membre sur le châssis membre

Parfois, le châssis maître ne peut pas supprimer un membre d'un groupe. Cela peut se produire si la connexion réseau au membre est perdue. Pour supprimer un membre du groupe sur le châssis membre :

1. Connectez-vous au châssis membre en utilisant les privilèges d'administrateur de châssis.
2. Dans le volet de gauche, cliquez su **Présentation du châssis** > **Configurer** > **Administration de groupe**.
3. Sélectionnez **Aucun**, puis cliquez sur **Appliquer**.

Accès à la page Web d'un châssis membre ou d'un serveur

Vous pouvez accéder à la page Web du châssis membre, à la console distante du serveur ou à la page Web du serveur iDRAC à partir de la page du groupe de châssis maîtres. Si le périphérique membre possède les mêmes informations d'identification que le châssis maître, vous pouvez utiliser ces informations pour accéder au périphérique membre.

REMARQUE : L'authentification unique (SSO) et la connexion par carte à puce ne sont pas prises en charge dans la gestion multichâssis (MCM). L'accès aux membres via l'authentification unique (SSO) depuis le châssis maître nécessite un nom d'utilisateur ou un mot de passe commun entre le maître et les membres. L'utilisation d'un nom d'utilisateur ou d'un mot de passe commun ne fonctionne qu'avec les utilisateurs Active Directory, locaux et LDAP.

Pour naviguer vers les périphériques membres :

1. Connectectez-vous au châssis maître.
2. Sélectionnez **Groupe : nom** dans l'arborescence.
3. Si un CMC membre correspond à la destination requise, sélectionnez **Lancer CMC** en regard du châssis requis.

   Si l'un des serveurs d'un châssis correspond à la destination requise :

a. Sélectionnez l'image du châssis de destination.
b. Dans l'image du châssis qui s'affiche dans la section **Intégrité**, sélectionnez le serveur.
c. Dans la boîte de dialogue **Liens rapides**, sélectionnez le périphérique de destination. Une nouvelle fenêtre s'affiche sur la page de destination ou l'écran de connexion.

REMARQUE : Dans MCM, tous les Liens rapides associés aux serveurs ne sont pas affichés.

Propagation des propriétés du châssis maître aux châssis membres

Vous pouvez appliquer les propriétés du maître aux châssis membres d'un groupe. Pour synchroniser un membre avec les propriétés du maître :

1. Connectez-vous au châssis maître avec des privilèges Administrateur.
2. Sélectionnez le châssis maître dans l'arborescence.
3. Cliquez sur **Configuration** > **Administration des groupes**.
4. Dans la section **Propagation des propriétés du châssis**, sélectionnez l'un des types de propagation :
   - Propagation en cas de changement : Sélectionnez cette option pour la propagation automatique des paramètres de propriété de châssis sélectionnés. Les changements de propriété sont propagés à tous les membres du groupe actuel, chaque fois que les propriétés du maître sont changées.
   - Propagation manuelle : Sélectionnez cette option pour la propagation manuelle des propriétés du châssis maître du groupe à ses membres. Les paramètres de propriété du châssis maître sont propagés aux membres du groupe uniquement lorsqu'un administrateur du châssis maître clique sur **Propager**.
5. Dans la section **Propriétés de propagation**, sélectionnez les catégories de propriétés de la configuration maître à propager aux châssis membres.

   Sélectionnez uniquement les catégories de paramètres que vous souhaitez configurer de manière identique parmi tous les membres du groupe de châssis. Par exemple, sélectionnez la catégorie **Propriétés de journalisation et d'alerte** pour permettre à tous les châssis du groupe de partager les paramètres de configuration de journalisation et d'alerte du châssis maître.
6. Cliquez sur **Enregistrer**.

   Si l'option **Propagation en cas de changement** est sélectionnée, les châssis membres adoptent les propriétés du maître. Si l'option **Propagation manuelle** est sélectionnée, cliquez sur **Propager** lorsque que vous voulez propager les paramètres choisis aux châssis membres. Pour plus d'informations sur la propagation des propriétés du châssis maître aux châssis membres, consultez l'*Aide en ligne*.

Inventaire des serveurs pour un groupe CMC

Un groupe est un châssis maître contenant de 0 à 8 châssis. La page **Intégrité du groupe de châssis** affiche tous les châssis membres et permet d'enregistrer le rapport d'inventaire des serveurs dans un fichier en utilisant la fonction de téléchargement de navigateur Standard. Le rapport contient des données sur :

- tous les serveurs présents dans le groupe de châssis (y compris le maître). ;
- les logements vides et les logements d'extension (y compris modules serveur pleine hauteur et double largeur).

Enregistrement de l'inventaire des serveurs

Pour enregistrer le rapport d'inventaire des serveurs en utilisant l'interface Web CMC :

1. Dans le volet de gauche, sélectionnez **Groupe**.
2. Sur la page **Intégrité du groupe de châssis**, cliquez sur **Enregistrer le rapport d'inventaire**. La boîte de dialogue **Téléchargement de fichier** qui s'affiche vous invite à ouvrir ou enregistrer le fichier.
3. Cliquez sur **Enregistrer** et spécifiez le chemin et le nom du fichier de rapport d'inventaire des modules serveur.

   REMARQUE : Le maître du groupe de châssis, les châssis membres du groupe de châssis et le module serveur dans le châssis associé doivent être sous tension pour pouvoir obtenir le rapport d'inventaire de module serveur le plus précis.

Données exportées

Le rapport d'inventaire des serveurs contient les dernières données renvoyées par chaque membre du groupe de châssis au cours de l'opération d'interrogation normale du maître du groupe de châssis (toutes les 30 secondes).

Pour obtenir le rapport d'inventaire des serveurs le plus exact :

- Le maître du groupe de châssis et tous les châssis membres de ce groupe doivent avoir l'état **Alimentation de châssis activée**.
- Tous les serveurs dans le châssis associé doivent être sous tension.

Les données d'inventaire des châssis et des serveurs associés n'apparaissent pas forcément dans le rapport d'inventaire si certains des châssis membres du groupe de châssis ont les caractéristiques suivantes :

- Dans l'état **Alimentation de châssis désactivée**
- Hors tension

REMARQUE : Si vous insérez un serveur alors que le châssis est hors tension, le numéro de modèle ne s'affiche nulle part dans l'interface Web tant que le châssis n'est remis sous tension.

Le tableau suivant répertorie les champs de données et la configuration requise spécifiques signalés pour chaque serveur :

Tableau 17. Description des champs de l'inventaire du module de serveur

Champ de données	Exemple
Nom du châssis	Chef de châssis de centre de données
Adresse IP du châssis	192.168.0.1
Emplacement de logement	1
Nom du logement	SLOT-01
Nom d'hôte	Serveur Web d'entreprise **REMARQUE : requiert un agent Server Administrator exécuté sur le serveur; autrement, le champ sera vierge.**
Système d'exploitation	Windows Server 2008 **REMARQUE : requiert un agent Server Administrator exécuté sur le serveur; autrement, le champ sera vierge.**
Modèle	PowerEdgeM610
Service Tag	1PB8VF1
Total de mémoire système	4 Go / **REMARQUE : Exige VRTX CMC 1.0 (ou une version ultérieure) sur le membre ; autrement le champ est vide.**
Nbr d'UC	2 **REMARQUE : Exige VRTX CMC 1.0 (ou une version ultérieure) sur le membre ; autrement le champ est vide.**
Infos sur l'UC	UC Intel (R) Xeon (R) E5502 à 1,87GHzn **REMARQUE : Exige VRTX CMC 1.0 (ou une version ultérieure) sur le membre ; autrement le champ est vide.**

Format des données

Le rapport d'inventaire est généré dans un fichier `.CSV` afin qu'il puisse être importé dans différents outils, tels que Microsoft Excel. Le fichier `.CSV` de rapport d'inventaire peut être importé dans le modèle. Pour ce faire, sélectionnez **Données** > **À partir du texte** dans MS Excel. Une fois le rapport d'inventaire importé dans MS Excel, si un message s'affiche pour demander des informations supplémentaires, sélectionnez l'option de fichier délimité par des virgules pour importer le fichier dans MS Excel.

Version de micrologiciel et d'inventaire de groupe de châssis

La page **Version de micrologiciel de groupe de châssis** affiche l'inventaire de groupes et les versions de micrologiciel des serveurs et des composants de serveur présents dans le châssis. Cette page vous permet également d'organiser les informations d'inventaire et de filtrer l'affichage des versions de micrologiciel. La vue qui s'affiche est basée sur les serveurs ou n'importe quel composant du serveur présent dans le châssis :

- BIOS
- iDRAC
- CPLD
- USC
- Diagnostics
- Pilotes SE
- RAID
- Carte réseau

REMARQUE : Les informations d'inventaire affichées pour le groupe de châssis, le châssis membre, les serveurs et les composants de serveur, sont mises à jour chaque fois qu'un châssis est ajouté au groupe ou en est retiré.

Affichage de l'inventaire de groupe de châssis

Pour afficher le groupe de châssis à l'aide de l'interface Web CMC, dans le volet gauche, sélectionnez **Groupe**. Cliquez sur **Propriétés** > **Version du micrologiciel**. La page **Version du micrologiciel du groupe de châssis** affiche tous les châssis présents dans le groupe.

Affichage de l'inventaire de châssis sélectionnés à l'aide de l'interface Web

Pour afficher l'inventaire de châssis sélectionnés à l'aide de l'interface Web :

1. Dans l'arborescence système, sélectionnez **Groupe**. Cliquez sur **Propriétés** > **Version de micrologiciel**.
   La page **Version du micrologiciel du groupe de châssis** affiche tous les châssis du groupe.
2. Dans la section **Sélectionner un châssis**, sélectionnez le châssis membre dont vous souhaitez afficher l'inventaire.
   La section **Filtre d'affichage du micrologiciel** affiche l'inventaire de serveurs des châssis sélectionnés et des versions de micrologiciel de tous les composants de serveur.

Affichage des versions de micrologiciel de composant de serveur sélectionné à l'aide de l'Interface Web

Pour afficher les versions du micrologiciel des composants du serveur sélectionnés à l'aide de l'interface Web CMC :

1. Dans le volet gauche, sélectionnez **Groupe**. Cliquez sur **Propriétés** > **Version du micrologiciel**.
   La page **Version du micrologiciel du groupe de châssis** affiche tous les châssis du groupe.
2. Dans la section **Sélectionner un châssis**, sélectionnez le châssis membre dont vous souhaitez afficher l'inventaire.
3. Dans la section **Filtre d'affichage du micrologiciel**, sélectionnez **Composants**.
4. Dans la liste **Composants**, sélectionnez le composant requis (BIOS, iDRAC, CPLD, USC, Diagnostics, OS Drive, périphériques RAID (jusqu'à 2) et périphériques NIC (jusqu'à 6)) dont vous souhaitez afficher la version micrologicielle .
   Les versions de micrologiciel du composant sélectionné de tous les serveurs dans le châssis sélectionné s'affichent.

Profils de configuration du châssis

La fonction Profils de configuration du châssis vous permet de configurer le châssis avec les profils de configuration du châssis stockés dans le partage réseau ou dans la station de gestion locale ; elle vous permet également de restaurer la configuration du châssis.

Pour accéder à la page **Profils de configuration du châssis** de l'interface Web CMC, dans l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **Configuration** > **Profils**. La page **Profils de configuration du châssis** s'affiche.

Vous pouvez effectuer les tâches suivantes à l'aide de la fonction Profils de configuration du châssis :

- Configurer un châssis à l'aide des profils de configuration du châssis dans la station de gestion locale pour la configuration initiale.
- Enregistrer les paramètres de configuration du châssis actuels dans un fichier XML sur le partage réseau ou sur la station de gestion locale.
- Restaurer la configuration du châssis.
- Importer des profils de châssis (fichiers XML) sur le partage réseau à partir d'une station de gestion locale.
- Exporter les profils de châssis (fichiers XML) du partage réseau vers une station de gestion locale.
- Appliquer, modifier, supprimer ou exporter une copie des profils stockés sur le partage réseau.

Enregistrement de la configuration du châssis

Vous pouvez enregistrer la configuration actuelle du châssis dans un fichier XML sur un partage réseau ou une station de gestion locale. Les configurations incluent toutes les propriétés du châssis qui peuvent être modifiés à l'aide de l'interface Web CMC et les commandes RACADM. Vous pouvez également utiliser le fichier XML qui est enregistré pour restaurer la configuration sur le même châssis ou pour configurer d'autres châssis.

REMARQUE : Les paramètres de serveur et d'iDRAC ne sont pas enregistrés ou restaurés avec la configuration du châssis.

Pour enregistrer la configuration actuelle du châssis, effectuez les tâches suivantes :

1. Accédez à la page **Profils de configuration du châssis**. Dans la section **Enregistrement et sauvegarde** > **Enregistrer la configuration actuelle** , entrez un nom de profil dans le champ **Nom du profil**.

   REMARQUE : Lors de l'enregistrement de la configuration actuelle du châssis, le jeu de caractères étendu ASCII standard est pris en charge. Toutefois, les caractères spéciaux suivants ne sont pas pris en charge :

   “, ., *, >, <, \, /, : et |

2. Sélectionnez l'un des types de profils suivants à partir de l'option **Type de profil** :
   - **Remplacer** : comprend des attributs de toute la configuration CMC sauf les attributs d'écriture seule tels que les mots de passe utilisateur et les numéros de service. Ce type de profil est utilisé comme fichier de configuration de sauvegarde pour restaurer la configuration du châssis complète notamment des informations d'identité, telles que les adresses IP.
   - **Cloner** : comprend tous les attributs de profil de type **Remplacer**. Il est indiqué d'ignorer les attributs d'identité tels que l'adresse MAC et l'adresse IP pour des raisons de sécurité. Ce type de profil est utilisé pour cloner un nouveau châssis.
3. Sélectionnez l'un des emplacements suivants dans le menu déroulant **Emplacement de profil** pour stocker le profil :
   - **Local** : pour enregistrer le profil dans la station de gestion locale.
   - **Partage réseau** : pour enregistrer le profil dans un emplacement partagé.
4. Cliquez sur **Enregistrer** pour enregistrer le profil à l'emplacement sélectionné.
   Une fois l'action terminée, le message indiquant `Operation Successful` s'affiche :

   REMARQUE : Pour afficher les paramètres enregistrés dans le fichier XML, dans la section Profils stockés, sélectionnez le profil enregistré, puis cliquez sur Afficher dans la colonne Afficher les profils.

Restauration d'un profil de configuration du châssis

Vous pouvez restaurer la configuration d'un châssis en important le fichier de sauvegarde (`.xml` ou `.bak`) sur la station de gestion locale ou le partage réseau où les configurations de châssis sont enregistrées. Les configurations comprennent toutes les propriétés disponibles via l'interface Web CMC, les commandes RACADM et les paramètres.

Pour restaurer la configuration du châssis, effectuez les tâches suivantes :

1. Accédez à la page **Profils de configuration du châssis**. Dans la section **Restaurer une configuration** > **Restauration la configuration du châssis**, cliquez sur **Parcourir**, puis sélectionnez le fichier de sauvegarde pour importer la configuration du châssis enregistrée.
2. Cliquez sur l'option **Restaurer une configuration** pour charger un fichier de sauvegarde crypté (`.bak`) ou un fichier de profil `.xml` stocké sur le CMC.
   L'interface Web CMC revient à la page de connexion après une opération de restauration réussie.

REMARQUE : Si les fichiers de sauvegarde (.bak) de versions antérieures de CMC sont chargés sur la dernière version de CMC où FIPS est activé, reconfigurez les 16 mots de passe des utilisateurs locaux CMC. Toutefois, le mot de passe du premier utilisateur est réinitialisé à « calvin ».

REMARQUE : Lorsqu'un profil de configuration de châssis est importé d'un CMC qui ne prend pas en charge la fonction FIPS à un CMC dans lequel elle est activée, la fonction FIPS reste activée dans le CMC.

REMARQUE : Si vous modifiez le mode FIPS dans le profil de configuration du châssis, le paramètre `DefaultCredentialMitigation` est activé.

Affichage des profils de configuration du châssis stockés

Pour afficher les profils de configuration du châssis stockés sur le partage réseau, accédez à la page **Profils de configuration du châssis**. Dans la section **Profils de configuration du châssis** > **Profils stockés**, sélectionnez le profil, puis cliquez sur **Afficher** dans la colonne **Afficher le profil**. La page **Afficher les paramètres** s'affiche. Pour en savoir plus sur les paramètres affichés, voir l'*Aide en ligne du CMC*.

Application des profils de configuration du châssis

Vous pouvez appliquer la configuration du châssis au châssis si les profils de configuration du châssis sont disponibles en tant que profils stockés sur le partage réseau. Pour lancer une opération de configuration du châssis, appliquez un profil stocké à un châssis.

Pour appliquer un profil à un châssis, procédez comme suit :

1. Accédez à la page **Profils de configuration du châssis**. Dans la section **Profils stockés**, sélectionnez le profil stocké que vous souhaitez appliquer.
2. Cliquez sur **Appliquer le profil**.

   Un message d'avertissement s'affiche indiquant que l'application d'un nouveau profil écrasera les paramètres actuels et redémarrera les châssis sélectionnés. Vous êtes invité à confirmer si vous souhaitez poursuivre l'opération.
3. Cliquez sur **OK** pour appliquer le profil au serveur sélectionné.

Exportation des profils de configuration du châssis

Vous pouvez exporter les profils de configuration du châssis enregistrés sur le partage réseau vers un chemin spécifié sur une station de gestion.

Pour exporter un profil stocké, effectuez les tâches suivantes :

1. Accédez à la page **Profils de configuration du châssis**. Dans la section **Profils de configuration du châssis** > **Profils stockés**, sélectionnez le profil souhaité, puis cliquez sur **Exporter une copie du profil**.
   La boîte de dialogue **Téléchargement de fichier** qui s'affiche vous invite à ouvrir ou à enregistrer le fichier.
2. Cliquez sur **Enregistrer** ou **Ouvrir** pour exporter le profil vers l'emplacement requis.

Modification des profils de configuration du châssis

Vous pouvez modifier le nom du profil de configuration de châssis d'un châssis.

Pour modifier un nom du profil de configuration de châssis, procédez comme suit :

1. Accédez à la page **Profils de configuration du châssis**. Dans la section **Profils de configuration du châssis** > **Profils stockés**, sélectionnez le profil souhaité, puis cliquez sur **Modifier le profil**.
   La fenêtre **Modifier un profil** s'affiche.
2. Entrez un nom de profil souhaité dans le champ **Nom du profil**, puis cliquez sur **Modifier le profil**.
   Le message `Operation Successful`(Opération réussie) s'affiche.
3. Cliquez sur **OK**.

Suppression des profils de configuration du châssis

Vous pouvez supprimer un profil de configuration du châssis qui est stocké sur le partage réseau.

Pour supprimer un profil de configuration du châssis, procédez comme suit :

1. Accédez à la page **Profils de configuration du châssis**. Dans la section **Profils de configuration du châssis** > **Profils stockés**, sélectionnez le profil souhaité, puis cliquez sur **Supprimer le profil**.
   Un message d'avertissement s'affiche, indiquant que la suppression d'un profil supprimerait définitivement le profil sélectionné.
2. Cliquez sur **OK** pour supprimer le profil sélectionné.

Configuration de plusieurs CMC à l'aide de RACADM

À l'aide de RACADM, vous pouvez configurer un ou plusieurs CMC avec des propriétés identiques.

Lorsque vous interrogez une carte CMC en utilisant son ID de groupe et de son ID d'objet, RACADM crée le fichier de configuration `racadm.cfg` à partir des informations récupérées. En exportant ce fichier vers un ou plusieurs contrôleurs CMC, vous pouvez configurer les contrôleurs avec des propriétés identiques en un minimum de temps.

REMARQUE : Certains fichiers de configuration contiennent des informations CMC uniques (comme l'adresse IP statique) qui doivent être modifiées avant d'exporter le fichier vers d'autres CMC.

1. Utilisez RACADM pour effectuer une requête auprès du CMC cible contenant la configuration appropriée.

   REMARQUE : Le fichier de configuration généré est `myfile.cfg`. Vous pouvez renommer le fichier. Le fichier `.cfg` ne contient aucun mot de passe utilisateur. Lorsque vous téléversez le fichier `.cfg` vers le nouveau CMC, vous devez ajouter à nouveau tous les mots de passe.

2. À l'invite de commande, entrez :

   ```
   racadm getconfig -f myfile.cfg
   ```

   REMARQUE : La redirection d'une configuration CMC vers un fichier à l'aide de `getconfig -f` est uniquement prise en charge par l'interface de RACADM distant.

3. Modifiez le fichier de configuration dans un éditeur de texte brut (facultatif). Tout caractère de formatage spécial présent dans le fichier de configuration peut corrompre la base de données RACADM.
4. Utilisez le fichier de configuration que vous venez de créer pour modifier le CMC cible. À l'invite de commande, entrez ce qui suit :

   ```
   racadm config -f myfile.cfg
   ```

5. Réinitialisez le CMC cible configuré. À l'invite de commande, entrez :

   ```
   racadm reset
   ```

   La sous-commande `getconfig -f myfile.cfg` demande la configuration CMC de la carte CMC active et génère le fichier `myfile.cfg`. Si nécessaire, vous pouvez renommer ce fichier ou l'enregistrer à un autre emplacement.

   Vous pouvez utiliser la commande `getconfig` pour effectuer les actions suivantes :

   - afficher toutes les propriétés de configuration dans un groupe (spécifié par le nom de groupe et l'index) ;
   - afficher toutes les propriétés de configuration d'un utilisateur par nom d'utilisateur.

   La sous-commande `config` charge les informations dans d'autres CMC. Server Administrator utilise la commande `config` pour synchroniser la base de données des utilisateurs et des mots de passe.

Création d'un fichier de configuration CMC

Le fichier de configuration CMC, `<filename>.cfg`, est utilisé avec la commande `racadm config -f <filename>.cfg` pour créer un fichier texte simple. La commande vous permet de créer un fichier de configuration (semblable à un fichier `.ini`) et de configurer le CMC à partir de ce fichier.

Vous pouvez utiliser n'importe quel nom de fichier, et le fichier ne nécessite pas d'extension `.cfg` (même s'il est désigné par cette extension dans cette sous-section).

REMARQUE : Pour plus d'informations sur la sous-commande `getconfig`, reportez-vous au *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX*.

RACADM analyse le fichier `.cfg` lorsqu'il est chargé pour la première fois sur le contrôleur CMC afin de vérifier la présence d'un groupe et de noms d'objet valides et de s'assurer que les règles de syntaxe simples sont bien respectées. Les erreurs sont signalées par le numéro de ligne qui a détecté l'erreur et sont accompagnées d'un message qui explique la nature du problème. L'ensemble du fichier est analysé et toutes les erreurs s'affichent. Si une erreur est détectée dans le fichier `.cfg`, les commandes d'écriture ne sont pas transmises au CMC. Vous devez corriger toutes les erreurs avant de pouvoir effectuer une configuration.

Pour vérifier les erreurs avant de créer le fichier de configuration, utilisez l'option `-c` avec la sous-commande `config`. Avec l'option `-c`, la sous-commande `config` vérifie uniquement la syntaxe sans écrire sur le CMC.

Tenez compte des consignes suivantes lorsque vous créez un fichier `.cfg` :

- Si l'analyseur rencontre un groupe indexé, c'est la valeur de l'objet ancré qui différencie les différents index.

  L'analyseur lit tous les index du CMC associés à ce groupe. Tous les objets contenus dans ce groupe sont modifiés lors de la configuration du CMC. Si un objet modifié représente un nouvel index, l'index est créé sur le CMC lors de la configuration.
- Vous ne pouvez pas spécifier l'index de votre choix dans un fichier `.cfg`.

  Vous pouvez créer et supprimer des index. Au fil du temps, le groupe peut être fragmenté avec des index utilisés et non utilisés. Si un index est présent, il est modifié. Si aucun index n'est présent, le premier index disponible est utilisé.

  Cette méthode apporte une certaine flexibilité lors de l'ajout d'entrées indexées si vous n'avez pas besoin de rechercher des correspondances d'index exactes entre tous les CMC gérés. Les nouveaux utilisateurs sont ajoutés au premier index disponible. Si tous les index sont pleins, un fichier `.cfg` qui parvient à analyser et à s'exécuter correctement sur un contrôleur CMC peut ne pas fonctionner correctement sur un autre ; vous devez alors ajouter un nouvel utilisateur.
- Utilisez la sous-commande `racresetcfg` pour configurer les deux contrôleurs CMC avec des propriétés identiques.

  Utilisez la sous-commande `racresetcfg` pour rétablir les valeurs d'origine par défaut du CMC, puis exécutez la commande `racadm config -f <filename>.cfg`. Assurez-vous que le fichier `.cfg` contient tous les objets, les utilisateurs, les index et les autres paramètres souhaités. Pour obtenir une liste complète des objets et des groupes, reportez-vous au *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX*.

  PRÉCAUTION : Utilisez la sous-commande `racresetcfg` pour réinitialiser la base de données et les paramètres d'interface réseau du CMC aux paramètres par défaut d'origine et pour supprimer tous les utilisateurs ainsi que les configurations d'utilisateurs. Alors que l'utilisateur root est disponible, les paramètres des autres utilisateurs sont également réinitialisés à leur valeur par défaut.
- Si vous saisissez la commande `racadm getconfig -f <filename> .cfg`, la commande génère un fichier `.cfg` pour la configuration actuelle du CMC. Ce fichier de configuration peut être utilisé comme exemple et comme point de départ pour votre propre fichier `.cfg` spécifique.

Règles d'analyse

- Les lignes qui commencent par le caractère de hachage « # » sont traitées comme des commentaires.

  Une ligne de commentaire doit commencer dans la première colonne. Un caractère « # » contenu dans une autre colonne est traité de la même façon qu'un caractère #.

  Certains paramètres de modem peuvent comprendre des caractères # dans leurs chaînes. Aucun caractère d'échappement n'est nécessaire. Vous pouvez être amené à générer un `.cfg` à partir d'une commande `racadm getconfig -f <filename> .cfg`, puis à exécuter une commande `racadm config -f <filename> .cfg` sur un autre CMC, sans ajouter de caractères d'échappement.

  Par exemple :

  ```
  #
  # This is a comment
  [cfgUserAdmin]
  cfgUserAdminPageModemInitString= <Modem init # not
  a comment>
  ```
- Toutes les entrées de groupe doivent être placées entre crochets d'ouverture et de fermeture ([et]).

  Le caractère de début [qui indique un nom de groupe doit se trouver dans la première colonne. Ce nom de groupe doit être spécifié avant tous les objets contenus dans ce groupe. Les objets qui ne sont associés à aucun nom de groupe génèrent une erreur. Les données de configuration sont organisées en groupes, comme défini dans le chapitre traitant des propriétés de base de données du

Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX. L'exemple suivant permet d'obtenir un nom de groupe, un objet ainsi que la valeur de propriété de l'objet :

```
[cfgLanNetworking] -{group name}
cfgNicIpAddress=143.154.133.121 {object name}
{object value}
```

- Tous les paramètres sont spécifiés en tant que paires « objet=valeur » sans espace entre l'objet, le signe = et la valeur. Les espaces insérés après la valeur sont ignorés. Un espace contenu à l'intérieur d'une chaîne de valeurs reste inchangé. N'importe quel caractère placé à droite du signe = (par exemple, un autre signe = ou les signes #, [,], etc.) est traité tel quel. Ces caractères sont valides pour les scripts de chat des modems.

```
[cfgLanNetworking] -{group name}
cfgNicIpAddress=143.154.133.121 {object value}
```

- L'analyseur `.cfg` ignore les entrées d'objet d'index.

  Vous ne pouvez pas spécifier l'index à utiliser. Si l'index existe déjà, soit il est utilisé, soit une nouvelle entrée est créée dans le premier index disponible pour ce groupe.

  La commande `racadm getconfig -f <filename>.cfg` insère un commentaire devant les objets d'index et vous permet de visualiser les commentaires inclus.

  REMARQUE : vous pouvez créer un groupe indexé manuellement en utilisant la commande suivante :

  ```
  racadm config -g <groupname>  -o <anchored object> -i <index 1-4> <unique anchor name>
  ```

- La ligne d'un groupe indexé ne peut pas être supprimée d'un fichier `.cfg`. Si vous supprimez la ligne à l'aide d'un éditeur de texte, RACADM s'arrête lorsqu'il analyse le fichier de configuration et signale une erreur.

  Vous devez supprimer un objet indexé manuellement en utilisant la commande suivante :

  ```
  racadm config -g <groupname>  -o <objectname> -i <index 1-4> ""
  ```

  REMARQUE : Une chaîne de caractères NULL (identifiée par deux guillemets ("")) demande au CMC de supprimer l'index du groupe spécifié.

  Pour voir le contenu d'un groupe indexé, utilisez la commande suivante :

  ```
  racadm getconfig -g <groupname> -i <index 1-4>
  ```

- Pour les groupes indexés, l'objet ancre doit être le premier objet après la paire [ ]. Vous trouverez ci-dessous des exemples de groupes indexés actuels :

  ```
  [cfgUserAdmin]
  cfgUserAdminUserName= <USER_NAME>
  ```

- Lorsque vous utilisez l'interface RACADM distante pour capturer les groupes de configuration dans un fichier, si vous avez omis de définir une propriété clé au sein d'un groupe, le groupe de configuration n'est pas enregistré dans le fichier de configuration. Si vous avez besoin de cloner ces groupes de configuration sur d'autres CMC, vous devez définir la propriété clé avant d'exécuter la commande `getconfig -f`. Vous pouvez également saisir manuellement les propriétés manquantes dans le fichier de configuration après avoir exécuté la commande `getconfig -f`. Cela s'applique à tous les groupes indexés par RACADM.

  La liste suivante répertorie les groupes indexés qui présentent ce comportement ainsi que leurs propriétés de clé correspondantes :

  - cfgUserAdmin — cfgUserAdminUserName
  - cfgEmailAlert — cfgEmailAlertAddress
  - cfgTraps — cfgTrapsAlertDestIPAddr
  - cfgStandardSchema — cfgSSADRoleGroupName
  - cfgServerInfo — cfgServerBmcMacAddress

Modification de l'adresse IP CMC

Lorsque vous modifiez l'adresse IP CMC dans le fichier de configuration, supprimez toutes les entrées `<variable>=<value>` inutiles. Seule l'étiquette contenant « [» et «] » du groupe de variables réel est conservée, y compris les deux entrées `<variable>=<value>` qui concernent le changement d'adresse IP.

Exemple :

```
#
# Object Group "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.10.110
cfgNicGateway=10.35.10.1
```

Ce fichier est mis à jour comme suit :

```
#
# Object Group "cfgLanNetworking"
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.9.143
# comment, the rest of this line is ignored
cfgNicGateway=10.35.9.1
```

La commande `racadm config -f <myfile>.cfg` analyse le fichier et identifie les erreurs par numéro de ligne. Un fichier correct met à jour les entrées appropriées. En outre, vous pouvez utiliser la commande `getconfig` de l'exemple précédent pour confirmer la mise à jour.

Utilisez ce fichier pour télécharger des modifications à l'échelle de l'entreprise ou pour configurer de nouveaux systèmes sur le réseau à l'aide de la commande `racadm getconfig -f <myfile>.cfg`.

REMARQUE : « *Anchor* » est un mot réservé qui ne doit pas être utilisé dans le fichier `.cfg`.

Configuration de plusieurs CMC au moyen de RACADM à l'aide des profils de configuration du châssis

À l'aide des profils de configuration du châssis, vous pouvez exporter les profils de configuration du châssis en tant que fichier XML et importer celui-ci dans un autre châssis.

Utilisez la commande RACADM `get` pour l'opération d'exportation et la commande `set` pour l'opération d'importation.Vous pouvez exporter des profils de châssis (fichiers XML) à partir de CMC sur le partage réseau ou vers une station de gestion locale et importer des profils de châssis (fichiers XML) à partir du partage réseau ou depuis une station de gestion locale.

REMARQUE : Par défaut, l'exportation effectuée est de type clone. Utilisez la commande `--clone` pour obtenir le profil de type clone dans le fichier XML.

Les opérations d'importation et d'exportation vers et depuis le partage réseau peuvent être effectuées via le RACADM local, ainsi que le RACADM distant. En revanche, les opérations d'importation et d'exportation vers et depuis la gestion locale peuvent être effectuées uniquement par l'intermédiaire d'une interface RACADM distante.

Exportation des profils de configuration du châssis

Vous pouvez exporter les profils de configuration du châssis sur le partage réseau à l'aide de la commande `get`.

1. Pour exporter les profils de configuration du châssis en tant que fichier `clone.xml` vers le partage réseau CIFS à l'aide de la commande `get`, saisissez la commande suivante :

   ```
   racadm get -f clone.xml -t xml -l //xx.xx.xx.xx/PATH -u USERNAME -p PASSWORDCMC
   ```

2. Pour exporter les profils de configuration du châssis en tant que fichier `clone.xml` vers le partage réseau NFS à l'aide de la commande `get`, saisissez la commande suivante :

   ```
   racadm get -f clone.xml -t xml -l xx.xx.xx.xx:/PATH
   ```

Vous pouvez exporter les profils de configuration du châssis sur un partage réseau au moyen d'une interface RACADM à distance.

1. Pour exporter les profils de configuration du châssis en tant que fichier clone.xml dans le partage réseau CIFS, saisissez la commande suivante :

```
racadm -r xx.xx.xx.xx -u USERNAMECMC -p PASSWORDCMC get -f clone.xml -t xml -l //
xx.xx.xx.xx/PATH -u USERNAME -p PASSWORD
```

2. Pour exporter les profils de configuration du châssis en tant que fichier clone.xml dans le partage réseau NFS, saisissez la commande suivante :

```
racadm -r xx.xx.xx.xx -u USERNAMECMC -p PASSWORDCMC get -f clone.xml -t xml -l
xx.xx.xx.xx:/PATH
```

Vous pouvez exporter les profils de configuration du châssis vers la station de gestion locale au moyen de l'interface RACADM à distance.

1. Pour exporter les profils de configuration du châssis en tant que fichier clone.xml, saisissez la commande suivante :

```
racadm -r xx.xx.xx.xx -u USERNAMECMC -p PASSWORDCMC get -f clone.xml -t xml
```

Importation des profils de configuration du châssis

Vous pouvez importer les profils de configuration du châssis depuis un partage réseau vers un autre châssis à l'aide de la commande `set`.

1. Pour importer les profils de configuration du châssis depuis le partage réseau CIFS, saisissez la commande suivante :

```
 racadm set -f clone.xml -t xml -l //xx.xx.xx.xx/PATH -u USERNAME -p PASSWORDCMC
```

2. Pour importer les profils de configuration du châssis de partage réseau NFS, saisissez la commande suivante :

```
racadm set -f clone.xml -t xml -l xx.xx.xx.xx:/PATH
```

Vous pouvez importer les profils de configuration du châssis à partir d'un partage réseau au moyen de l'interface RACADM à distance.

1. Pour importer les profils de configuration du châssis depuis le partage réseau CIFS, saisissez la commande suivante :

```
racadm -r xx.xx.xx.xx -u USERNAMECMC -p PASSWORDCMC  set -f clone.xml -t xml -l //
xx.xx.xx.xx/PATH -u USERNAME -p PASSWORD
```

2. Pour importer les profils de configuration du châssis de partage réseau NFS, saisissez la commande suivante :

```
racadm -r xx.xx.xx.xx -u USERNAMECMC -p PASSWORDCMC set -f clone.xml -t xml -l
xx.xx.xx.xx:/PATH
```

Vous pouvez importer les profils de configuration du châssis depuis la station de gestion locale au moyen de l'interface RACADM à distance.

1. Pour exporter les profils de configuration du châssis en tant que fichier clone.xml, saisissez la commande suivante :

```
racadm -r xx.xx.xx.xx -u USERNAMECMC -p PASSWORDCMC set -f clone.xml -t xml
```

Règles d'analyse

Vous pouvez modifier manuellement les propriétés d'un fichier XML exporté de profils de configuration du châssis.

Un fichier XML contient les propriétés suivantes :

- `System Configuration`, qui est le nœud parent.
- `component`, qui est le nœud enfant principal.
- `Attributes`, qui contient le nom et la valeur. Vous pouvez modifier ces champs. Par exemple, vous pouvez modifier la valeur `Asset Tag` de la façon suivante :

```
<Attribute Name="ChassisInfo.1#AssetTag">xxxxxx</Attribute>
```

Exemple de fichier XML :

```
<SystemConfiguration Model="PowerEdge M1000e
"ServiceTag="NOBLE13"
```

```
TimeStamp="Tue Apr  7 14:17:48 2015" ExportMode="2">
<!--Export type is Replace-->
<!--Exported configuration may contain commented attributes. Attributes may be commented due
to dependency,
destructive nature, preserving server identity or for security reasons.-->
<Component FQDD="CMC.Integrated.1">
<Attribute Name="ChassisInfo.1#AssetTag">00000</Attribute>
<Attribute Name="ChassisLocation.1#DataCenterName"></Attribute>
<Attribute Name="ChassisLocation.1#AisleName"></Attribute>
<Attribute Name="ChassisLocation.1#RackName"></Attribute>
….
</Component>
</SystemConfiguration>
```

Affichage et fermeture des sessions CMC

Vous pouvez afficher le nombre d'utilisateurs connectés à iDRAC7 et mettre fin aux sessions utilisateur.

REMARQUE : Pour mettre fin à une session, vous devez disposer du privilège d'Administrateur de configuration du châssis.

Affichage et fermeture des sessions CMC à l'aide de l'interface Web

Pour afficher une session ou y mettre fin avec l'interface Web :

1. Dans le volet gauche, accédez à **Présentation du châssis**, puis cliquez sur **Réseau** > **Sessions** .

   La page **Sessions** affiche l'ID de session, le nom d'utilisateur, l'adresse IP et le type de session. Pour plus d'informations sur ces propriétés, voir l'*Aide en ligne*.

2. Pour mettre fin à la session, cliquez sur **Fermer** en regard de la session en question.

Affichage et fermeture des sessions CMC avec RACADM

Vous devez disposer de privilèges Administrateur pour mettre fin aux sessions CMC avec RACADM.

Pour afficher les sessions utilisateur en cours, utilisez la commande `getssninfo`.

Pour mettre fin à une session utilisateur, utilisez la commande `closessn`.

Pour plus d'informations sur ces commandes, voir le *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX), accessible sur **dell.com/support/manuals**.

7

Configuration des serveurs

Vous pouvez définir les paramètres suivants d'un serveur :

- Noms de logement
- Paramètres réseau d'iDRAC
- Paramètres des numéros LAN virtuel du DRAC
- Périphérique de démarrage initial
- FlexAddress de serveur
- Partage de fichier à distance
- Paramètres BIOS en utilisant un clone de serveur

Sujets :

Définition des noms de logement

Les noms des emplacements sont utilisés pour identifier des serveurs individuels. Pour choisir des noms d'emplacements, les règles suivantes s'appliquent :

- Les noms peuvent contenir un maximum de 24 caractères ASCII non étendus (codes ASCII de 32 à 126). Les caractères standard et spéciaux ne sont pas autorisés.
- Les noms d'emplacements doivent être uniques dans le boîtier. Deux emplacements ne peuvent pas porter le même nom.
- Les chaînes de caractères ne sont pas sensibles à la casse. `Server-1, server-1, and SERVER-1` sont des noms équivalents.
- Les noms de logements ne doivent pas commencer par les chaînes de caractères suivantes :
  - Switch-
  - Fan-
  - PS-
  - DRAC-
  - MC-
  - Châssis
  - Housing-Left
  - Housing-Right
  - Housing-Center
- Les chaînes `Server-1` via `Server-4` peuvent être utilisées, mais uniquement pour l'emplacement correspondant. Par exemple, `Server-3` est un nom valide pour l'emplacement 3 mais pas pour l'emplacement 4. Cependant, `Server-03` est un nom valide pour n'importe quel emplacement.

  REMARQUE : Pour renommer un logement, vous devez disposer du privilège Administrateur de configuration du châssis.

Le paramètre de nom de l'emplacement défini dans l'interface Web réside uniquement dans le contrôleur CMC. Si le serveur est retiré du boîtier, le paramètre du nom de l'emplacement est supprimé du serveur.

La définition d'un nom de logement dans l'interface Web CMC remplace toujours les modifications apportées au nom d'affichage dans l'interface iDRAC.

Pour modifier un nom de logement dans l'interface Web CMC :

1. Dans le volet de gauche, accédez à **Présentation du châssis** > **Présentation du serveur** > **Configuration** > **Noms des logements**.
2. Dans la page **Noms des logements**, modifiez le nom du logement dans le champ **Nom du logement**.
3. Pour utiliser le nom d'hôte d'un serveur comme nom d'emplacement, sélectionnez l'option **Utiliser un nom d'hôte pour le nom d'emplacement**. Vous remplacez ainsi les noms d'emplacement statiques par le nom d'hôte (nom système) du serveur, le cas échéant. Pour ce faire, l'agent OMSA doit être installé sur le serveur. Pour en savoir plus sur l'agent OMSA, reportez-vous au *Guide d'utilisation – Administrateur d'OpenManage Server* disponible à l'adresse dell.com/support/manuals.
4. Pour utiliser le nom DNS d'iDRAC comme nom de logement, sélectionnez l'option **Utiliser le nom DNS d'iDRAC comme nom d'emplacement**. Cette option remplace les noms des logements statiques par les noms DNS d'iDRAC respectifs, si disponibles. Si les noms DNS d'iDRAC ne sont pas disponibles, les noms des logements modifiés ou par défaut s'affichent.

   REMARQUE : Pour sélectionner l'option Utiliser le nom DNS d'iDRAC comme nom de logement, vous devez disposer du privilège Administrateur de configuration du châssis.

5. Pour enregistrer les paramètres, cliquez sur **Appliquer**.

Pour restaurer le nom de logement par défaut du serveur (SLOT-01 sur SLOT-04, en fonction de la position de l'emplacement du serveur concerné), cliquez sur **Restaurer la valeur par défaut**.

Configuration des paramètres réseau iDRAC

Pour utiliser cette fonction, vous devez disposer d'une licence d'entreprise. Vous pouvez configurer le paramètre de configuration réseau iDRAC d'un serveur. Vous pouvez utiliser les paramètres QuickDeploy pour configurer les paramètres de configuration réseau iDRAC par défaut et le mot de passe racine pour les serveurs qui sont installés ultérieurement. Ces paramètres par défaut sont les paramètres QuickDeploy d'iDRAC.

Pour plus d'informations sur l'iDRAC, voir le *Guide de l'utilisateur d'iDRAC* à l'adresse **dell.com/support/manuals**.

Configuration des paramètres réseau iDRAC QuickDeploy

Utilisez les paramètres QuickDeploy pour définir les paramètres réseau des nouveaux serveurs insérés.

Pour activer et définir les paramètres iDRAC QuickDeploy :

1. Dans le volet de gauche, cliquez sur **Présentation du serveur** > **Configuration** > **iDRAC**.
2. Sur la page **Déployer iDRAC**, dans la section **Paramètres QuickDeploy**, spécifiez les paramètres indiqués dans le tableau suivant. Pour plus d'informations sur les champs, voir l'*aide en ligne*.

Tableau 18. Paramètres de QuickDeploy

Réglage	Description
Action à l'insertion du serveur	Sélectionnez l'une des options suivantes dans la liste : · Aucune action : aucune action n'est effectuée lors de l'insertion du serveur. · QuickDeploy uniquement : sélectionnez cette option pour appliquer les paramètres réseau d'iDRAC lorsqu'un nouveau serveur est inséré dans le châssis. Les paramètres de déploiement automatique spécifiés sont utilisés pour configurer le nouvel iDRAC, y compris le mot de passe de l'utilisateur root si l'option Modifier le mot de passe root est sélectionnée. · Profil de serveur uniquement : sélectionnez cette option pour appliquer un profil de serveur attribué lorsqu'un nouveau serveur est inséré dans le châssis. · Déploiement rapide et profil de serveur : sélectionnez cette option pour appliquer les paramètres réseau d'iDRAC, puis le profil de serveur attribué lorsqu'un nouveau serveur est inséré dans le châssis. .
Définir le mot de passe Root d'iDRAC lors de l'insertion du serveur	Sélectionnez l'option de changement du mot de passe root iDRAC pour qu'il corresponde au mot de passe du champ **Mot de passe root iDRAC** lorsqu'un serveur est inséré.
Mot de passe Root d'iDRAC	Si vous sélectionnez les options **Définir le mot de passe root iDRAC lors de l'insertion du serveur** et **QuickDeploy activé**, cette valeur de mot de passe est affectée au mot de passe de l'utilisateur root iDRAC d'un serveur lorsque vous

Tableau 18. Paramètres de QuickDeploy (suite)

Réglage	Description
	insérez le serveur dans le châssis. Ce mot de passe peut contenir de 1 à 20 caractères imprimables (espaces comprises).
Confirmez le mot de passe Root d'iDRAC	Permet d'entrer de nouveau le mot de passe fourni dans le champ **Mot de passe**.
Activer le LAN pour iDRAC	Active ou désactive le canal iDRAC LAN. Par défaut, cette option est désélectionnée.
Activer IPv4 pour iDRAC	Active ou désactive l'IPv4 sur iDRAC. Par défaut, cette option est sélectionnée.
Activer IPMI sur le LAN pour iDRAC	Active ou désactive la fonction IPMI sur canal LAN pour chaque iDRAC présent dans le châssis. Par défaut, cette option est sélectionnée.
Activer le protocole DHCP IPv4 pour iDRAC	Active ou désactive DHCP pour chaque iDRAC présent dans le châssis. Si cette option est activée, les champs **IP de QuickDeploy**, **Masque de sous-réseau de QuickDeploy** et **Passerelle de QuickDeploy** sont désactivés et ne peuvent pas être modifiés car DHCP est utilisé pour attribuer automatiquement ces paramètres à chaque iDRAC. Pour sélectionner cette option, vous devez sélectionner l'option **Activer IPv4 pour iDRAC**. L'adresse IP de QuickDeploy est fournie avec deux options : 2 et 4.
Première adresse IPv4 d'iDRAC (logement 1)	Spécifie l'adresse IP statique de l'iDRAC du serveur installé dans le logement 1 du boîtier. L'adresse IP de chacun des iDRAC suivants est incrémentée de 1 pour chaque logement, à partir de l'adresse IP statique du logement 1. Lorsque la valeur « adresse IP plus numéro de logement » est supérieure au masque de sous-réseau, un message d'erreur s'affiche. **REMARQUE : Le masque de sous-réseau et la passerelle ne sont pas incrémentés comme l'adresse IP.** Par exemple, si l'adresse IP de départ est `192.168.0.250` et que le masque de sous-réseau est `255.255.0.0` alors l'adresse IP de QuickDeploy pour le logement 15 est `192.168.0.265`. Si le masque de sous-réseau est `255.255.255.0`, le message d'erreur `QuickDeploy IP address range is not fully within QuickDeploy Subnet` s'affiche lorsque vous cliquez sur **Enregistrer les paramètres QuickDeploy** ou **Remplir automatiquement avec les paramètres QuickDeploy**.
Masque de réseau IPv4 d'iDRAC	Spécifie le masque de sous-réseau QuickDeploy assigné à tout serveur nouvellement inséré.
Passerelle IPv4 d'iDRAC	Définit la passerelle par défaut QuickDeploy affectée à l'ensemble du module DRAC présent dans le châssis.
Activer IPv6 pour iDRAC	Active l'adressage IPv6 pour chaque contrôleur iDRAC présent dans le châssis prenant en charge IPv6.
Activer la configuration automatique IPv6 d'iDRAC	Permet à l'iDRAC d'obtenir les paramètres IPv6 (adresse et longueur de préfixe) auprès d'un serveur DHCPv6 et autorise également la configuration automatique des adresses sans état. Par défaut, cette option est activée.
Passerelle IPv6 d'iDRAC	Spécifie la passerelle IPv6 à attribuer aux iDRAC. La valeur par défaut est « :: ».
Longueur du préfixe IPv6 d'iDRAC	Spécifie la longueur de préfixe à attribuer pour les adresses IPv6 de l'iDRAC. La valeur par défaut est 64.
Utilisez les paramètres DNS du CMC	Communiquez les paramètres du serveur DNS du CMC (IPv4 et IPv6) à l'iDRAC lorsqu'un serveur lame est inséré au châssis.
Activer le nom DNS d'iDRAC	Sélectionnez Activer le nom DNS d'iDRAC pour appliquer le préfixe du nom DNS d'iDRAC aux serveurs lames insérés dans le châssis. Par défaut, l'option Activer le nom DNS d'iDRAC est désactivée.
Nom DNS d'iDRAC (préfixe)	Vous pouvez configurer le préfixe du nom DNS d'iDRAC uniquement si l'option Activer le nom DNS d'iDRAC est sélectionnée. Le préfixe du nom DNS peut contenir au maximum 59 caractères et au minimum un caractère. Les caractères pris en charge sont les suivants :

Tableau 18. Paramètres de QuickDeploy (suite)

Réglage	Description
	• Alphanumériques : « a-b » ou « A-B » • Numériques : 0-9 • Tiret : « - » Assurez-vous que le préfixe du nom DNS ne commence pas par un tiret. Le préfixe par défaut est « idrac ». Seul le préfixe du nom DNS d'iDRAC est stocké dans le profil de serveur.

3. Cliquez sur **Enregistrer les paramètres QuickDeploy** pour mémoriser les valeurs. Si vous avez modifié les paramètres réseau de l'iDRAC, cliquez sur **Appliquer les paramètres réseau d'iDRAC** pour déployer les paramètres vers l'iDRAC.

   La fonction QuickDeploy est exécutée uniquement si elle est activée et si un serveur est inséré dans le châssis. Si **Définir le mot de passe Root d'iDRAC lors de l'insertion du serveur** et **QuickDeploy activé** sont activées, l'utilisateur est invité à utiliser l'interface LCD pour autoriser ou interdire la modification du mot de passe. S'il existe des paramètres de configuration réseau qui diffèrent des paramètres de l'iDRAC actuels, l'utilisateur est invité à accepter ou rejeter les modifications.

   REMARQUE : S'il existe un LAN ou une différence IPMI sur LAN, l'utilisateur est invité à accepter le paramètre d'adresse IP de QuickDeploy. Si la différence est le paramètre DHCP, l'utilisateur est invité à accepter le paramètre DHCP de QuickDeploy.

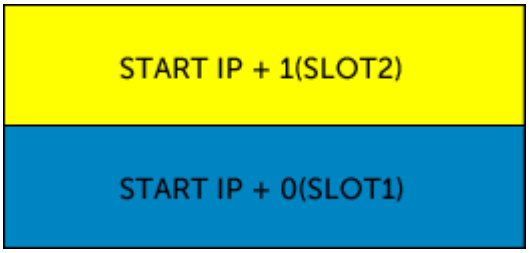
   Pour copier les paramètres QuickDeploy vers la section **Paramètres réseau iDRAC**, cliquez sur **Remplir automatiquement avec les paramètres QuickDeploy**. Les paramètres de configuration réseau QuickDeploy sont copiés vers les champs correspondants de la table **Paramètres de configuration réseau iDRAC**.

   REMARQUE : Les modifications apportées aux champs QuickDeploy sont immédiates, mais les modifications apportées à un ou plusieurs paramètres de configuration réseau du serveur de l'iDRAC peuvent nécessiter quelques minutes pour se propager du CMC vers l'iDRAC. Le fait de cliquer trop tôt sur Actualiser pourrait n'afficher que des données partiellement correctes pour un ou plusieurs serveurs de l'iDRAC.

Affectation d'adresses IP QuickDeploy aux serveurs

Cette illustration montre l'attribution des adresses IP QuickDeploy aux serveurs lorsqu'il existe quatre serveurs demi-hauteur dans le châssis VRTX :

L'illustration suivante montre l'affectation des adresses IP QuickDeploy aux serveurs lorsqu'il existe deux lames standard un châssis VRTX :



Modification des paramètres réseau iDRAC de chaque iDRAC de serveur

À l'aide de cette fonctionnalité, vous pouvez définir les paramètres de configuration réseau iDRAC de chaque serveur installé. Les valeurs initiales affichées pour chaque champ correspondent aux valeurs actuelles lues à partir de l'iDRAC. Pour utiliser cette fonction, vous devez disposer d'une licence d'entreprise.

Pour modifier les paramètres réseau iDRAC7 :

1. Dans le volet de gauche, cliquez sur **Présentation du serveur** et sur **Configurer**. Sur la page**Déployer iDRAC**, la section **Paramètres de réseau iDRAC** répertorie le nom DNS d'iDRAC, ainsi que les paramètres de configuration réseau IPv4 et IPv6 de tous les serveurs installés.
2. Modifiez les paramètres réseau iDRAC selon vos besoins pour le ou les serveurs.

   REMARQUE : Vous devez sélectionner l'option Activer le LAN pour spécifier les paramètres IPv4 ou IPv6. Pour plus d'informations sur les champs, consultez l'*Aide en ligne*.

3. Pour déployer le paramètre sur iDRAC, cliquez sur **Appliquer les paramètres réseau d'iDRAC**. Toutes les modifications apportées aux **Paramètres QuickDeploy** sont également enregistrées.

   Le tableau **Paramètres réseau d'iDRAC** reflète les futurs paramètres de configuration réseau. Les valeurs affichées pour les serveurs installés peuvent ou non être identiques aux paramètres de configuration réseau iDRAC actuellement installés. Cliquez sur **Actualiser** pour mettre à jour la page **Déployer iDRAC** avec chaque paramètre de configuration réseau iDRAC installé une fois les modifications effectuées.

   REMARQUE : Les modifications apportées aux champs QuickDeploy sont immédiates, mais celles apportées à un ou plusieurs paramètres de configuration réseau du serveur de l'iDRAC peuvent nécessiter quelques minutes pour se propager du CMC vers l'iDRAC. Le fait de cliquer trop tôt sur Actualiser pourrait n'afficher que des données partiellement correctes pour un ou plusieurs serveurs de l'iDRAC.

Modification des paramètres réseau iDRAC avec RACADM

Les commandes RACADM `config` et `getconfig` prennent en charge l'option `-m <module>` pour les groupes de configuration suivants :

- `cfgLanNetworking`
- `cfgIPv6LanNetworking`
- `cfgRacTuning`
- `cfgRemoteHosts`
- `cfgSerial`
- `cfgSessionManagement`

Pour plus d'informations sur les valeurs par défaut des propriétés et les plages, voir le document *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* sur le site **dell.com/support/manuals**.

Configuration des paramètres de balise du LAN virtuel iDRAC

Les balises de LAN virtuel (VLAN) permettent à plusieurs LAN virtuels de coexister sur le même câble réseau physique et de séparer le trafic réseau pour des raisons de sécurité ou de gestion de la charge. Lorsque vous activez la fonction VLAN, chaque paquet réseau reçoit une balise VLAN. Les balises VLAN sont des propriétés de châssis. Elles demeurent associées au châssis même lorsque vous retirez un composant.

REMARQUE : L'ID VLAN configuré à l'aide du CMC est appliqué à l'iDRAC uniquement lorsque l'iDRAC est en mode dédié. Si l'iDRAC est en mode LOM partagé, les modifications de l'ID VLAN effectuées dans l'iDRAC ne sont pas affichées dans l'interface du CMC.

Configuration des paramètres de numéro du LAN virtuel d'iDRAC avec la RACADM

- Spécifiez l'ID de VLAN virtuel et la priorité d'un serveur particulier avec la commande suivante :

  ```
  racadm setniccfg -m server-<n> -v <VLAN id> <VLAN priority>
  ```

  Les valeurs valides de <*n*> sont comprises entre 1 et 4.

  Les valeurs valides de <*VLAN*> sont comprises ent re 1 et 4 000 et 4 021 et 4 094. La valeur par défaut est 1.

  Les valeurs valides de <*VLAN priority*> sont comprises entre 0 et 7. La valeur par défaut est 0.

  Par exemple :

  ```
  racadm setniccfg -m server-1 -v 1 7
  ```

  Par exemple :

  ```
  
  ```

- Pour supprimer un VLAN de serveur, désactivez les fonctions VLAN du réseau du serveur spécifié :

  ```
  racadm setniccfg -m server-<n> -v
  ```

  Les valeurs valides de <*n*> sont comprises entre 1 et 4.

  Par exemple :

  ```
  racadm setniccfg -m server-1 -v
  ```

Configuration des paramètres de balise VLAN iDRAC à l'aide de l'interface Web

Pour configurer le LAN virtuel (VLAN) pour le serveur :

1. Accédez à l'une des pages suivantes :
   - Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Réseau** > **VLAN**.
   - Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Présentation du serveur** et cliquez sur**Configurer** > **VLAN**.
2. Sur la page **Paramètres de balise VLAN**, dans la section **iDRAC**, activez VLAN pour le ou les serveurs, définissez la priorité et entrez l'ID. Pour plus d'informations sur les champs, voir l'*Aide en ligne*.
3. Cliquez sur **Appliquer** pour enregistrer les paramètres.

Définition du premier périphérique de démarrage

Vous pouvez définir le premier périphérique de démarrage CMC de chaque serveur. Ce périphérique peut ne pas correspondre au premier périphérique de démarrage du serveur ou peut même ne pas représenter un périphérique présent dans le serveur. Il représente un périphérique envoyé par le contrôleur CMC au serveur, qui est utilisé comme premier périphérique de démarrage du serveur. Ce périphérique peut être défini comme premier périphérique de démarrage par défaut ou comme périphérique utilisable une seule fois pour pouvoir démarrer une image afin d'exécuter des tâches, telles qu'exécuter des diagnostics ou réinstaller un système d'exploitation.

Vous pouvez définir le premier périphérique de démarrage pour le démarrage suivant uniquement ou pour tous les démarrages suivants. Vous pouvez également définir le premier périphérique de démarrage du serveur. Le système démarre depuis le périphérique sélectionné lors du redémarrage suivant et des redémarrages ultérieurs, et ce périphérique reste le premier périphérique de démarrage dans la séquence de démarrage du BIOS tant que vous ne le changez pas dans l'interface Web CMC (**Présentation du châssis** > **Présentation du serveur** > **Configuration** > **Premier périphérique de démarrage** ou dans la séquence de démarrage du BIOS.

REMARQUE : Le paramètre de premier périphérique de démarrage défini dans l'interface Web CMC remplace les paramètres de démarrage du BIOS système.

Le périphérique de démarrage que vous définissez doit exister et contenir un support amorçable.

Vous pouvez définir les périphériques suivants comme premier périphérique de démarrage.

Tableau 19. Périphériques de démarrage

Périphérique de démarrage	Description
PXE	Démarrage à partir d'un protocole PXE (environnement d'exécution prédémarrage) sur la carte d'interface réseau.
Disque dur	Démarrage à partir du disque dur sur le serveur.
CD/DVD local	Démarrage à partir d'un lecteur de CD/DVD sur le serveur.
Disquette virtuelle	Démarrage sur le lecteur de disquette virtuel. Ce lecteur de disquette (ou image de disquette) se trouve sur un autre ordinateur du réseau de gestion et est rattaché via la visionneuse de console de l'interface utilisateur graphique (GUI) iDRAC.
CD/DVD virtuel	Démarrage depuis un lecteur de CD/DVD virtuel ou une image ISO de CD/DVD. Ce lecteur optique ou cette image ISO se trouve sur un autre ordinateur ou disque de démarrage disponible sur le réseau de gestion, et il est rattaché via la visionneuse de console de l'interface utilisateur graphique iDRAC.
Carte SD locale	Démarrage depuis la carte locale SD (Secure Digital) : uniquement pour les serveurs prenant en charge les systèmes iDRAC6 et iDRAC7.
Disquette locale	Démarrage à partir d'une disquette insérée dans le lecteur local de disquette.
Partage de fichier à distance	Démarrage à partir d'une image RFS (Remote File Share). Ce fichier d'image de disquette est rattaché via la visionneuse de console de l'interface utilisateur graphique (GUI) iDRAC.

Définition du premier périphérique d'amorçage pour plusieurs serveurs dans l'interface Web CMC

REMARQUE : Pour définir le premier périphérique d'amorçage des serveurs, vous devez disposer des privilèges Administrateur de serveur ou Administrateur de configuration du châssis, ainsi que les privilèges Connexion à l'iDRAC.

Pour définir le premier périphérique d'amorçage de plusieurs serveurs :

1. Dans le volet de gauche, cliquez sur **Présentation du serveur** > **Configurer** > **Premier périphérique d'amorçage**. La liste des serveurs s'affiche.
2. Dans la colonne **Premier périphérique d'amorçage**, dans le menu déroulant d'un serveur, sélectionnez le périphérique d'amorçage à utiliser pour le serveur.
3. Si vous souhaitez que le serveur s'amorce sur le périphérique sélectionné à chaque amorçage, désélectionnez l'option **Démarrer une seule fois** pour le serveur. Pour que le serveur s'amorce sur le périphérique sélectionné uniquement pour le prochain cycle d'amorçage, sélectionnez l'option **Démarrer une seule fois** pour le serveur concerné.
4. Cliquez sur **Appliquer** pour enregistrer les paramètres.

Définition du premier périphérique d'amorçage pour un seul serveur dans l'interface Web CMC

REMARQUE : Pour définir le premier périphérique d'amorçage pour les serveurs, vous devez posséder les privilèges Administrateur du serveur ou Administrateur de configuration du châssis, ainsi que les privilèges Connexion à l'iDRAC.

Pour définir le premier périphérique d'amorçage de chaque serveur :

1. Dans le volet de gauche, cliquez sur **Présentation du serveur** et sur le serveur dont vous voulez définir le premier périphérique d'amorçage.
2. Accédez à **Configuration** > **Périphérique de démarrage initial**. La page **Périphérique de démarrage initial** s'affiche.
3. Dans le menu déroulant **Périphérique de démarrage initial**, sélectionnez le périphérique d'amorçage à utiliser pour chaque serveur.
4. Si vous souhaitez que le serveur s'amorce sur le périphérique sélectionné à chaque amorçage, désélectionnez l'option **Démarrer une seule fois** pour le serveur. Pour que le serveur s'amorce sur le périphérique sélectionné uniquement pour le prochain cycle d'amorçage, sélectionnez l'option **Démarrer une seule fois** pour le serveur concerné.

5. Cliquez sur **Appliquer** pour enregistrer les paramètres.

Définition du premier périphérique de démarrage à l'aide de l'interface RACADM

Pour définir le premier périphérique de démarrage, utilisez l'objet `cfgServerFirstBootDevice`.

Pour activer un seul démarrage pour un périphérique, utilisez l'objet `cfgServerBootOnce`.

Pour plus d'informations sur ces objets, voir le *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX) sur le site dell.com/support/manuals.

Configuration de FlexAddress pour serveur

Pour plus d'informations sur la configuration de FlexAddress pour les serveurs, voir la rubrique Configuration de FlexAddress pour la structure au niveau châssis et des logements à l'aide de l'interface Web CMC. Pour utiliser cette fonction, vous devez disposer d'une licence d'entreprise.

Configuration d'un partage de fichiers distant

La fonction Remote Virtual Media File Share (partage de fichiers sur support virtuel distant) permet de mapper un fichier d'un disque partagé du réseau vers un ou plusieurs serveurs via le contrôleur CMC afin de déployer ou de mettre à jour un système d'exploitation. Une fois la connexion établie, le fichier distant est accessible comme s'il se trouvait sur un serveur local. Deux types de médias sont pris en charge : les disquettes et les CD/DVD.

Pour effectuer une opération de partage de fichiers distant (connexion, déconnexion ou déploiement), vous devez disposer de droits d'**Administrateur de configuration du châssis** ou d'**Administrateur de serveur**. Pour utiliser cette fonction, vous devez disposer d'une licence d'entreprise.

REMARQUE : Si vous utilisez CIFS et faites partie d'un domaine Active Directory, entrez le nom de domaine et l'adresse IP dans le chemin d'accès du fichier image.

Pour configurer le partage de fichier distant :

1. Dans le volet de gauche, cliquez sur **Présentation du serveur** > **Configurer** > **Partage de fichiers distants**.
2. Sur la page **Déployer le partage de fichiers distant**, saisissez les données appropriées dans les champs. Pour plus d'informations sur les descriptions de champs, voir l'*Aide en ligne*.
3. Pour vous connecter à un partage de fichiers distant, cliquez sur **Se connecter**. Pour vous connecter à un partage de fichiers distant, vous devez indiquer le chemin d'accès, le nom d'utilisateur et le mot de passe. La réussite de l'opération vous permet d'accéder aux médias.

   Cliquez sur **Déconnecter** pour vous déconnecter d'un partage de fichiers distant précédemment connecté.

   Cliquez sur **Déployer** pour déployer le périphérique du média.

   REMARQUE : Avant de cliquer sur le bouton Déployer, veillez à enregistrer tous les fichiers de travail, car cette action redémarre le serveur.

   Lorsque vous cliquez sur Déployer ; les tâches suivantes sont exécutées :

   - **Le partage de fichiers distant est connecté.**
   - **Le fichier est sélectionné en tant que premier périphérique de démarrage pour les serveurs.**
   - **Le serveur est redémarré.**
   - **Le serveur est mis sous tension s'il est hors tension.**

Configuration des paramètres de profil à l'aide de la réplication de la configuration de serveur

La fonction de réplication des configurations de serveur vous permet d'appliquer tous les paramètres de profil depuis un serveur particulier à un ou plusieurs serveurs. Les paramètres de profil qui peuvent être répliqués sont ceux qui peuvent être modifiés et qui doivent être répliqués à travers les serveurs. Les trois groupes de profils de serveurs s'affichent et peuvent être répliqués :

- BIOS : ce groupe inclut uniquement les paramètres BIOS d'un serveur. Ces profils sont générés par CMC pour PowerEdge VRTX version 1.00 et version ultérieure.
- BIOS et de l'amorçage : ce groupe contient les paramètres du BIOS et de l'amorçage d'un serveur. Ces profils sont générés par CMC pour PowerEdge VRTX version 1.00 et version ultérieure.
- Tous les paramètres : cette version contient tous les paramètres du serveur et de ses composants. Ces profils sont générés depuis :
  - CMC pour PowerEdge VRTX version 1.00 et version ultérieure
  - Serveurs de 12e génération avec iDRAC7 1.00.00 ou version ultérieure et Lifecycle Controller 2 version 1.1 ou ultérieure
  - Serveurs de 13è génération avec iDRAC8 avec Lifecycle Controller 2.00.00.00 ou version ultérieure

La fonction de réplication de configuration de serveur prend en charge les serveurs iDRAC et les serveurs ultérieurs. Les serveurs RAC de génération antérieure sont répertoriés, mais ils sont grisés sur la page principale, et vous ne pouvez pas utiliser cette fonction.

Pour utiliser la fonction de réplication des configurations de serveur :

- iDRAC doit correspondre à la version minimale requise.
- Le serveur doit être sous tension.

Vous pouvez :

- Afficher les paramètres du profil d'un serveur ou ceux d'un profil enregistré.
- Enregistrer le profil d'un serveur.
- Appliquer un profil à d'autres serveurs.
- Importer les profils stockés depuis un poste de gestion ou d'un partage de fichiers distant.
- Modifier le nom du profil et sa description.
- Exporter les profils stockés vers un poste de gestion ou un partage de fichiers distant.
- Supprimer les profils stockés.
- Déployer les profils sélectionnés vers les périphériques cibles à l'aide de l'option **Déploiement rapide**.
- Afficher les activités dans le journal pour des tâches récentes d'un profil de serveur.

Accéder à la page Profils de serveur

Vous pouvez ajouter et gérer des profils de serveur et les appliquer à un ou plusieurs serveurs à l'aide de la page **Profils de serveur**.

Pour accéder à la page **Profils de serveur** à l'aide de l'interface Web CMC, dans le volet gauche, accédez à **Présentation du châssis** **Présentation du serveur**. Cliquez sur **Configuration Profils**. La page **Profils de serveur**s'affiche.

Ajout ou enregistrement d'un profil

Avant de copier les propriétés d'un serveur, vous devez capturer les propriétés dans un profil stocké. Créez un profil stocké et indiquez le nom et entrez la description facultative de chaque profil. Vous pouvez enregistrer un maximum de 16 profils stockés sur le support de stockage étendu non volatile CMC.

REMARQUE : Si un partage distant est disponible, vous pouvez stocker un maximum de 100 profils en utilisant le stockage étendu CMC et le partage distant. Pour plus d'informations, reportez-vous à la section Configuration d'un partage réseau en utilisant l'interface Web CMC.

La suppression ou la désactivation du support de stockage étendu non volatile empêche l'accès aux profils stockés et désactive la fonction de réplication de configuration de serveur.

Pour ajouter ou enregistrer un profil :

1. Dans la page **Profils de serveur**, dans la section **Profils stockés**, cliquez sur **Appliquer et enregistrer les profils**.
2. Sélectionnez le serveur à partir duquel vous voulez générer le profil depuis ses paramètres, puis cliquez sur **Enregistrer le profil**. La section **Enregistrer un profil** s'affiche.
3. Sélectionnez **Stockage étendu** ou **Partage réseau** comme emplacement pour enregistrer le profil.

REMARQUE : L'option Partage réseau est activée et les détails s'affichent dans la section Profils stockés uniquement si le partage réseau est monté et accessible. Si le partage réseau n'est pas connecté, configurez-le pour le châssis. Pour ce faire, cliquez sur Modifier dans la section Profils stockés. Pour plus d'informations sur la configuration du partage réseau, reportez-vous à la section Configuration du partage réseau en utilisant l'interface Web CMC.

4. Dans les champs **Nom du profil** et **Description**, entrez le nom du profil et sa description (facultative), puis cliquez sur **Enregistrer le profil**.

   REMARQUE : Lors de la sauvegarde d'un profil de serveur, le jeu de caractères ASCII étendus standard est pris en charge. Toutefois, les caractères spéciaux suivants ne sont pas pris en charge :

   ), “, ., *, >, <, \, /, :, |, #, ?, et ,

   CMC communique avec le LC pour obtenir les paramètres de profil disponibles et les stocker dans un profil nommé.

   Un indicateur de progression montre que l'opération d'enregistrement est en cours. Lorsque l'action est terminée, le message « Opération réussie » s'affiche.

   REMARQUE : Le processus de collecte des paramètres s'exécute en arrière-plan. Par conséquent, le nouveau profil peut prendre un certain temps pour s'afficher. Si le nouveau profil ne s'affiche pas, recherchez les erreurs dans le journal du profil.

Application d'un profil

La réplication de la configuration de serveur est possible uniquement si les profils de serveur sont disponibles en tant que profils stockés dans le support non volatil sur le CMC ou stockés sur le partage distant. Pour lancer une opération de réplication de configuration de serveur, vous pouvez appliquer un profil stocké à un ou plusieurs serveurs.

REMARQUE : Si un serveur ne prend pas en charge le Lifecycle Controller de Dell ou que le châssis est hors tension, vous ne pouvez pas appliquer de profil au serveur.

Pour appliquer un profil à un ou plusieurs serveurs :

1. Accédez à la page **Profils de serveur**. Dans la section **Enregistrer et appliquer des profils**, sélectionnez les serveurs auxquels vous voulez appliquer le profil sélectionné.
   Le menu déroulant **Sélectionner le profil** est activé.

   REMARQUE : Le menu déroulant Sélectionner le profil affiche tous les profils disponibles, triés par type, y compris ceux qui se trouvent sur le partage distant et la carte SD.

2. Depuis le menu déroulant **Sélectionner un profil**, sélectionnez le profil à appliquer.
   L'option **Appliquer le profil** est activée.
3. Cliquez sur **Appliquer le profil**.

   Un message vous indique que l'application d'un nouveau profil de serveur écrase les paramètres actuels et redémarre également les serveurs sélectionnés. Vous êtes invité à confirmer si vous souhaitez poursuivre l'opération.

   REMARQUE : Pour effectuer des opérations de clonage de serveur sur les serveurs, vous devez activer l'option CSIOR pour les serveurs. Si l'option CSIOR est désactivée, un message d'avertissement vous indique que l'option CSIOR n'est pas activée pour les serveurs. Pour effectuer l'opération de clonage de lame, assurez-vous d'activer l'option CSIOR sur les serveurs.

4. Cliquez sur **OK** pour appliquer le profil au serveur sélectionné.

   Le profil sélectionné est appliqué au ou aux serveurs et celui-ci ou ceux-ci sont redémarrés immédiatement, si nécessaire. Pour plus d'informations, voir l'*Aide en ligne CMC*.

Importation de profil

Vous pouvez importer vers CMC un profil de serveur qui est stocké sur une station de gestion.

Pour importer un profil stocké depuis CMC :

1. Dans la page **Profils de serveur**, dans la section **Profils stockés**, cliquez sur **Importer un profil**.
   La section **Importer un profil de serveur** s'affiche.
2. Cliquez sur **Parcourir** pour accéder au profil à partir de l'emplacement souhaité, puis cliquez sur **Importer le profil**.

   Pour plus d'informations sur les champs, voir l'*aide en ligne*.

Exportation de profil

Vous pouvez exporter un profil de serveur stocké vers un chemin de dossier de fichiers sur une station de gestion.

Pour exporter un profil stocké :

1. Dans la page **Profils de serveur**, dans la section **Profils stockés**, sélectionnez le profil souhaité, puis cliquez sur **Exporter une copie du profil**.
   La boîte de dialogue **Téléchargement de fichier** qui s'affiche vous invite à ouvrir ou à enregistrer le fichier.
2. Cliquez sur **Enregistrer** ou **Ouvrir** pour exporter le profil vers l'emplacement requis.

   REMARQUE : Si le profil source se trouve sur la carte SD, un message s'affiche pour indiquer que si le profil est exporté, la description est perdue. Cliquez sur OK pour poursuivre l'exportation du profil.

   Un message s'affiche vous invitant à sélectionner la destination du fichier :

   - Partage local ou de réseau si le fichier source se situe sur une carte SD.

     REMARQUE : L'option Partage réseau est activée et les détails s'affichent dans la section Profils stockés uniquement si le partage réseau est monté et accessible. Si le partage réseau n'est pas connecté, configurez-le pour le châssis. Pour ce faire, cliquez sur Modifier dans la section Profils stockés. Pour plus d'informations, reportez-vous à la section Configuration d'un partage réseau en utilisant l'interface Web CMC.
   - Carte locale ou SD si le fichier source se situe sur le partage réseau.

   Pour plus d'informations sur les champs, voir l'*aide en ligne*.
3. Sélectionnez **Stockage local**, **étendu** ou **Partage réseau** comme emplacement de destination sur la base des options qui s'affichent.
   - Si vous sélectionnez l'option **Local**, la boîte de dialogue qui apparaît vous permet d'enregistrer le profil dans un répertoire local.
   - Si vous sélectionnez **Stockage étendu** ou **Partage réseau**, une boîte de dialogue **Enregistrer le profil** s'affiche.
4. Cliquez sur **Enregistrer le profil** pour enregistrer le profil vers l'emplacement sélectionné.

REMARQUE : L'interface Web CMC capture le profil de configuration normal du serveur (instantané du serveur), qui peut être utilisé pour la réplication sur un système cible. Cependant, certaines configurations comme celles de RAID et des attributs d'identité ne sont pas propagées vers le nouveau serveur. Pour plus d'informations sur les autres modes d'exportation pour les configurations de RAID et des attributs d'identité, consultez le livre blanc, *Clonage de serveur avec des profils de configuration de serveur*, à l'adresse DellTechCenter.com.

Modification d'un profil

Vous pouvez modifier le nom et la description d'un profil de serveur stocké sur le support CMC non volatile (carte SD), ou le nom d'un profil de serveur stocké sur le partage distant.

Pour modifier un profil stocké :

1. Dans la page **Profils de serveur**, dans la section **Profils stockés**, sélectionnez le profil souhaité, puis cliquez sur **Modifier le profil**.
   La section **Modifier le profil du serveur — <Profile Name>** s'affiche.
2. Modifiez le nom et la description du profil de serveur, puis cliquez sur **Modifier le profil**.

   REMARQUE : Vous pouvez modifier la description du profil uniquement pour les profils stockés sur des cartes SD.

   Reportez-vous à *l'Aide en ligne* pour plus d'informations.

Suppression d'un profil

Vous pouvez supprimer un profil de serveur stocké sur le support CMC non volatile (carte SD) ou sur le partage réseau.

Pour supprimer un profil stocké :

1. Dans la page **Profils de serveur**, dans la section **Profils stockés**, sélectionnez le profil souhaité, puis cliquez sur **Supprimer le profil**.
   Un message d'avertissement s'affiche, indiquant que la suppression d'un profil supprime définitivement le profil sélectionné.
2. Cliquez sur **OK** pour supprimer le profil sélectionné.
   Reportez-vous à *l'Aide en ligne* pour plus d'informations.

Affichage des paramètres de profil

Pour afficher les paramètres de profil d'un serveur sélectionné, accédez à la page **Profils de serveur**. Dans la section **Profils de serveur**, cliquez sur **Afficher** dans la colonne **Profil du serveur** du serveur approprié. La page **Afficher les paramètres** s'affiche.

Pour en savoir plus sur les paramètres affichés, voir l'*aide en ligne*.

REMARQUE : La fonction de réplication de la configuration du serveur CMC récupère et affiche les paramètres d'un serveur particulier, uniquement si l'option Collecte de l'inventaire système au redémarrage (CSIOR) est activée.

Pour activer CSIOR :

- Serveurs 12e génération : après avoir redémarré le serveur, lorsque le logo de la société s'affiche, appuyez sur F2. Sur la page des **paramètres iDRAC** , dans le volet gauche, cliquez sur **Lifecycle Controller**, puis sur **CSIOR** pour que les modifications soient appliquées.
- Serveurs de 13e génération : après avoir redémarré le serveur, lorsque vous y êtes invité, appuyez sur F10 pour accéder au Lifecycle Controller. Allez à la page **Inventaire du matériel** en cliquant sur **Configuration matérielle** > **Inventaire du matériel**. Sur la page **Inventaire du matériel**, cliquez sur **Collecter l'inventaire système au redémarrage**.

Affichage des paramètres de profil stocké

Pour afficher les paramètres des profils de serveur stockés, accédez à la page **Profils de serveur**. Dans la section **Profils stockés**, cliquez sur **Afficher** dans la colonne **Afficher le profil** du profil de serveur souhaité. La page **Afficher les paramètres** s'affiche. Pour plus d'informations sur les paramètres affichés, voir l'*Aide en ligne*.

Affichage du journal de profil

Pour afficher le journal de profil, dans la page **Profils de serveur**, voir la section **Journal de profil récent**. Cette section répertorie les 10 dernières entrées du journal de profil directement depuis les opérations de configuration du serveur. Chaque entrée du journal affiche la gravité, l'heure et la date de soumission de l'opération de configuration de serveur, ainsi que la description des messages du journal de réplication. Les entrées du journal sont également disponibles dans le journal RAC. Pour afficher les autres entrées disponibles, cliquez sur **Aller au journal de profil**. La page **Journal de profil** s'affiche. Pour en savoir plus, voir l'*Aide en ligne*.

Statut d'achèvement et dépannage

Pour vérifier la condition d'achèvement de l'application d'un profil BIOS :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Présentation du serveur** > **Configurer** > **Profils**.
2. Dans la page **Profils de serveur**, notez l'ID de la tâche soumise (JID) dans la section **Journal de profil récent**.
3. Dans le volet de gauche, cliquez sur **Présentation du serveur** > **Dépannage** > **Tâches Lifecycle Controller**. Recherchez la même JID (Identification de tâche) dans le tableau **Tâches**. Pour plus d'informations sur l'exécution des tâches Lifecycle Controller à l'aide du contrôleur CMC, voir Opérations des tâches Lifecycle Controller.
4. Cliquez sur le lien **Afficher le journal** pour afficher les résultats de *Lclogview* du Lifecycle Controller de l'iDRAC du serveur spécifique. Les résultats de fin ou d'échec affichés sont similaires aux informations du serveur spécifique affichées dans le journal du Lifecycle Controller de l'iDRAC.

Profils de déploiement rapide

La fonction de déploiement rapide (Quick Deploy) permet d'attribuer un profil stocké à un logement de serveur. Tout serveur inséré dans ce logement prenant en charge la réplication de configuration de serveur est configuré à l'aide du profil attribué au logement. Vous pouvez exécuter l'action de déploiement rapide uniquement si l'option **Action lorsque le serveur est inséré** qui figure dans la page **Déployer iDRAC** a la valeur **Profil de serveur** ou **Déploiement rapide et profil de serveur**. La sélection de cette option permet d'appliquer le profil de serveur affecté lorsqu'un nouveau serveur est inséré dans le châssis. Pour accéder à la page **Déployer iDRAC**, sélectionnez **Présentation du serveur** > **Configuration** > **iDRAC**. Les profils pouvant être déployés se trouvent sur la carte SD ou le partage distant. Pour configurer les profils pour le déploiement rapide, vous devez détenir les privilèges d'**Administrateur de châssis**.

REMARQUE :

Attribution de profils de serveur à des logements

La page **Profils de serveur** vous permet d'attribuer des profils de serveur à des logements. Pour attribuer un profil à des logements de châssis :

1. Dans la page **Profils de serveur** , cliquez sur **Profils pour QuickDeploy** .
   Les attributions de profil actuelles s'affichent pour les logements dans les cases de sélection contenues dans la colonne **Attribuer un profil**.
   REMARQUE : Vous pouvez exécuter l'action Quick Deploy uniquement si l'option Action lorsque le serveur est inséré dans la page Déployer iDRAC a la valeur Profil du serveur ou Déploiement rapide et profil du serveur. La sélection de cette option permet d'appliquer le profil de serveur affecté lorsqu'un nouveau serveur est inséré dans le châssis.
2. Dans le menu déroulant, sélectionnez le profil à attribuer au logement requis. Vous pouvez sélectionner un profil à appliquer à plusieurs logements.
3. Cliquez sur **Attribuer un profil**.
   Le profil est attribué aux logements sélectionnés

REMARQUE :

- **Un logement auquel aucun profil n'est appliqué est désigné par le terme « Aucun profil sélectionné » qui apparaît dans la case sélectionnée.**
- **Pour supprimer une attribution de profil d'un ou de plusieurs logements, sélectionnez les logements, puis cliquez sur Supprimer l'attribution. Un message s'affiche pour indiquer que la suppression d'un profil d'un ou de plusieurs emplacements supprime les paramètres de configuration dans le profil d'un ou de plusieurs serveurs insérés dans le ou les logements lors de l'activation de la fonction Profils de déploiement rapide. Cliquez sur OK pour supprimer les attributions de profil.**
- **Pour supprimer toutes les attributions de profil d'un logement, dans la liste déroulante, sélectionnez l'option Aucun profil sélectionné.**

REMARQUE : Lorsqu'un profil est déployé sur un serveur à l'aide de la fonction Profils de déploiement rapide, l'avancement et les résultats de l'application sont consignés dans le journal du profil.

REMARQUE :

- **Si un profil attribué se trouve sur le partage réseau qui n'est pas accessible lorsqu'un serveur est inséré dans le logement, l'écran LCD affiche un message indiquant que le profil attribué n'est pas disponible pour le Logement <X>.**
- **L'option Partage réseau est activée et les détails s'affichent dans la section Profils stockés uniquement si le partage réseau est monté et accessible. Si le partage réseau n'est pas connecté, configurez-le pour le châssis. Pour ce faire, cliquez sur Modifier dans la section Profils stockés. Pour plus d'informations, reportez-vous à la section Configuration d'un partage réseau en utilisant l'interface Web CMC.**

Profils d'identité de démarrage

Pour accéder à la page **Profils d'identité de démarrage** dans l'interface Web CMC, dans l'arborescence système, accédez à **Présentation du châssis** > **Présentation du serveur**. Cliquez sur **Configuration** > **Profils**. La page **Profils de serveur** s'affiche. Sur la page **Profils de serveur**, cliquez sur **Profils d'identité de démarrage**.

Les profils d'identité de démarrage contiennent les paramètres NIC ou FC qui sont nécessaires pour démarrer un serveur à partir d'un périphérique cible SAN et de noms MAC et WWN virtuels uniques. Ces derniers étant disponibles sur plusieurs châssis par le biais d'un partage CIFS ou NFS, vous pouvez rapidement déplacer à distance une identité du serveur non-fonctionnel d'un châssis vers un serveur de rechange situé dans le même châssis ou dans un autre châssis en lui permettant de s'amorcer avec le système d'exploitation et les applications du serveur défaillant. L'avantage principal de cette fonction est l'utilisation d'un pool d'adresses MAC virtuelles unique et partagé par tous les châssis.

Cette fonctionnalité vous permet de gérer le fonctionnement en ligne du serveur, sans intervention physique si le serveur arrête de fonctionner. Vous pouvez effectuer les tâches suivantes à l'aide de la fonction Profils d'identité de démarrage :

- Configuration initiale
  - Créez une plage d'adresses MAC virtuelles. Pour créer une adresse MAC, vous devez disposer des privilèges d'Administrateur de serveur et d'Administrateur de configuration du châssis.
  - Enregistrez les modèles de profil d'identité de démarrage et personnalisez-les sur le partage réseau en modifiant et en incluant les paramètres de démarrage SAN utilisés par chaque serveur.

- Préparez les serveurs qui utilisent la configuration initiale avant l'application de leurs profils d'identité de démarrage.
- Appliquez les profils d'identité de démarrage à chaque serveur et démarrez-les à partir de SAN.

- Configurez un ou plusieurs serveurs de secours auxiliaires pour une reprise rapide.
  - Préparez des serveurs de secours qui utilisent la configuration initiale, avant l'application de leurs profils d'identité de démarrage.
- Utilisez la charge de travail d'un serveur défaillant dans un nouveau serveur en effectuant les tâches suivantes :
  - Effacez l'identité de démarrage du serveur non opérationnel pour éviter la duplication des adresses MAC au cas où le serveur se rétablirait.
  - Appliquez l'identité de démarrage d'un serveur défaillant à un serveur de secours auxiliaire.
  - Démarrez le serveur avec les nouveaux paramètres d'identité de démarrage pour récupérer rapidement la charge de travail.

Enregistrement des profils d'identité de démarrage

Vous pouvez enregistrer des profils d'identité de démarrage sur le partage réseau CMC. Le nombre de profils que vous pouvez stocker dépend de la disponibilité des adresses MAC. Pour plus d'informations, voir la section *Configuration du partage réseau à l'aide de l'interface Web CMC*.

Dans le cas de cartes Emulex Fibre Channel (FC), l'attribut **Activer/Désactiver l'amorçage à partir de SAN** dans la ROM en option est désactivé par défaut. Activez l'attribut dans la ROM en option et appliquez le profil d'identité de démarrage au serveur pour l'amorçage à partir du réseau SAN.

Pour enregistrer un profil, procédez comme suit :

1. Accédez à la page **Profils de serveur**. Dans la section **Profils d'identité de démarrage**, sélectionnez le serveur qui possède les paramètres requis avec lesquels vous souhaitez générer le profil, puis sélectionnez FQDD dans le menu déroulant **FQDD**.
2. Cliquez sur **Enregistrer une identité**. La section **Enregistrer une identité** s'affiche.

   REMARQUE : L'identité de démarrage est enregistrée uniquement si l'option Partage réseau est activée et accessible. Des informations détaillées s'affichent dans la section Profils stockés section. Si le Partage réseau n'est pas connecté, configurez-le pour le châssis. Pour configurer le partage réseau, cliquez sur Modifier dans la section Profils stockés. Pour plus d'informations, voir la section *Configuration du partage réseau via l'interface Web CMC*.

3. Dans les champs **Nom du profil de base** et **Nombre de profils**, entrez le nom du profil et le nombre de profils à enregistrer.

   REMARQUE : Lors de la sauvegarde d'un profil d'identité de démarrage, le jeu de caractères ASCII étendu standard est pris en charge. Toutefois, les caractères spéciaux suivants ne sont pas pris en charge :

   , ,.,*, >, <, \, /, :, |, #, ? et ,

4. Sélectionnez une adresse MAC pour le profil de base dans le menu déroulant **Adresse MAC virtuelle**, puis cliquez sur **Enregistrer le profil**.

   Le nombre de modèles créés dépend du nombre de profils que vous spécifiez. Le CMC communique avec le Lifecycle Controller pour obtenir les paramètres de profil de serveur disponibles et les stocker en tant que profil nommé. Le format pour fichier de nom est — `<base profile name>_<profile number>_<MAC address>`. Par exemple : `FC630_01_0E0000000000`.

   Un indicateur de progression montre que l'opération d'enregistrement est en cours. Une fois l'action terminée, le message **Opération réussie** s'affiche.

   REMARQUE : Le processus permettant de collecter les paramètres s'exécute en arrière-plan. Par conséquent, le nouveau profil peut prendre quelque temps pour s'afficher. Si le nouveau profil ne s'affiche pas, vérifiez le journal de profil pour afficher les erreurs.

Application des profils d'identité de démarrage

Vous pouvez appliquer des paramètres de profil d'identité de démarrage si les profils d'identité de démarrage sont disponibles en tant que profils stockés sur le partage réseau. Pour lancer une opération de configuration d'identité de démarrage, vous pouvez appliquer un profil stocké à un seul serveur.

REMARQUE : Si un serveur ne prend pas en charge le Lifecycle Controller ou si le châssis est hors tension, vous ne pouvez pas appliquer de profil au serveur.

Pour appliquer un profil à un serveur, procédez comme suit :

1. Accédez à la page **Profils de serveur**. Dans la section **Profils d'identité de démarrage**, sélectionnez le serveur auquel vous souhaitez appliquer le profil sélectionné.
   Le menu déroulant **Sélectionner le profil** est activé.

REMARQUE : Le menu déroulant Sélectionner un profil affiche tous les profils disponibles qui sont triés par type dans le partage réseau.

2. Depuis le menu déroulant **Sélectionner un profil**, sélectionnez le profil à appliquer.
   L'option **Appliquer l'identité** est activée.
3. Cliquez sur **Appliquer l'identité**.

   Un message d'avertissement s'affiche indiquant que l'application d'une nouvelle identité écrase les paramètres actuels et redémarre également le serveur sélectionné. Vous êtes invité à confirmer si vous souhaitez poursuivre l'opération.

   REMARQUE : Pour effectuer des opérations de réplication de la configuration de serveur sur le serveur, l'option CSIOR doit être activée pour les serveurs. Si l'option CSIOR est désactivée, un message d'avertissement s'affiche indiquant que l'option CSIOR n'est pas activée pour le serveur. Pour effectuer l'opération de réplication de la configuration de serveur, activez l'option CSIOR sur le serveur.

4. Cliquez sur **OK** pour appliquer le profil d'identité de démarrage au serveur sélectionné.

   Le profil sélectionné est appliqué au serveur et le serveur est immédiatement redémarré. Pour plus d'informations, voir l'*Aide en ligne CMC*.

   REMARQUE : Vous pouvez appliquer un profil d'identité de démarrage à une seule partition FQDD de carte réseau (NIC) d'un serveur à la fois. Pour appliquer le même profil d'identité de démarrage à une partition FQDD de carte réseau (NIC) d'un autre serveur, vous devez le dissocier du serveur auquel il a été associé en premier lieu.

Effacement des profils d'identité de démarrage

Avant d'appliquer un nouveau profil d'identité de démarrage à un serveur de secours, vous pouvez effacer les configurations d'identité de démarrage existantes du serveur sélectionné à l'aide de l'option **Effacer l'identité** disponible dans l'interface Web CMC.

Pour effacer des profils d'identité de démarrage :

1. Accédez à la page **Profils de serveur**. Dans la section **Profils d'identité de démarrage**, sélectionnez le serveur dont vous souhaitez effacer le profil d'identité de démarrage.

   REMARQUE : Cette option est activée uniquement si l'un des serveurs est sélectionné et des profils d'identité de démarrage sont appliqués aux serveurs sélectionnés.

2. Cliquez sur **Effacer l'identité**.
3. Cliquez sur **OK** pour effacer le profil d'identité de démarrage du serveur sélectionné.
   L'opération d'effacement désactive l'identité d'E/S et la stratégie de persistance du serveur. À la fin de l'opération d'effacement, le serveur est mis hors tension.

Affichage des profils d'identité de démarrage stockés

Pour afficher les profils d'identité de démarrage stockés sur le partage réseau, accédez à la page **Profils de serveur**. Dans la section **Profils d'identité de démarrage** > **Profils stockés**, sélectionnez le profil, puis cliquez sur **Afficher** dans la colonne **Afficher le profil**. La page **Afficher les paramètres** s'affiche. Pour en savoir plus sur les paramètres affichés, voir l'*Aide en ligne du CMC*.

Importation des profils d'identité de démarrage

Vous pouvez importer des profils d'identité de démarrage stockés sur la station de gestion vers le partage réseau.

Pour importer un profil stocké sur le partage réseau à partir de la station de gestion, procédez comme suit :

1. Accédez à la page **Profils de serveur**. Dans la section **Profils d'identité de démarrage** > **Profils stockés**, cliquez sur **Importer un profil**.
   La section **Importer un profil** s'affiche.
2. Cliquez sur **Parcourir** pour accéder au profil à partir de l'emplacement souhaité, puis cliquez sur **Importer le profil**.

   Pour plus d'informations, voir l'*Aide en ligne CMC*.

Exportation des profils d'identité de démarrage

Vous pouvez exporter des profils d'identité de démarrage enregistrés sur le partage réseau vers un chemin d'accès spécifié sur une station de gestion.

Pour exporter un profil stocké, effectuez les tâches suivantes :

1. Accédez à la page **Profils de serveur**. Dans la section **Profils d'identité de démarrage** > **Profils stockés**, sélectionnez le profil souhaité, puis cliquez sur **Exporter le profil**.
   La boîte de dialogue **Téléchargement de fichier** qui s'affiche vous invite à ouvrir ou à enregistrer le fichier.
2. Cliquez sur **Enregistrer** ou **Ouvrir** pour exporter le profil vers l'emplacement requis.

Suppression des profils d'identité de démarrage

Vous pouvez supprimer un profil d'identité de démarrage stocké sur le partage réseau.

Pour supprimer un profil stocké, procédez comme suit :

1. Accédez à la page **Profils de serveur**. Dans la section **Profils d'identité de démarrage** > **Profils stockés**, sélectionnez le profil souhaité, puis cliquez sur **Supprimer le profil**.
   Un message d'avertissement s'affiche, indiquant que la suppression d'un profil supprimerait définitivement le profil sélectionné.
2. Cliquez sur **OK** pour supprimer le profil sélectionné.
   Pour plus d'informations, voir l'*Aide en ligne CMC*.

Gestion du pool d'adresses MAC virtuelles

Vous pouvez créer, ajouter, supprimer et désactiver des adresses MAC à l'aide de l'option **Gestion du pool d'adresses MAC virtuelles**. Vous pouvez utiliser uniquement des adresses MAC de monodiffusion dans le pool d'adresses MAC virtuelles. Les plages d'adresses MAC suivantes sont autorisées dans le contrôleur CMC.

- 02:00:00:00:00:00 - F2:FF:FF:FF:FF:FF
- 06:00:00:00:00:00 - F6:FF:FF:FF:FF:FF
- 0A:00:00:00:00:00 - FA:FF:FF:FF:FF:FF
- 0E:00:00:00:00:00 - FE:FF:FF:FF:FF:FF

Pour afficher l'option **Gérer une adresse MAC virtuelle** par l'interface Web CMC, dans l'arborescence système, accédez à **Présentation du châssis** > **Présentation du serveur**. Cliquez sur **Configuration** > **Profils** > **Profils d'identité de démarrage** . La section **Gérer le pool d'adresses MAC virtuelles** s'affiche.

REMARQUE : Les adresses MAC virtuelles sont gérées dans le fichier `vmacdb.xml` du partage réseau. Un fichier de verrouillage caché (`.vmacdb.lock`) est ajouté et supprimé à partir du partage réseau afin de sérialiser les opérations d'identité de démarrage à partir de plusieurs châssis.

Création d'un pool d'adresses MAC

Vous pouvez créer un pool d'adresses MAC dans le réseau à l'aide de l'option **Gérer le pool d'adresses MAC virtuelles** disponible dans l'interface Web CMC.

REMARQUE : La section Créer un pool d'adresses MAC s'affiche uniquement si la base de données des adresses MAC (`vmacdb.xml`) n'est pas disponible dans le partage réseau. Dans ce cas, les options Ajouter une adresse MAC et Supprimer une adresse MAC sont désactivées.

Pour créer un pool d'adresse MAC :

1. Accédez à la page **Profils de serveur**. Dans la section **Profils d'identité de démarrage** > **Gérer le pool d'adresses MAC virtuelles** .
2. Entrez l'adresse MAC de début du pool d'adresses MAC dans le champ **Adresse MAC de début**.
3. Entrez le nombre d'adresses MAC dans le champ **Nombre d'adresses MAC**.
4. Cliquez sur **Créer un pool d'adresses MAC** pour créer le pool d'adresses MAC.
   Une fois la base de données des adresses MAC créée dans le partage réseau, la section **Gérer le pool d'adresses MAC virtuelles** affiche la liste et l'état des adresses MAC stockées dans le partage réseau. Cette section vous permet désormais d'ajouter ou de supprimer des adresses MAC à partir du pool d'adresses MAC.

Ajout d'adresses MAC

Vous pouvez ajouter une plage d'adresses MAC sur le partage réseau à l'aide de l'option **Ajouter des adresses MAC** disponible dans l'interface Web CMC.

REMARQUE : Vous ne pouvez pas ajouter une adresse MAC qui existe dans le pool d'adresses MAC. Un message d'erreur s'affiche, indiquant que l'adresse MAC nouvellement ajoutée existe dans le pool.

Pour ajouter des adresses MAC sur le partage réseau :

1. Accédez à la page **Profils de serveur**. Dans la section **Profils d'identité de démarrage** > **Gérer le pool d'adresses MAC virtuelles**, cliquez sur **Ajouter des adresses MAC**.
2. Entrez l'adresse MAC de début du pool d'adresses MAC dans le champ **Adresse MAC de début**.
3. Entrez le nombre d'adresses MAC que vous souhaitez ajouter, dans le champ **Nombre d'adresses MAC**.

   Les valeurs valides sont comprises entre 1 et 3 000.
4. Cliquez sur **OK** pour ajouter des adresses MAC.

   Pour plus d'informations, voir l'*Aide en ligne CMC*.

Suppression d'adresses MAC

Vous pouvez supprimer une plage d'adresses MAC du partage réseau à l'aide de l'option **Supprimer des adresses MAC** disponible dans l'interface Web CMC.

REMARQUE : Vous ne pouvez pas supprimer d'adresses MAC si elles sont actives sur le nœud ou attribuées à un profil.

Pour supprimer des adresses MAC du partage réseau :

1. Accédez à la page **Profils de serveur**. Dans la section **Profils d'identité de démarrage** > **Gérer le pool d'adresses MAC virtuelles**, cliquez sur **Supprimer des adresses MAC**.
2. Entrez l'adresse MAC de début du pool d'adresses MAC dans le champ **Adresse MAC de début**.
3. Entrez le nombre d'adresses MAC à supprimer, dans le champ **Nombre d'adresses MAC**.
4. Cliquez sur **OK** pour supprimer des adresses MAC.

Désactivation d'adresses MAC

Vous pouvez désactiver les adresses MAC actives à l'aide de l'option **Désactiver l'/les adresses MAC** dans l'interface Web CMC.

REMARQUE : Utilisez l'option Désactiver l'/les adresses MAC uniquement si le serveur ne répond pas à l'action Effacer l'identité ou si l'adresse MAC n'est utilisée dans aucun serveur.

Pour supprimer des adresses MAC du partage réseau :

1. Accédez à la page **Profils de serveur**. Dans la section **Profils d'identité de démarrage** > **Gérer le pool d'adresses MAC virtuelles**, sélectionnez les adresses MAC actives à désactiver.
2. Cliquez sur **Désactiver des adresses MAC**.

Lancement d'iDRAC à l'aide d'une connexion directe (SSO)

Le CMC assure une gestion limitée des composants individuels du châssis, comme les serveurs. Pour une gestion totale de ces composants individuels, le CMC fournit un point de lancement pour l'interface Web du contrôleur de gestion (iDRAC) du serveur.

Comme cette fonctionnalité utilise l'authentification unique, un utilisateur peut lancer l'interface Web d'iDRAC sans avoir à rouvrir une session. Les stratégies d'authentification unique sont les suivantes :

- Un utilisateur CMC disposant de privilèges d'administration de serveurs est automatiquement connecté à iDRAC à l'aide de l'authentification unique (SSO). Une fois sur le site iDRAC, cet utilisateur reçoit automatiquement des privilèges d'administration. Il en va de même si le même utilisateur ne possède pas de compte sur iDRAC, ou si le compte ne possède pas les privilèges d'administrateur.
- Un utilisateur CMC qui ne dispose **PAS** de privilèges d'administrateur sur le serveur, mais qui possède le même compte sur iDRAC, est automatiquement connecté à iDRAC à l'aide de l'authentification unique (SSO). Une fois sur le site iDRAC, cet utilisateur dispose des privilèges qui ont été créés pour le compte iDRAC.

- Un utilisateur CMC qui ne dispose pas de privilèges d'administrateur sur le serveur, ou qui ne possède pas le même compte sur iDRAC, n'est pas automatiquement connecté à iDRAC à l'aide de l'authentification unique (SSO). Cet utilisateur est alors redirigé vers la page d'ouverture de session de l'iDRAC en cliquant sur **Lancer l'interface de l'iDRAC**.

REMARQUE : Dans ce contexte, le terme « même compte » signifie que l'utilisateur possède le même nom de connexion et le même mot de passe pour le CMC et pour iDRAC. Si un utilisateur possède le même nom de connexion mais avec un mot de passe différent, le système considère qu'il utilise le même compte.

REMARQUE : Les utilisateurs peuvent être invités à ouvrir une session sur iDRAC (voir la troisième puce de la stratégie d'authentification unique ci-dessus).

REMARQUE : Si le réseau local de réseau iDRAC est désactivé (Réseau local = non), l'authentification unique n'est pas disponible.

Lorsque vous cliquez sur **Lancer l'interface de l'iDRAC**, une page d'erreur peut s'afficher si :

- le serveur est retiré du châssis ;
- l'adresse IP d'iDRAC a été modifiée ;
- iDRAC rencontre un problème de connexion réseau.

Dans MCM, lorsque l'interface Web d'iDRAC est lancée à partir d'un châssis membre, les informations d'identification utilisateur du châssis organisateur et du châssis membre doivent être identiques. Sinon, la session actuelle du châssis membre est annulée et la page de connexion du châssis membre s'affiche.

Lancement d'iDRAC depuis la page Condition du serveur

Pour lancer la console de gestion d'iDRAC pour un serveur individuel :

1. Dans le volet de gauche, développez **Présentation du serveur**. Les quatre serveurs apparaissent dans la liste développée **Présentations des serveurs**.
2. Cliquez sur le serveur pour lequel vous voulez lancer l'interface Web iDRAC.
3. Sur la page **État des serveurs** , cliquez sur **Lancer iDRAC**.
   L'interface Web iDRAC s'affiche. Pour plus d'informations sur les champs, voir l'*Aide en ligne*.

Lancement d'iDRAC depuis la page Condition des serveurs

Pour lancer la console de gestion iDRAC depuis la page **Condition des serveurs** :

1. Dans le volet gauche, cliquez sur **Présentation du serveur**.
2. Sur la page **État des serveurs**, cliquez sur **Lancer iDRAC** pour le serveur pour lequel vous voulez lancer l'interface Web iDRAC.

Lancement de la console distante

Vous pouvez lancer une session KVM (Keyboard-Video-Mouse- Clavier-Écran-Souris) directement sur le serveur. La fonction de console distante est prise en charge uniquement lorsque toutes les conditions suivantes sont réunies :

- Le châssis est sous tension,
- Serveurs prenant en charge iDRAC7 et iDRAC8.
- L'interface de réseau local sur le serveur est activée.
- Le système hôte dispose du JRE (Java Runtime Environment) 6 Update 16 ou ultérieur.
- Le navigateur sur le système hôte autorise les fenêtres contextuelles (le blocage de fenêtres contextuelles est désactivé).

Vous pouvez également lancer la console distante depuis l'interface Web iDRAC. Pour plus d'informations, voir le *Guide d'utilisation d'iDRAC* accessible sur le site dell.com/support/manuals.

Lancement de la console distante depuis la page Intégrité du châssis

Pour lancer une console distante depuis l'interface Web CMC :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** et sur **Propriétés**.
2. Sur la page **Intégrité du châssis**, cliquez sur le serveur défini dans le graphique du châssis.
3. Dans la section **Liens rapides**, cliquez sur le lien **Lancer la console distante** pour lancer la console distante.

Lancement de la console distante depuis la page Condition du serveur

Pour lancer une console distante pour un serveur particulier :

1. Dans le volet de gauche, développez **Présentation du serveur**. Les quatre serveurs apparaissent dans la liste développée des serveurs.
2. Cliquez sur le serveur pour lequel vous voulez lancer la console distante.
3. Dans la page **État du serveur**, cliquez sur **Lancer la console distante**.

Lancement de la console distante depuis la page Condition des serveurs

Pour lancer une console distante de serveur à partir de la page **Condition des serveurs** :

1. Dans le volet de gauche, accédez à **Présentation du serveur**, puis cliquez sur **Propriétés** > **État**. La page **Condition des serveurs** s'affiche.
2. Cliquez sur **Lancer la console distante** pour le serveur voulu.

8

Configuration du CMC pour envoyer des alertes

Vous pouvez configurer des alertes et des actions pour certains événements qui se produisent sur le châssis. Un événement est généré lorsque l'état d'un périphérique ou d'un service a changé ou qu'une condition d'erreur est détectée. Si un événement correspond à un filtre d'événement et que vous avez configuré ce filtre pour générer un message d'alerte (alerte par e-mail ou interruption SNMP), une alerte est envoyée à une ou plusieurs destinations configurées comme adresse électronique, adresse IP ou serveur externe.

Pour configurer le CMC afin qu'il envoie des alertes :

1. Activez l'option **Alertes d'événement de châssis**.
2. Vous pouvez également filtrer les alertes en fonction d'une catégorie ou d'un niveau de gravité.
3. Configurez les paramètres d'alerte par e-mail ou par interruption SNMP.
4. Activez les alertes d'événement de châssis pour envoyer une alerte par e-mail ou des interruptions SNMP à des destinations définies.

Sujets :

Activation ou désactivation des alertes

Pour envoyer des alertes aux destinations configurées, vous devez activer l'option d'alertes globales. Cette propriété écrase le paramètre d'alertes individuelles.

Vérifiez que les destinations des alertes par e-mail ou par SNMP sont configurées pour recevoir les alertes.

Activation ou désactivation des alertes à l'aide de l'interface Web CMC

Pour activer ou désactiver la génération d'alertes :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Alertes**.
2. Sur la page **Événements du châssis**, dans la section **Activation des alertes de châssis**, sélectionnez **Activer les alertes d'événement de châssis** pour activer l'alerte ou désactivez l'option pour désactiver l'alerte.
3. Pour enregistrer les paramètres, cliquez sur **Appliquer**.

Filtrage des alertes

Vous pouvez filtrer les alertes en fonction d'une catégorie ou d'un niveau de gravité.

Filtrage des alertes à l'aide de l'interface Web iDRAC7

Pour filtrer les alertes en fonction de la catégorie et de la gravité :

REMARQUE : Pour modifier la configuration des événements de châssis, vous devez disposer du privilège Configuration des alertes.

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Alertes**.
2. Sur la page **Événements de châssis**, dans la section **Filtre des alertes, sélectionnez une ou plusieurs des catégories suivantes** :
   - **Intégrité du système**
   - **Stockage**

- **Configuration**
- **Audit**
- **Mises à jour**

3. Sélectionnez un ou plusieurs des niveaux de gravité suivants :
   - **Critique**
   - **Avertissement**
   - **Informatif**

   La section **Alertes surveillées** contient le résultat en fonction de la catégorie et de la gravité sélectionnées. Pour plus d'informations sur les champs de cette page, voir l'*Aide en ligne*.
4. Cliquez sur **Appliquer**.

Définition d'alertes d'événement à l'aide de l'interface RACADM

Pour définir une alerte d'événement, exécutez la commande `eventfilters`. Pour plus d'informations, voir le *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX) sur le site **dell.com/support//manuals**.

Configuration de destinations d'alerte

La station de gestion utilise le protocole SNMP (Simple Network Management Protocol - P protocole de gestion de réseau simple) pour recevoir des données depuis CMC.

Vous pouvez configurer les destinations d'alerte IPv4 et IPv6, les paramètres e-mail et les paramètres de serveur SMTP et tester ces paramètres.

Avant de définir les paramètres d'alerte par e-mail ou interruption SNMP, vérifiez que vous disposez du privilège Administrateur de configuration du châssis.

Configuration de destinations d'alerte pour interruption SNMP

Vous pouvez configurer des adresses IPv6 ou IPv4 pour qu'elles reçoivent les interruptions SNMP.

Configuration des destinations d'alerte pour interruption SNMP à l'aide de l'interface Web CMC

Pour configurer les paramètres de destination d'alerte IPv4 ou IPv6 en utilisant l'interface Web CMC :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Alertes** > **Paramètres d'interruption**.
2. Dans la page **Destination de l'alerte d'événement de châssis**, entrez ce qui suit :
   - Dans le champ **Destination**, entrez une adresse IP valide. Utilisez le format IPv4 avec quatre groupes de chiffres séparés par des points, la notation standard d'adresse IPv6 ou le nom de domaine qualifié. Par exemple : `123.123.123.123` ou `2001:db8:85a3::8a2e:370:7334` ou `dell.com`.

     Choisissez un format cohérent avec votre technologie ou infrastructure de réseau. La fonction d'interruption test ne peut pas détecter les choix incorrects sur la base de la configuration réseau actuelle (par exemple, l'utilisation d'une destination IPv6 dans un environnement IPv4 uniquement).
   - Dans le champ **Chaîne de communauté**, entrez la chaîne de communauté valide à laquelle la station de gestion de destination appartient.

     Cette chaîne de communauté est différente de celle définie dans la page **Présentation du châssis** > **Réseau** > **Services**. La chaîne de communauté des interruptions SNMP est celle que le contrôleur CMC utilise pour les interruptions sortantes destinées aux stations de gestion. La chaîne de communauté de la page **Présentation du châssis** > **Réseau** > **Services** est celle que les stations de gestion emploient pour interroger le démon SNMP sur le contrôleur CMC.
   - Sous **Activé**, cochez la case correspondant à l'adresse IP de destination pour permettre à cette adresse de recevoir les interruptions. Vous pouvez spécifier jusqu'à quatre adresses IP.
3. Cliquez sur **Appliquer** pour enregistrer les paramètres.

4. Pour vérifier que l'adresse IP reçoit bien les interruptions SNMP, cliquez sur **Envoyer** dans la colonne **Interruption SNMP de test**.

   Les destinations d'alerte IP sont configurées.

Configuration de destinations d'alerte par interruption SNMP avec RACADM

Pour configurer des destinations d'alerte IP avec RACADM :

1. Ouvrez une console série/Telnet/SSH d'accès à CMC, puis ouvrez une session.

   REMARQUE : Vous ne pouvez définir qu'un seul masque de filtre pour les alertes SNMP et par e-mail. Si vous avez déjà sélectionné le masque de filtre, n'exécutez pas la tâche 2 et passez à l'étape 3.

2. Activez la génération d'alertes :

   ```
   racadm config -g cfgAlerting -o cfgAlertingEnable 1
   ```

3. Définissez les filtres d'événements en exécutant la commande `racadm eventfilters set`.
   a. Pour effacer tous les paramètres d'alerte disponibles, exécutez la commande `racadm eventfilters set -c cmc.alert.all -n none`
   b. Définissez l'utilisation d'une gravité comme paramètre. Par exemple, tous les événements d'information dans une catégorie de stockage sont affectés de l'action de mise hors tension et d'alertes par e-mail et SNMP pour les notifications : `racadm eventfilters set -c cmc.alert.storage.info -n email,snmp`
   c. Définissez l'utilisation d'une sous-catégorie comme paramètre. Par exemple, l'action de mise hors tension est affectée à toutes les configurations dans la sous-catégorie d'octroi des licences de la sous-catégorie d'audit et toutes les notifications sont activées : `racadm eventfilters set -c cmc.alert.audit.lic -n all`
   d. Définissez l'utilisation d'une sous-catégorie et d'une gravité comme paramètre. Par exemple, l'action de mise hors tension est affectée à tous les événements d'information dans la catégorie d'octroi des licences de la catégorie d'audit et toutes les notifications sont désactivées : `racadm eventfilters set -c cmc.alert.audit.lic.info -n none`
4. Activez les alertes par interruption :

   ```
   racadm config -g cfgTraps -o cfgTrapsEnable 1 -i <index>
   ```

   Où `<index>` est une valeur comprise entre 1 et 4. Le contrôleur CMC utilise le numéro d'index pour distinguer jusqu'à quatre adresses de destination configurables pour les alertes par interruption. Vous pouvez spécifier les destinations sous forme d'adresses numériques de format approprié (IPv6 ou IPv4) ou de noms de domaine qualifiés (FQDN, (Fully-Qualified Domain Name).
5. Spécifiez une adresse IP de destination pour la réception des alertes par interruption :

   ```
   racadm config -g cfgTraps -o cfgTrapsAlertDestIPAddr <adresse IP> -i <index>
   ```

   où `<IP address>` est une destination valide et `<index>` est la valeur d'index spécifiée à l'étape 4.
6. Spécifiez le nom de communauté :

   ```
   racadm config -g cfgTraps -o cfgTrapsCommunityName <nom de communauté> -i <index>
   ```

   où `<community name>` est la communauté SNMP à laquelle appartient le châssis, et `<index>` est la valeur d'index spécifiée aux étapes 4 et 5.

   Vous pouvez configurer jusqu'à quatre destinations pour les alertes par interruption. Pour ajouter d'autres destinations, répétez les étapes 2 à 6.

   REMARQUE : Les commandes des étapes 2 à 6 remplacent les paramètres existants définis pour l'index spécifié (1 à 4). Pour déterminer si un index possède des valeurs déjà configurées, entrez `racadm getconfig -g cfgTraps -i <index>`. Si l'index est déjà configuré, des valeurs apparaissent pour les objets `cfgTrapsAlertDestIPAddr` et `cfgTrapsCommunityName`.

7. Pour tester une interruption d'événement pour une destination d'alerte :

   ```
   racadm testtrap -i <index>
   ```

   où `<index>` est une valeur comprise entre 1 et 4 représentant la destination d'alerte à tester.

Si vous ne connaissez pas le numéro d'index, exécutez la commande suivante :

```
racadm getconfig -g cfgTraps -i <index>
```

Configuration des paramètres d'alerte par e-mail

Lorsque CMC détecte un événement sur châssis, comme un avertissement portant sur l'environnement ou une panne de composant, il peut être configuré pour envoyer une alerte par e-mail vers une ou plusieurs adresses e-mail.

Configurez le serveur de messagerie SMTP pour qu'il accepte les e-mails relayés depuis l'adresse IP CMC. Cette fonction est normalement désactivée sur la plupart des serveurs de messagerie pour des raisons de sécurité. Pour savoir comment le configurer en toute sécurité, voir la documentation fournie avec le serveur SMTP.

REMARQUE : Si vous utilisez le serveur de messagerie Microsoft Exchange Server 2007, veillez à ce que le nom de domaine d'iDRAC soit configuré pour que le serveur de messagerie puisse recevoir les alertes par e-mail d'iDRAC.

REMARQUE : Les alertes par e-mail prennent en charge les adresses iPv4 et IPv6. Le nom de domaine DNS DRAC doit être défini lorsque vous utilisez IPv6.

Si votre réseau comporte un serveur SMTP qui envoie et renouvelle l'adresse IP périodiquement, et si les adresses sont différentes, il existe une durée de temporisation où ce paramètre ne fonctionne pas, en raison d'un changement dans l'adresse IP de serveur SMTP spécifiée. Dans ce cas, utilisez le nom DNS.

Définition des paramètres des alertes par e-mail à l'aide de l'interface Web CMC :

Pour configurer les paramètres d'alerte par e-mail en utilisant l'interface Web :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Alertes** > **Paramètres d'alerte par e-mai**.
2. Définissez les paramètres de serveur de messagerie SMTP et les adresses e-mail de destination des alertes. Pour plus d'informations sur les champs, voir l'*Aide en ligne*.
3. Cliquez sur **Appliquer** pour enregistrer les paramètres.
4. Cliquez sur **Envoyer** dans la section **E-mail test** afin d'envoyer un e-mail de test à la destination d'alerte par e-mail spécifiée.

Définition des paramètres des alertes par e-mail à l'aide de RACADM

Pour envoyer un e-mail test à une destination d'alerte par e-mail :

1. Ouvrez une console série/Telnet/SSH d'accès à CMC, puis ouvrez une session.
2. Activez la génération d'alertes :

   ```
   racadm config -g cfgAlerting -o cfgAlertingEnable 1
   ```

   REMARQUE : Un seul masque de filtrage peut être défini par les alertes SNMP et par e-mail. Si vous avez déjà défini un masque de filtrage, n'exécutez pas la tâche de l'étape 3.

3. Spécifiez les événements pour lesquels des alertes doivent être générées :

   ```
   racadm config -g cfgAlerting -o cfgAlertingFilterMask <mask value>
   ```

   Où `<mask value>` est une valeur hexadécimale comprise entre 0x0 et 0xffffffff, exprimée avec les caractères 0x de début. Le tableau Masques de filtrage des interruptions d'événement indique les masques de filtrage de chaque type d'événement. Pour savoir comment calculer la valeur hexadécimale du masque de filtrage à activer, voir l'étape 3 dans Configuration de destinations d'alerte par interruption SNMP à l'aide de RACADM.
4. Activer une génération d'alerte par e-mail :

   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEnable 1 -i <index>
   ```

   où `<index>` est une valeur comprise entre 1 et 4. Le contrôleur CMC utilise le numéro d'index pour distinguer jusqu'à quatre adresses e-mail de destination pouvant être définies.

5. Spécifiez une adresse e-mail de destination pour recevoir les alertes par e-mail en entrant :

```
racadm config -g cfgEmailAlert -o cfgEmailAlertAddress <email address> -i <index>
```

où `<email address>` correspond à une adresse IP valide et `<index>` à la valeur d'index spécifiée à l'étape 4.

6. Spécifiez le nom de la personne qui reçoit l'alerte par e-mail :

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEmailName <email name> -i <index>
```

Où `<email name>` est le nom de la personne ou du groupe qui doit recevoir l'alerte par e-mail, et `<index>` est la valeur d'index spécifiée aux étapes 4 et 5. Le nom du destinataire d'e-mail peut contenir jusqu'à 32 caractères alphanumériques, tirets, caractères de soulignement et points. Les espaces ne sont pas valides.

7. Configurez l'hôte SMTP :

```
racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr host.domain
```

Où `host.domain` est le nom FQDN (Fully Qualified Domain Name - Nom de domaine entièrement qualifié).

Vous pouvez définir jusqu'à quatre adresses e-mail de destination pour recevoir des alertes par e-mail. Pour ajouter plus d'adresses e-mail, exécutez les étapes 2 à 6.

REMARQUE : Les commandes des étapes 2 à 6 remplacent les paramètres existants définis pour l'index que vous indiquez (1 à 4). Pour déterminer si un index a des valeurs déjà définies, tapez `racadm getconfig -g cfgEmailAlert — I <index>`. Si l'index est déjà défini, des valeurs apparaissent pour les objets `cfgEmailAlertAddress` et `cfgEmailAlertEmailName`.

Pour plus d'informations, voir le document *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX) sur le site **dell.com/support/manuals**.

9

Configuration des comptes et des privilèges des utilisateurs

Vous pouvez configurer des comptes utilisateur avec des privilèges spécifiques (autorisation basée su un rôle) pour gérer le système avec le contrôleur CMC et garantir la sécurité de ce système. Par défaut, le contrôleur CMC est configuré avec un compte d'administrateur local. Ce nom par défaut est `root` et le mot de passe est `calvin`. En tant qu'administrateur, vous pouvez configurer des comptes utilisateur pour autoriser d'autres utilisateurs à accéder au contrôleur CMC.

Vous pouvez définir jusqu'à 16 utilisateurs locaux ou utiliser des services d'annuaire, comme Microsoft Active Directory ou LDAP, pour définir des comptes utilisateur supplémentaires. L'utilisation d'un service d'annuaire permet de disposer d'un emplacement central pour la gestion des comptes d'utilisateur autorisés.

Le contrôleur CMC prend en charge l'accès basé sur les rôles pour les utilisateurs possédant un ensemble de privilèges associés. Les rôles disponibles sont Administrateur, Opérateur, Lecture seule et Aucun. Le rôle définit les privilèges maximaux disponibles.

Sujets :

Types d'utilisateur

Il existe deux types d'utilisateur :

- Utilisateurs CMC ou utilisateurs de châssis
- Utilisateurs iDRAC ou utilisateurs de serveur (puisque l'iDRAC réside sur un serveur)

Les utilisateurs CMC et iDRAC peuvent être des utilisateurs locaux ou des utilisateurs des services d'annuaire.

Sauf si un utilisateur CMC dispose du privilège d'**Administrateur de serveur**, les privilèges octroyés à un utilisateur CMC ne sont pas automatiquement transférés à ce même utilisateur sur un serveur, car les utilisateurs du serveur sont créés indépendamment des utilisateurs CMC. Autrement dit, les utilisateurs Active Directory CMC et les utilisateurs Active Directory iDRAC résident dans deux branches distinctes de l'arborescence Active Directory. Pour créer un utilisateur du serveur local, les utilisateurs disposant du privilège de configuration d'utilisateurs doivent se connecter directement au serveur. Les utilisateurs disposant du privilège de configuration d'utilisateurs ne peuvent pas créer d'utilisateur de serveur depuis le CMC, et inversement. Cette règle protège la sécurité et l'intégrité des serveurs.

Tableau 20. Types d'utilisateurs

Droits	Description
Ouverture de session utilisateur CMC	L'utilisateur peut se connecter à CMC et afficher toutes les données CMC, mais ne peut pas ajouter ni modifier de données, ni exécuter de commandes. Un utilisateur peut posséder d'autres privilèges, sans nécessairement disposer du privilège d'ouverture de session sur CMC. Cette fonction est utile lorsqu'un utilisateur n'est temporairement plus autorisé à se connecter. Lorsque le privilège d'ouverture de session sur CMC de cet utilisateur est rétabli, l'utilisateur conserve tous les autres privilèges précédemment octroyés.
Administrateur de configuration du châssis	L'utilisateur peut ajouter ou modifier des données qui : • Identifient le châssis, tels que le nom du châssis et son emplacement. • Sont attribuées spécifiquement au châssis, tels que le mode IP (statique ou DHCP), l'adresse IP statique, la passerelle statique et le masque de sous-réseau statique. • Fournissent des services au châssis, telles que la date et heure, la mise à jour de micrologiciel et la réinitialisation du CMC.

Tableau 20. Types d'utilisateurs (suite)

Droits	Description
	• Sont associées au châssis, telles que le nom de logement et la priorité du logement. Bien que ces propriétés s'appliquent aux serveurs, il s'agit de propriétés du châssis qui concernent les logements plutôt que les serveurs eux-mêmes. C'est pourquoi il est possible d'ajouter ou de modifier des noms et priorités de logement, même si aucun serveur n'est présent dans le logement concerné. Lorsqu'un serveur est déplacé vers un autre châssis, il hérite du nom et de la priorité de logement associés au logement qu'il occupe dans le nouveau châssis. Le nom et la priorité précédents du châssis restent associés au châssis précédent. **REMARQUE : Les utilisateurs CMC dotés du privilège Administrateur de configuration du châssis peuvent configurer les paramètres d'alimentation. Cependant, le privilège Administrateur de contrôle du châssis est nécessaire pour effectuer des opérations d'alimentation de châssis, y compris la mise sous tension, la mise hors tension et le cycle d'alimentation.**
Administrateur de configuration des utilisateurs	L'utilisateur peut : • Ajouter un nouvel utilisateur. • Changer le mot de passe d'un utilisateur • Changer les privilèges d'un utilisateur • Activer ou désactiver le privilège de connexion d'un utilisateur, mais conserver le nom et les autres privilèges de l'utilisateur dans la base de données.
Administrateur des effacements de journaux	L'utilisateur peut effacer le journal matériel et le journal CMC.
Administrateur de contrôle du châssis (contrôle de l'alimentation)	Les utilisateurs CMC dotés du privilège **Administrateur d'alimentation du châssis** peuvent effectuer toutes les opérations liées à l'alimentation. Ils peuvent contrôler les opérations d'alimentation du châssis, y compris la mise sous tension, la mise hors tension et le cycle d'alimentation. **REMARQUE : Le privilège d'Administrateur de configuration du châssis est nécessaire pour configurer des paramètres d'alimentation.**
Server Administrator	Ceci est un privilège général : les droits d'administrateur de serveur sont des droits permanents qui autorisent l'utilisateur CMC à effectuer des opérations sur n'importe quel serveur présent dans le châssis. Lorsqu'un utilisateur possédant le privilège d'**Administrateur de serveur** émet une action à exécuter sur un serveur, le micrologiciel du CMC envoie la commande au serveur ciblé sans vérifier les privilèges de l'utilisateur sur le serveur. Autrement dit, le privilège d'**Administrateur de serveur** permet de passer outre l'absence de privilèges d'administrateur sur le serveur. Sans les droits d'**Administrateur de serveur**, un utilisateur créé sur le châssis ne peut exécuter une commande sur un serveur que lorsque les conditions suivantes sont réunies : • Le même nom d'utilisateur est utilisé sur le serveur. • Le même nom d'utilisateur doit avoir exactement le même mot de passe sur le serveur. • L'utilisateur doit avoir le droit d'exécuter la commande. Lorsqu'un utilisateur CMC qui ne dispose pas du privilège d'**Administrateur de serveur** émet une action à exécuter sur un serveur, le CMC envoie une commande au serveur ciblé avec le nom et le mot de passe de connexion de cet utilisateur. Si l'utilisateur n'existe pas sur le serveur ou si le mot de passe ne correspond pas, l'utilisateur se voit dans l'impossibilité d'effectuer l'action. Si l'utilisateur existe sur le serveur cible et si le mot de passe correspond, le serveur répond avec les privilèges accordés à l'utilisateur sur le serveur. Selon les privilèges renvoyés par le serveur, le micrologiciel du CMC décide si l'utilisateur a le droit d'effectuer l'action.
	Nous avons répertorié ci-dessous les privilèges octroyés à l'administrateur du serveur ainsi que les actions qu'il peut effectuer sur le serveur. Ces droits ne sont appliqués que lorsque l'utilisateur du châssis ne possède pas le droit d'administration du serveur sur le châssis. Administration et configuration du serveur : • Définir l'adresse IP

Tableau 20. Types d'utilisateurs (suite)

Droits	Description
	· Définir la passerelle · Définir le masque de sous-réseau · Définir le périphérique de démarrage initial Configurer les utilisateurs : · Définir le mot de passe root d'iDRAC · Réinitialisation d'iDRAC Administration de contrôle du serveur : · Mise sous tension · Mise hors tension · Cycle d'alimentation · Arrêt normal · Redémarrage du serveur
Utilisateur d'alertes de test	L'utilisateur peut envoyer des messages d'alerte d'essai.
Administrateur de commandes de débogage	L'utilisateur peut exécuter des commandes de diagnostic système.
Administrateur de structure A	L'utilisateur peut définir et configurer le module IOM de la structure A.
Administrateur de structure B	L'utilisateur peut définir et configurer la structure B qui correspond à la première carte mezzanine dans les serveurs et qui est connectée aux circuits de la structure B dans le sous-système PCIe partagé dans la carte principale.
Administrateur de structure C	L'utilisateur peut définir et configurer la structure C qui correspond à la seconde carte mezzanine dans les serveurs et qui est connectée aux circuits de la structure C dans le sous-système PCIe partagé dans la carte principale.

Les groupes d'utilisateurs CMC fournissent une série de groupes d'utilisateurs disposant de privilèges préattribués.

REMARQUE : Si vous sélectionnez Administrateur, Utilisateur privilégié ou Utilisateur invité et que vous ajoutez ou supprimez ensuite un droit du jeu prédéfini, le groupe CMC devient automatiquement personnalisé.

Tableau 21. Privilèges de groupe CMC

Groupe d'utilisateurs	Privilèges accordés
Administrateur	· Ouverture de session utilisateur CMC · Administrateur de configuration du châssis · Administrateur de configuration des utilisateurs · Administrateur des effacements de journaux · Server Administrator · Utilisateur d'alertes de test · Administrateur de commandes de débogage · Administrateur de structure A
Utilisateur privilégié	· Ouverture de session · Administrateur des effacements de journaux · Administrateur de contrôle du châssis (contrôle de l'alimentation) · Server Administrator · Utilisateur d'alertes de test · Administrateur de structure A
Utilisateur invité	Ouverture de session
Personnalisée	Sélectionnez n'importe quelle combinaison des autorisations suivantes :

Tableau 21. Privilèges de groupe CMC (suite)

Groupe d'utilisateurs	Privilèges accordés
	• Ouverture de session utilisateur CMC • Administrateur de configuration du châssis • Administrateur de configuration des utilisateurs • Administrateur des effacements de journaux • Administrateur de contrôle du châssis (contrôle de l'alimentation) • Server Administrator • Utilisateur d'alertes de test • Administrateur de commandes de débogage • Administrateur de structure A
Aucun	Aucun droit attribué

Tableau 22. Comparaison des privilèges des administrateurs CMC, des utilisateurs privilégiés et des utilisateurs invités

Privilège défini	Droits d'administrateur	Droits d'utilisateur privilégié	Droits d'utilisateur invité
Ouverture de session utilisateur CMC	Oui	Oui	Oui
Administrateur de configuration du châssis	Oui	Non	Non
Administrateur de configuration des utilisateurs	Oui	Non	Non
Administrateur des effacements de journaux	Oui	Oui	Non
Administrateur de contrôle du châssis (contrôle de l'alimentation)	Oui	Oui	Non
Server Administrator	Oui	Oui	Non
Utilisateur d'alertes de test	Oui	Oui	Non
Administrateur de commandes de débogage	Oui	Non	Non
Administrateur de structure A	Oui	Oui	Non

Modification des paramètres du compte administrateur de l'utilisateur root

Pour renforcer la sécurité, il est vivement recommandé de modifier le mot de passe par défaut du compte racine (Utilisateur 1). Le compte racine est le compte administratif par défaut fourni avec le contrôleur CMC.

Pour changer le mot de passe par défaut du compte racine :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** et sur **Authentification des utilisateurs**.
2. Sur la page **Utilisateurs**, dans la colonne **ID utilisateur**, cliquez sur **1**.

   REMARQUE : L'ID utilisateur 1 correspond au compte utilisateur racine fourni par défaut avec le contrôleur CMC. Vous ne pouvez pas le modifier.
3. Sur la page **Configuration de l'utilisateur**, sélectionnez l'option **Changer le mot de passe**.
4. Entrez le nouveau mot de passe dans le champ **Mot de passe**, puis entrez-le de nouveau dans le champ **Confirmer le mot de passe**.
5. Cliquez sur **Appliquer**. Le mot de passe de l'utilisateur ayant l'ID **1** est modifié.

Configuration des utilisateurs locaux

Vous pouvez définir jusqu'à 16 utilisateurs locaux dans le contrôleur CMC avec des privilèges d'accès spécifiques. Avant de créer un utilisateur CMC local, vérifiez s'il existe déjà des utilisateurs. Vous pouvez définir des noms d'utilisateur, des mots de passe et des rôles

avec des privilèges pour ces utilisateurs. Les noms d'utilisateur et les mots de passe peuvent être changés dans n'importe quelle interface sécurisée CMC (telle que l'interface Web, RACADM ou WS-MAN).

Définition des utilisateurs locaux à l'aide de l'interface Web CMC

REMARQUE : Vous devez disposer du privilège Configurer les utilisateurs pour pouvoir créer un utilisateur CMC.

Pour ajouter et configurer des utilisateurs CMC locaux :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** et sur **Authentification des utilisateurs**.
2. Sur la page **Utilisateurs locaux**, dans la colonne **ID utilisateur**, cliquez sur un numéro d'ID. La page **Définition de l'utilisateur** s'affiche.

   REMARQUE : L'ID utilisateur 1 correspond au compte utilisateur racine fourni par défaut avec un contrôleur CMC. Vous ne pouvez pas le modifier.

3. Activez l'ID utilisateur, puis spécifiez le nom, le mot de passe et les privilèges d'accès de l'utilisateur. Pour plus d'informations sur les options, voir l'*Aide en ligne*.
4. Cliquez sur **Appliquer**. L'utilisateur est créé avec les privilèges appropriés.

Configuration d'utilisateurs locaux à l'aide de RACADM

REMARQUE : Vous devez vous connecter comme utilisateur `root` pour pouvoir exécuter des commandes RACADM sur un système Linux distant.

Vous pouvez configurer jusqu'à 16 utilisateurs dans la base de données de propriétés CMC. Avant d'activer manuellement un utilisateur CMC, vérifiez s'il existe déjà des utilisateurs.

Si vous configurez un nouveau contrôleur CMC ou que vous avez utilisé la commande racadm `racresetcfg`, le seul utilisateur actuel est `root`, dont le mot de passe est `calvin`. La sous-commande `racresetcfg` réinitialise les valeurs par défaut de tous les paramètres de configuration. Toutes les modifications précédentes sont perdues.

REMARQUE : les utilisateurs peuvent être activés et désactivés au fil du temps ; la désactivation d'un utilisateur ne le supprime pas de la base de données.

Pour vérifier si un utilisateur existe, ouvrez une console textuelle Telnet / SSH sur CMC, connectez-vous et entrez la commande suivante une fois pour chaque index compris entre 1 et 16 :

```
racadm getconfig -g cfgUserAdmin -i <index>
```

REMARQUE : Vous pouvez également entrer `racadm getconfig -f <myfile.cfg>` et afficher ou modifier le fichier `myfile.cfg` qui contient tous les paramètres de configuration CMC.

Plusieurs paramètres et ID d'objet sont affichés avec leurs valeurs actuelles. Deux objets sont importants ici :

```
# cfgUserAdminIndex=XX
cfgUserAdminUserName=
```

Si l'objet `cfgUserAdminUserName` n'a pas de valeur, le numéro d'index, indiqué par l'objet `cfgUserAdminIndex`, peut être utilisé. Si un nom est affiché après « = », cet index est pris par ce nom d'utilisateur.

Lorsque vous activez ou désactivez manuellement un utilisateur avec la sous-commande racadm `config`, vous devez spécifier l'index avec l'option `-i`.

Notez que l'objet `racadm config -f racadm.cfg` dans l'exemple précédent contient le caractère « # ». Cela indique qu'il s'agit d'un objet en lecture seule. En outre, si vous utilisez la commande racadm config -f racadm.cfg pour définir un nombre de groupes/objets à écrire, l'index ne peut pas être spécifié. Un nouvel utilisateur est ajouté au premier index disponible. Ce comportement offre une plus grande souplesse pour la configuration d'un deuxième contrôleur CMC avec les mêmes paramètres que le contrôleur CMC principal.

Ajout d'un utilisateur CMC avec RACADM

Pour ajouter un nouvel utilisateur à la configuration CMC :

1. Définissez le nom d'utilisateur.
2. Définissez le mot de passe.
3. Définissez les privilèges d'utilisateur. Pour plus d'informations sur les privilèges utilisateur, reportez-vous à la section Types d'utilisateur.
4. Activez l'utilisateur.

Exemple :

L'exemple suivant explique comment ajouter le nouvel utilisateur « Jean » avec le mot de passe « 123456 » et le privilège Connexion sur CMC.

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName
-i 2
john
racadm config -g cfgUserAdmin -o cfgUserAdminPassword
-i 2
123456
racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminPrivilege
0x00000001
racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminEnable 1
```

REMARQUE : Pour la liste des valeurs de masque de bits valides de privilèges utilisateur spécifiques, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX*. La valeur de privilège est 0 par défaut, ce qui signifie que les privilèges d'un utilisateur ne sont pas activés.

Pour vérifier qu'un utilisateur a été ajouté avec les privilèges corrects, utilisez la commande suivante :

```
racadm getconfig -g cfgUserAdmin -i 2
```

Pour plus d'informations sur les commandes RACADM, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX* sur le site **dell.com/support/manuals**.

Désactivation d'un utilisateur CMC

Lorsque vous utilisez RACADM, les utilisateurs doivent être désactivés manuellement et de manière individuelle. Vous ne pouvez pas supprimer des utilisateurs en utilisant un fichier de configuration.

Pour supprimer un utilisateur CMC, utilisez la commande suivante :

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i <index>"" racadm config -g
cfgUserAdmin -i 2 -o cfgUserAdminPrivilege 0x0
```

Une chaîne null entre guillemets doubles ("") indique au contrôleur CMC qu'il doit supprimer la configuration utilisateur à l'index indiqué et restaurer les valeurs par défaut définies en usine de la configuration utilisateur.

Activation d'un utilisateur CMC avec des droits

Pour activer un utilisateur avec des droits (droit basé sur un rôle) :

1. recherchez un index d'utilisateur disponible en utilisant la commande suivante :

   ```
   racadm getconfig -g cfgUserAdmin -i <index>
   ```

2. Tapez les commandes suivantes avec les nouveaux nom d'utilisateur et mot de passe.

   ```
   racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <index> <valeur de masque
   binaire de privilège d'utilisateur>
   ```

   REMARQUE : Pour la liste des valeurs de masque de bits de privilèges utilisateur spécifiques, voir le document *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX) sur le site dell.com/support/manuals. La valeur de privilège par défaut est 0 qui indique que l'utilisateur ne dispose pas de privilèges activés.

Configuration des utilisateurs d'Active Directory

Si votre société utilise le logiciel Microsoft Active Directory, vous pouvez le configurer pour fournir un accès à CMC, ce qui permet d'ajouter des privilèges CMC aux utilisateurs existants et de les contrôler dans le service d'annuaire. Cette fonction est disponible sous licence.

REMARQUE : Sur les systèmes d'exploitation suivants, vous pouvez reconnaître les utilisateurs CMC en utilisant Active Directory.

- **Microsoft Windows 2000**
- **Microsoft:Windows Server 2003**
- **Microsoft Windows Server 2008**

Vous pouvez configurer l'authentification des utilisateurs via Active Directory pour la connexion au CMC. Vous pouvez également fournir des droits basés sur un rôle pour qu'un administrateur puisse configurer des privilèges pour chaque utilisateur.

Mécanismes d'authentification Active Directory pris en charge

Vous pouvez utiliser Active Directory pour définir l'accès utilisateur CMC, en utilisant deux méthodes :

- La solution de *Schéma standard*, qui utilise uniquement les objets de groupe Active Directory par défaut Microsoft.
- La solution de *Schéma étendu*, qui inclut des objets Active Directory personnalisés fournis par Dell. Tous les objets de contrôle d'accès sont gérés dans Active Directory. Cela offre une souplesse maximale pour la configuration de l'accès des utilisateurs aux différents CMC avec divers niveaux de privilèges.

Présentation d'Active Directory avec le schéma standard

Comme le montre la figure ci-dessous, l'utilisation du schéma standard pour l'intégration d'Active Directory exige des opérations de configuration à la fois dans Active Directory et dans le CMC.

Dans Active Directory, un objet Groupe standard est utilisé comme groupe de rôles. Tout utilisateur qui dispose d'un accès à CMC est membre du groupe de rôles. Pour que cet utilisateur puisse accéder à une carte CMC spécifique, le nom du groupe de rôles et son nom de domaine doivent être configurés sur la carte CMC concernée. Le rôle et le niveau de privilège sont définis pour chaque carte CMC, et non dans l'annuaire Active Directory. Vous pouvez définir jusqu'à cinq groupes de rôles dans chaque CMC. Le tableau suivant répertorie les privilèges par défaut des groupes de rôles.

Tableau 23. : Privilèges par défaut des groupes de rôles

Groupe de rôles	Niveau de privilège par défaut	Droits accordées	Masque binaire
1	Aucun	• Ouverture de session utilisateur CMC • Administrateur de configuration du châssis • Administrateur de configuration des utilisateurs • Administrateur des effacements de journaux • Administrateur de contrôle du châssis (contrôle de l'alimentation) • Server Administrator • Utilisateur d'alertes de test • Administrateur de commandes de débogage • Administrateur de structure A	0x00000fff
2	Aucun	• Ouverture de session utilisateur CMC • Administrateur des effacements de journaux • Administrateur de contrôle du châssis (contrôle de l'alimentation) • Server Administrator • Utilisateur d'alertes de test • Administrateur de structure A	0x00000ed9

Tableau 23. : Privilèges par défaut des groupes de rôles (suite)

Groupe de rôles	Niveau de privilège par défaut	Droits accordées	Masque binaire
3	Aucun	Ouverture de session utilisateur CMC	0x00000001
4	Aucun	Aucun droit attribué	0x00000000
5	Aucun	Aucun droit attribué	0x00000000

REMARQUE : Les valeurs Masque binaire sont utilisées uniquement lors de la définition du schéma standard avec le RACADM.

REMARQUE : Pour plus d'informations sur les privilèges utilisateur, voir « Types d'utilisateur ».

Configuration d'Active Directory avec le schéma standard

Pour configurer le contrôleur CMC pour la connexion Active Directory :

1. Sur un serveur Active Directory (contrôleur de domaine), ouvrez le **snap-in Utilisateurs et ordinateurs Active Directory**.
2. En utilisant l'interface Web CMC ou de RACADM :
   a. Créez un groupe ou sélectionnez un groupe existant.
   b. Configurez les privilèges du rôle.
3. Ajoutez l'utilisateur Active Directory comme membre du groupe Active Directory pour qu'il puisse accéder à iDRAC6.

Configuration d'Active Directory avec le schéma standard à l'aide de l'interface Web CMC

REMARQUE : Pour plus d'informations sur les divers champs, voir l'*Aide en ligne CMC*.

1. Dans le volet de gauche, accédez à **Présentation du châssis**, puis cliquez sur **Authentification utilisateur** > **Services d'annuaire**. La page **Services d'annuaire** s'affiche.
2. Sélectionnez **Microsoft Active Directory (Schéma standard)**. Les paramètres à configurer pour le schéma standard sont affichés dans la même page.
3. Dans la section **Paramètres communs** , sélectionnez les éléments suivants :
   - Sélectionnez **Activer Active Directory** et entrez la valeur du délai d'attente pour Active Directory dans le champ **Délai d'attente AD** .
   - Pour obtenir les contrôleurs de domaine Active Directory émanant d'une recherche DNS, sélectionnez l'option **Rechercher les contrôleurs de domaine avec DNS**, puis sélectionnez l'une des options suivantes :
     - Sélectionnez **Domaine utilisateur de l'ouverture de session** pour effectuer la recherche DNS avec le nom de domaine de l'utilisateur d'ouverture de session.
     - Sinon, sélectionnez **Définir un domaine** et saisissez le nom de domaine à utiliser pour la recherche DNS.
   - Pour que le CMC puisse utiliser les adresses du serveur de contrôleur de domaine Active Directory, sélectionnez **Spécifier les adresses du contrôleur de domaine** . Ces adresses des serveurs sont les adresses des contrôleurs de domaine où les comptes d'utilisateur et les groupes de rôles sont situés.
4. Cliquez sur **Appliquer** pour enregistrer les paramètres.

   REMARQUE : Vous devez appliquer les paramètres avant de continuer. Si vous ne le faites pas, ils sont perdus lorsque vous passez à une autre page.
5. Dans la section **Groupes de rôles avec schéma standard** , cliquez sur un **Groupe de rôles**. La page **Configurer le groupe de rôles** s'affiche.
6. Spécifiez le nom, le domaine et les privilèges d'un groupe de rôles.
7. Cliquez sur **Appliquer** pour enregistrer les paramètres de groupe de rôles, puis cliquez sur **Retour à la page Configuration**.
8. Si vous avez activé la validation de certificat, vous devez téléverser le certificat autosigné racine de la forêt de domaines vers CMC. Dans la section **Gérer les certificats**, entrez le chemin du fichier de certificat ou naviguez jusqu'à ce fichier. Cliquez sur **Téléverser** pour téléverser le fichier vers CMC.

REMARQUE : La valeur Chemin de fichier indique le chemin relatif du fichier de certificat que vous téléversez. Vous devez saisir le chemin absolu de ce fichier, à savoir son chemin complet, son nom et son extension.

Les certificats SSL des contrôleurs de domaine doivent être signés par le certificat racine signé par l'autorité de certification. Ce certificat racine doit être disponible sur la station de gestion qui accède à CMC.

9. Si vous avez activé la connexion directe (SSO), accédez à la section **Fichier keytab Kerberos**, cliquez sur **Parcourir**, spécifiez le fichier keytab, puis cliquez sur **Téléverser**. Une fois l'opération terminée, un message s'affiche, signalant la réussite ou l'échec du téléversement.
10. Cliquez sur **Appliquer**. Le serveur Web CMC redémarre automatiquement lorsque vous cliquez sur **Appliquer**.
11. Déconnectez-vous de CMC, puis reconnectez-vous pour achever la configuration d'Active Directory pour CMC.
12. Sélectionnez **Châssis** dans l'arborescence système et naviguez jusqu'à l'onglet **Réseau**. La page **Configuration réseau** s'affiche.
13. Sous **Paramètres réseau**, si vous avez activé l'option **Utiliser DHCP (pour l'adresse IP de l'interface réseau CMC)**, sélectionnez **Utiliser DHCP pour obtenir des adresses de serveur DNS**.

    Pour saisir manuellement l'adresse IP d'un serveur DNS, désélectionnez l'option **Utiliser DHCP pour obtenir des adresses de serveur DNS**, puis entrez les adresses IP des serveurs DNS primaire et secondaire.
14. Cliquez sur **Appliquer les changements**.

    La configuration du schéma standard d'Active Directory CMC est terminée.

Configuration d'Active Directory avec le schéma standard à l'aide de l'interface RACADM

Depuis l'invite de commande RACADM, exécutez les commandes suivantes :

- Utilisation de la commande `config` :

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1
racadm config -g cfgActiveDirectory -o cfgADType 2
racadm config -g cfgStandardSchema -i <index> -o cfgSSADRoleGroupName <common name of the
role group>
racadm config -g cfgStandardSchema -i <index> -o cfgSSADRoleGroupDomain <fully qualified
domain name>
racadm config -g cfgStandardSchema -i <index> -o cfgSSADRoleGroupPrivilege <Bit Mask Value
for specific RoleGroup permissions>
```

```
racadm config -g cfgActiveDirectory -o cfgADDomainController1 <fully qualified domain name
or IP address of the domain controller>
racadm config -g cfgActiveDirectory -o cfgADDomainController2 <fully qualified domain name
or IP address of the domain controller>
racadm config -g cfgActiveDirectory -o cfgADDomainController3 <fully qualified domain name
or IP address of the domain controller>
```

REMARQUE : Entrez le nom de domaine complet qualifié du contrôleur de domaine et non pas celui du domaine. Par exemple, entrez `servername.dell.com` et non pas `dell.com`.

REMARQUE :

Au moins une des trois adresses doit être définie. Le contrôleur CMC tente de se connecter à chacune d'elles l'une après l'autre jusqu'à ce qu'il puisse établir une connexion. Avec le schéma standard, il s'agit des adresses des contrôleurs de domaine où se trouvent les comptes d'utilisateur et les groupes de rôles.

```
racadm config -g cfgActiveDirectory -o cfgADGlobalCatalog1 <fully qualified domain name or
IP address of the domain controller>
racadm config -g cfgActiveDirectory -o cfgADGlobalCatalog2 <fully qualified domain name or
IP address of the domain controller>
racadm config -g cfgActiveDirectory -o cfgADGlobalCatalog3 <fully qualified domain name or
IP address of the domain controller>
```

REMARQUE : Le serveur de catalogue global est uniquement nécessaire pour le schéma standard lorsque les comptes d'utilisateur et les groupes de rôles se trouvent dans des domaines différents. S'il existe plusieurs domaines, seul le groupe Universel peut être utilisé.

REMARQUE : Le nom de domaine complet qualifié ou l'adresse IP que vous spécifiez dans ce champ doit correspondre au champ Objet ou Autre nom de l'objet de votre certificat de contrôleur de domaine si la validation de certificat est activée.

Pour désactiver la validation de certificat durant l'établissement de liaison SSL, entrez la commande RACADM suivante :

- Utilisation de la commande `config` : `racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0`

Dans ce cas, il n'est pas nécessaire de téléverser le certificat CA (Certificate Authority).

Pour désactiver la validation de certificat au cours de la négociation SSL (facultatif) :

- Utilisation de la commande `config` : `racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1`

Dans ce cas, vous devez téléverser le certificat d'autorité de certification en utilisant la commande RACADM suivante :

```
racadm sslcertupload -t 0x2 -f <ADS root CA certificate>
```

REMARQUE : Si la validation de certificat est activée, définissez les adresses de serveur de contrôleur de domaine et le nom de domaine complet qualifié du catalogue global. Vérifiez que le service DNS est correctement configuré.

Présentation d'Active Directory avec schéma étendu

Pour utiliser la solution de schéma étendu, vous devez disposer de l'extension de schéma Active Directory.

Extensions de schéma Active Directory

Les données Active Directory sont une base de données distribuée d'*attributs* et de *classes*. Le schéma Active Directory contient les règles qui déterminent le type de données qu'il est possible d'ajouter ou d'inclure dans la base de données. La classe Utilisateur est un exemple de classe stockée dans la base de données. Le prénom, le nom, le numéro de téléphone, etc., sont des exemples d'attributs de cette classe.

Vous pouvez étendre la base de données Active Directory en ajoutant vos propres *attributs* et *classes* uniques pour répondre à des besoins spécifiques. Dell a étendu le schéma pour inclure les changements nécessaires à la prise en charge de l'authentification et de l'autorisation de la gestion à distance dans Active Directory.

Chaque *attribut* ou chaque *classe* ajoutés à un schéma Active Directory existant doivent être définis avec un ID unique. Pour maintenir l'unicité des ID dans le secteur, Microsoft gère une base de données d'identificateurs d'objet Active Directory (OID) pour que, lorsque les entreprises ajoutent des extensions au schéma, ces extensions soient garanties comme uniques et n'entrent pas en conflit. Pour étendre le schéma dans l'annuaire Active Directory de Microsoft, Dell a reçu des OID uniques, des extensions de nom uniques et des ID d'attribut liés de manière unique pour les attributs et les classes ajoutés au service d'annuaire :

- Extension Dell : `dell`
- OID de base Dell : `1.2.840.113556.1.8000.1280`
- Plage d'ID de lien RAC : `12070` à `12079`

Présentation des extensions de schéma

Dell a étendu le schéma pour inclure les propriétés *Association*, *Périphériques* et *Privilège*. La propriété *Association* permet de lier les utilisateurs ou groupes possédant un ensemble de privilèges spécifiques à un ou plusieurs périphériques RAC. Ce modèle fournit à l'administrateur une souplesse optimale concernant les diverses combinaisons d'utilisateurs, de privilèges RAC et de périphériques RAC sur le réseau, sans rendre le système plus complexe.

Si vous disposez sur le réseau de deux CMC à intégrer à Active Directory pour l'authentification et l'autorisation, créez au moins un objet Association et un objet Périphérique RAC pour chaque CMC. Vous pouvez créer plusieurs objets Association, et lier chacun à autant d'utilisateurs, de groupes d'utilisateurs ou d'objets Périphérique RAC que vous le souhaitez. Les utilisateurs et les objets Périphérique RAC peuvent être membres de n'importe quel domaine dans l'entreprise.

Cependant, chaque objet Association ne peut être lié (ou ne peut lier des utilisateurs, des groupes d'utilisateurs ou des objets Périphérique RAC) qu'à un seul objet Privilège. Cet exemple permet à l'administrateur de contrôler chacun des privilèges de l'utilisateur sur des CMC donnés.

L'objet Périphérique RAC est le lien que le logiciel RAC utilise pour envoyer à Active Directory des requêtes d'authentification et d'autorisation. Lorsqu'un RAC est ajouté au réseau, l'administrateur doit configurer ce RAC et son objet Périphérique avec le nom de son annuaire Active Directory, afin que les utilisateurs puissent employer l'authentification et l'autorisation Active Directory. L'administrateur doit également ajouter le RAC à au moins un objet Association pour permettre l'authentification des utilisateurs.

REMARQUE : L'objet Privilège RAC s'applique au contrôleur CMC.

Vous pouvez créer un nombre illimité (ou aussi faible que vous le souhaitez) d'objets Association. Cependant, vous devez créer au moins un objet Association et disposer d'un objet Périphérique RAC pour chaque RAC (CMC) du réseau à intégrer à Active Directory.

L'objet Association permet de créer un nombre quelconque d'utilisateurs, de groupes et d'objets Périphérique RAC. Toutefois, l'objet Association contient un seul objet Privilège pour chaque objet Association. L'objet Association connecte les *Utilisateurs* possédant des *Privilèges* sur les RAC (CMC).

De plus, vous pouvez configurer des objets Active Directory dans un même domaine ou dans plusieurs domaines. Par exemple, vous disposez de deux contrôleurs CMC (RAC 1 et RAC 2) et de trois utilisateurs Active Directory existants (utilisateur 1, utilisateur 2 et utilisateur 3). Vous souhaitez attribuer à l'utilisateur 1 et à l'utilisateur 2 un privilège Administrateur sur les deux contrôleurs CMC, et donner à l'utilisateur 3 le privilège Connexion sur la carte RAC 2.

Lors de l'ajout de groupes universels de domaines distincts, créez un objet Association avec une étendue universelle. Les objets Association par défaut créés par l'utilitaire Dell Schema Extender sont des groupes locaux de domaines et ils ne fonctionnent pas avec les groupes universels des autres domaines.

Pour configurer les objets pour le scénario de domaine unique :

1. Créez deux objets Association.
2. Créez deux objets Périphérique RAC, RAC1 et RAC2, pour représenter les deux CMC.
3. Créez deux objets Privilège, Priv1 et Priv2 ; Priv1 disposant de tous les privilèges (administrateur) et Priv2 disposant des privilèges d'ouverture de session.
4. Groupez Utilisateur1 et Utilisateur2 dans le Groupe1.
5. Ajoutez Groupe1 comme membre de l'objet Association 1 (A01), Priv1 comme objet Privilège dans A01, et RAC1 et RAC2 comme périphériques RAC dans A01.
6. Ajoutez Utilisateur3 comme membre de l'objet Association 2 (A02), Priv2 comme objet Privilège dans A02 et RAC2 comme périphérique RAC dans A02.

Pour configurer les objets pour le scénario de domaines multiples :

1. Vérifiez que la fonction de forêt de domaines est en mode natif ou Windows 2003.
2. Créez deux objets Association, nommés A01 (étendue Universel) et A02, dans n'importe quel domaine. La figure « Configuration des objets Active Directory dans plusieurs domaines » montre les objets de Domaine2.
3. Créez deux objets Périphérique RAC, RAC1 et RAC2, pour représenter les deux CMC.
4. Créez deux objets Privilège, Priv1 et Priv2 ; Priv1 disposant de tous les privilèges (administrateur) et Priv2 disposant des privilèges d'ouverture de session.
5. Placez utilisateur1 et utilisateur2 dans Groupe1. L'étendue de Groupe1 doit être Universel.
6. Ajoutez Groupe1 comme membre de l'objet Association 1 (A01), Priv1 comme objet Privilège dans A01, et RAC1 et RAC2 comme périphériques RAC dans A01.
7. Ajoutez Utilisateur3 comme membre de l'objet Association 2 (A02), Priv2 comme objet Privilège dans A02 et RAC2 comme périphérique RAC dans A02.

Configuration du schéma étendu Active Directory

Pour configurer Active Directory afin qu'il accède à CMC :

1. Développez le schéma d'Active Directory.
2. Développez le snap-in Utilisateurs et ordinateurs Active Directory.
3. Ajoutez des utilisateurs CMC et leurs privilèges à Active Directory.
4. Activez SSL sur chaque contrôleur de domaine.
5. Définissez les propriétés Active Directory du contrôleur CMC en utilisant l'interface Web ou RACADM.

Extension du schéma Active Directory

L'extension du schéma Active Directory ajoute une unité organisationnelle Dell, des classes et des attributs de schéma, des exemples de privilèges et des objets Association au schéma Active Directory. Avant d'étendre le schéma, vérifiez que vous disposez des privilèges d'administration de schéma dans le rôle de propriétaire FSMO (Flexible Single Master Operation) du contrôleur de domaine principal dans la forêt de domaines.

Vous pouvez étendre votre schéma en utilisant l'une des méthodes suivantes :

- utilitaire Dell Schema Extender ;
- fichier script LDIF.

Si vous utilisez le fichier script LDIF, l'unité organisationnelle Dell n'est pas ajoutée au schéma.

Les fichiers LDIF et Dell Schema Extender se trouvent sur votre DVD *Dell Systems Management Tools and Documentation* dans les répertoires respectifs suivants :

- `DVDdrive:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools \Remote_Management_Advanced\LDIF_Files`
- `<lecteur DVD>:\SYSMGMT\ManagementStation\support\OMActiveDirector y_Tools \Remote_Management_Advanced\Schema Extender`

Pour utiliser les fichiers LDIF, consultez les instructions des notes de mise à jour qui se trouvent dans le répertoire `LDIF_Files`.

Vous pouvez copier et exécuter Schema Extender ou les fichiers LDIF depuis n'importe quel emplacement.

Utilisation de Dell Schema Extender

PRÉCAUTION : Dell Schema Extender utilise le fichier SchemaExtenderOem.ini. Pour assurer le bon fonctionnement de Dell Schema Extender, ne modifiez pas le nom de ce fichier.

1. Dans l'écran d'**Accueil**, cliquez sur **Suivant**.
2. Lisez l'avertissement pour bien le comprendre, puis cliquez sur **Suivant**.
3. Sélectionnez **Utiliser les références d'ouverture de session actuelles** ou saisissez un nom d'utilisateur et un mot de passe ayant des droits d'administrateur de schéma.
4. Cliquez sur **Suivant** pour exécuter Dell Schema Extender.
5. Cliquez sur **Terminer**.

   Le schéma est étendu. Pour vérifier l'extension du schéma, utilisez la console MMC et le snap-in de schéma Active Directory pour vérifier l'existence des classes et attributs. Pour plus d'informations sur les classes et attributs, voir « Classes et attributs ». Consultez la documentation Microsoft pour plus d'informations sur l'utilisation de MMC et du snap-in de schéma Active Directory.

Classes et attributs

Tableau 24. Définitions de classe pour les classes ajoutées au schéma Active Directory

Nom de classe	Numéro d'identification d'objet (OID) attribué
delliDRACDevice	1.2.840.113556.1.8000.1280.1.7.1.1
delliDRACAssociation	1.2.840.113556.1.8000.1280.1.7.1.2
dellRAC4Privileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

Tableau 25. dellRacDevice Class

OID	1.2.840.113556.1.8000.1280.1.7.1.1
Description	Représente le périphérique Dell RAC. Vous devez configurer RAC en tant que delliDRACDevice dans Active Directory. Cette configuration permet à CMC d'envoyer des requêtes LDAP (Lightweight Directory Access Protocol - Protocole léger d'accès à l'annuaire) à Active Directory.
Type de classe	Classe structurelle
SuperClasses	dellProduct
Attributs	dellSchemaVersion dellRacType

Tableau 26. delliDRACAssociationObject Class

OID	1.2.840.113556.1.8000.1280.1.7.1.2
Description	Représente l'objet Association Dell. Cet objet fournit la connexion entre les utilisateurs et les périphériques.
Type de classe	Classe structurelle
SuperClasses	Groupe
Attributs	dellProductMembers

Tableau 26. delliDRACAssociationObject Class (suite)

OID	1.2.840.113556.1.8000.1280.1.7.1.2
	dellPrivilegeMember

Tableau 27. dellRAC4Privileges Class

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Description	Définit les privilèges (droits d'autorisation) du périphérique CMC.
Type de classe	Classe auxiliaire
SuperClasses	Aucun
Attributs	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsTestAlertUser dellIsDebugCommandAdmin dellPermissionMask1 dellPermissionMask2

Tableau 28. Classe dellPrivileges

OID	1.2.840.113556.1.8000.1280.1.1.1.4
Description	Fait office de classe de conteneurs pour les privilèges Dell (droits d'autorisation).
Type de classe	Classe structurelle
SuperClasses	Utilisateur
Attributs	dellRAC4Privileges

Tableau 29. Classe dellProduct

OID	1.2.840.113556.1.8000.1280.1.1.1.5
Description	Classe principale à partir de laquelle tous les produits Dell sont dérivés.
Type de classe	Classe structurelle
SuperClasses	Ordinateur
Attributs	dellAssociationMembers

Tableau 30. Liste des attributs ajoutés au schéma Active Directory

OID attribué/Identifiant d'objet de syntaxe	Valeur unique
Attribut : `dellPrivilegeMember` **Description** : liste des objets `dellPrivilege` appartenant à cet attribut. **OID** : 1.2.840.113556.1.8000.1280.1.1.2.1 **Nom unique** : (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
Attribut : `dellProductMembers` **Description** : liste des objets `dellRacDevices` appartenant à ce rôle. Cet attribut est le lien vers l'avant qui correspond au lien vers l'arrière `dellAssociationMembers`. **ID de lien** : 12070	FALSE

Tableau 30. Liste des attributs ajoutés au schéma Active Directory (suite)

OID attribué/Identifiant d'objet de syntaxe	Valeur unique
OID : 1.2.840.113556.1.8000.1280.1.1.2.2 **Nom unique** : (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
Attribut : `dellIsCardConfigAdmin` **Description** : VRAI si l'utilisateur possède les droits Configuration de la carte sur le périphérique. **OID** : 1.2.840.113556.1.8000.1280.1.1.2.4 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut : `dellIsLoginUser` **Description** : VRAI si l'utilisateur possède les droits Ouverture de session sur le périphérique. **OID** : 1.2.840.113556.1.8000.1280.1.1.2.3 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut : `dellIsUserConfigAdmin` **Description** : TRUE (VRAI) si l'utilisateur possède les droits d'Administrateur de configuration des utilisateurs sur le périphérique. **OID** : 1.2.840.113556.1.8000.1280.1.1.2.5 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut : `dellIsLogClearAdmin` **Description** : TRUE (VRAI) si l'utilisateur possède les droits d'Administrateur d'effacement des journaux sur le périphérique. **OID** : 1.2.840.113556.1.8000.1280.1.1.2.6 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut : `dellIsServerResetUser` **Description** : TRUE (VRAI) si l'utilisateur possède les droits de Réinitialisation du serveur sur le périphérique. **OID** : 1.2.840.113556.1.8000.1280.1.1.2.7 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut : `dellIsTestAlertUser` **Description** : TRUE (VRAI) si l'utilisateur possède les droits d'Utilisateur et test d'alertes sur le périphérique. **OID** : 1.2.840.113556.1.8000.1280.1.1.2.10 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut : `dellIsDebugCommandAdmin` **Description** : TRUE (VRAI) si l'utilisateur possède les droits d'Administrateur de commandes de débogage sur le périphérique. **OID** : 1.2.840.113556.1.8000.1280.1.1.2.11 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut : `dellSchemaVersion` **Description** : la version actuelle du schéma est utilisée pour mettre le schéma à jour. **OID** : 1.2.840.113556.1.8000.1280.1.1.2.12 Chaîne de non-prise en compte de la casse (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
Attribut : `dellRacType`	TRUE

Tableau 30. Liste des attributs ajoutés au schéma Active Directory (suite)

OID attribué/Identifiant d'objet de syntaxe	Valeur unique
Description : cet attribut est le type de RAC actuel pour l'objet dellRacDevice et le lien vers l'arrière correspondant au lien vers l'avant dellAssociationObjectMembers. **OID** : 1.2.840.113556.1.8000.1280.1.1.2.13 Chaîne de non-prise en compte de la casse (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	
Attribut : `dellAssociationMembers` **Description** : liste des objets dellAssociationObjectMembers appartenant à ce rôle. Cet attribut est le lien vers l'arrière vers l'attribut dellProductMembers Linked. **ID de lien** : 12071 **OID** : 1.2.840.113556.1.8000.1280.1.1.2.14 Nom distingué (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
Attribut : `dellPermissionsMask1` **OID** : 1.2.840.113556.1.8000.1280.1.6.2.1 Integer (LDAPTYPE_INTEGER)	
Attribut : `dellPermissionsMask2` **OID** : 1.2.840.113556.1.8000.1280.1.6.2.2 Integer (LDAPTYPE_INTEGER)	

Installation de l'extension Dell dans le snap-in Utilisateurs et ordinateurs Microsoft Active Directory

Lorsque vous étendez le schéma dans Active Directory, vous devez également étendre le snap-in Utilisateurs et ordinateurs Active Directory pour que l'administrateur puisse gérer les périphériques RAC (CMC), les utilisateurs et les groupes d'utilisateurs, les associations RAC et les privilèges RAC.

Lorsque vous installez le logiciel de gestion de systèmes à l'aide du DVD *Dell Systems Management Tools and Documentation*, vous pouvez étendre le snap-in en sélectionnant l'option **Snap-in Utilisateurs et ordinateurs Active Directory** pendant l'installation. Voir le *Dell OpenManage Software Quick Installation Guide* (Guide d'installation rapide du logiciel Dell OpenManage) pour plus d'informations sur l'installation du logiciel de gestion de systèmes. Pour les systèmes d'exploitation Windows 64 bits, le programme d'installation du snap-in se trouve dans `<DVDdrive>:\SYSMGMT\ManagementStation\support\OMActiveDirect ory_SnapIn644.`

Pour des informations supplémentaires sur le snap-in Utilisateurs et ordinateurs Active Directory, consultez la documentation Microsoft.

Ajout d'utilisateurs et de privilèges CMC à Active Directory

Le snap-in d'extension Dell Utilisateurs et ordinateurs Active Directory vous permet d'ajouter des utilisateurs et privilèges CMC en créant des objets Périphérique RAC, Association et Privilège. Pour ajouter chaque objet, procédez comme suit :

- Créez un objet Périphérique RAC
- Créez un objet Privilège.
- Créez un objet Association.
- Ajoutez des objets à un objet Association.

Création d'un objet Périphérique RAC

Pour créer un objet Périphérique RAC :

1. Dans la fenêtre **Racine de la console MMC**, cliquez avec le bouton droit sur un conteneur.
2. Sélectionnez **Nouveau** > **Dell Remote Management Object Advanced**.
3. Sur la page **Nouvel objet**, entrez le nom du nouvel objet. Ce nom doit être identique au nom CMC que vous entrez dans l'étape Configuration d'Active Directory avec le schéma standard en utilisant l'interface Web.
4. Sélectionnez **Objet Périphérique RAC**, puis cliquez sur **OK**.

Création d'un objet Privilège

Pour créer un objet Privilège :

REMARQUE : Vous devez créer un objet Privilège dans le même domaine que l'objet Association associé.

1. Dans la fenêtre **Racine de la console MMC**, cliquez avec le bouton droit sur un conteneur.
2. Sélectionnez **Nouveau** > **Dell Remote Management Object Advanced**.
3. Sur la page **Nouvel objet**, entrez le nom du nouvel objet.
4. Sélectionnez **Objet Privilège**, puis cliquez sur **OK**.
5. Cliquez avec le bouton droit de la souris sur l'objet Privilège que vous avez créé et sélectionnez **Propriétés**.
6. Cliquez sur l'onglet **Privilèges RAC**, et attribuez les privilèges voulus à l'utilisateur ou au groupe. Pour plus d'informations sur les privilèges utilisateur CMC, voir « Types d'utilisateur ».

Création d'un objet Association

L'objet Association est dérivé d'un groupe et doit contenir un type de groupe. L'étendue d'association spécifie le type de groupe de sécurité de l'objet Association. Lorsque vous créez un objet Association, choisissez l'étendue d'association qui s'applique au type des objets que vous prévoyez d'ajouter. Par exemple, si vous sélectionnez Universel, les objets Association sont disponibles uniquement lorsque le domaine Active Directory fonctionne en mode natif ou supérieur.

Pour créer un objet Association :

1. Dans la fenêtre **Racine de la console (MMC)**, cliquez avec le bouton droit sur un conteneur.
2. Sélectionnez **Nouveau** > **Dell Remote Management Object Advanced**.
3. Sur la page **Nouvel objet**, entrez le nom du nouvel objet et sélectionnez **Objet Association**.
4. Sélectionnez l'étendue de l'**objet Association**, puis cliquez sur **OK**.

Ajout d'objets à un objet Association

Utilisez la fenêtre **Propriétés de l'objet Association** pour associer des utilisateurs ou groupes d'utilisateurs, des objets Privilège et des périphériques ou groupes de périphériques RAC. Si vous utilisez Windows 2000 ou une version ultérieure, utilisez des groupes universels pour couvrir les domaines avec les objets Utilisateur ou RAC.

Vous pouvez ajouter des groupes d'utilisateurs et de périphériques RAC.

Ajout d'utilisateurs ou de groupes d'utilisateurs

Pour ajouter des utilisateurs ou des groupes d'utilisateurs :

1. Cliquez avec le bouton droit de la souris sur **l'objet Association** et sélectionnez **Propriétés**.
2. Sélectionnez l'onglet **Utilisateurs** et cliquez sur **Ajouter**.
3. Entrez le nom de l'utilisateur ou du groupe d'utilisateurs, puis cliquez sur **OK**.

Ajout de privilèges

Pour ajouter des privilèges :

1. Sélectionnez l'onglet **Objet Privilège** et cliquez sur **Ajouter**.
2. Entrez le nom de l'objet Privilège et cliquez sur **OK**.

   Cliquez sur l'onglet **Objet Privilège** pour ajouter l'objet Privilège à l'objet Association qui définit les privilèges de l'utilisateur ou du groupe d'utilisateurs lors de l'authentification auprès d'un périphérique DRAC. Vous ne pouvez ajouter qu'un seul objet Privilège à chaque objet Association.

Ajout de périphériques RAC ou de groupes de périphériques RAC

Pour ajouter des périphériques RAC ou des groupes de périphériques RAC :

1. Sélectionnez l'onglet **Produits** et cliquez sur **Ajouter**.
2. Entrez le nom des périphériques RAC ou des groupes de périphériques RAC, puis cliquez sur **OK**.
3. Dans la fenêtre **Propriétés**, cliquez sur **Appliquer**, puis sur **OK**.

   Cliquez sur l'onglet **Produits** pour ajouter un ou plusieurs périphériques RAC à l'objet Association. Les objets associés spécifient les périphériques RAC connectés au réseau qui sont disponibles pour les utilisateurs ou groupes d'utilisateurs définis. Il est possible d'ajouter plusieurs périphériques RAC à un objet Association.

Configuration d'Active Directory avec le schéma étendu à l'aide de l'interface Web CMC

Pour configurer Active Directory avec le schéma étendu dans l'interface Web CMC :

REMARQUE : Pour plus d'informations sur les champs, voir l'*Aide en ligne*.

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Authentification utilisateur** > **Présentation du châssis** > **Services d'annuaire**.
2. Sélectionnez **Microsoft Active Directory (Schéma étendu)**.
   Les paramètres devant être configurés pour le schéma étendu s'affichent sur la même page.
3. Dans la section **Paramètres communs** , sélectionnez les éléments suivants :
   - Sélectionnez **Activer Active Directory** et entrez la valeur du délai d'attente pour Active Directory dans le champ **Délai d'attente AD** .
   - Pour obtenir les contrôleurs de domaine Active Directory émanant d'une recherche DNS, sélectionnez l'option **Rechercher les contrôleurs de domaine avec DNS**, puis sélectionnez l'une des options suivantes :
     - Sélectionnez **Domaine utilisateur de l'ouverture de session** pour effectuer la recherche DNS avec le nom de domaine de l'utilisateur d'ouverture de session.
     - Sinon, sélectionnez **Définir un domaine** et saisissez le nom de domaine à utiliser pour la recherche DNS.
   - Pour que le CMC puisse utiliser les adresses du serveur de contrôleur de domaine Active Directory, sélectionnez **Spécifier les adresses du contrôleur de domaine** . Il s'agit des adresses des contrôleurs de domaine où l'objet Périphérique CMC et les objets associés sont situés.
4. Cliquez sur **Appliquer** pour enregistrer les paramètres.

   REMARQUE : Vous devez appliquer les paramètres avant de continuer. Si vous ne le faites pas, ils sont perdus lorsque vous passez à une autre page.
5. Dans la section **Paramètres du schéma étendu**, entrez le nom de périphérique et le nom de domaine CMC.
6. Si vous avez activé la validation de certificat, vous devez téléverser le certificat autosigné racine de la forêt de domaines vers CMC. Dans la section **Gérer les certificats**, entrez le chemin du fichier de certificat ou naviguez jusqu'à ce fichier. Cliquez sur **Téléverser** pour téléverser le fichier vers CMC.

   REMARQUE : La valeur `File Path` indique le chemin relatif du fichier de certificat que vous téléversez. Vous devez saisir le chemin absolu de ce fichier, à savoir son chemin complet, son nom et son extension.

   Les certificats SSL des contrôleurs de domaine doivent être signés par le certificat racine signé par l'autorité de certification. Ce certificat racine doit être disponible sur la station de gestion qui accède à CMC.

   PRÉCAUTION : La validation de certificat SSL est requise par défaut. Il est recommandé de ne pas désactiver ce certificat.
7. Si vous avez activé la connexion directe (SSO), accédez à la section Fichier keytab Kerberos, cliquez sur **Parcourir**, spécifiez le fichier keytab, puis cliquez sur **Téléverser**. Une fois l'opération terminée, un message s'affiche, signalant la réussite ou l'échec du téléversement.
8. Cliquez sur **Appliquer**.
   Le serveur Web CMC redémarre automatiquement lorsque vous cliquez sur **Appliquer**.
9. Connectez-vous à l'interface Web CMC.
10. Sélectionnez **Châssis** dans l'arborescence système,puis cliquez sur l'onglet **Réseau** et sur le sous-onglet **Réseau**. La page **Configuration du réseau** s'affiche.
11. Si l'option **Utiliser DHCP** est activée pour l'adresse IP de l'interface réseau CMC, effectuez l'une des opérations suivantes :
    - Sélectionnez l'option **Utiliser DHCP pour obtenir les adresses de serveur DNS** pour que le serveur DHCP puisse obtenir les adresses de serveur DNS automatiquement.
    - Configurez manuellement une adresse IP de serveur DNS en laissant la case **Utiliser DHCP pour obtenir des adresses de serveur DNS** décochée puis en tapant vos adresses IP de serveur DNS principal et d'autre serveur DNS dans les champs fournis à cet effet.
12. Cliquez sur **Appliquer les changements**.
    Les paramètres Active Directory du mode Schéma étendu sont configurés.

Configuration d'Active Directory avec le schéma étendu à l'aide de l'interface RACADM

Pour configurer Active Directory CMC avec le schéma étendu en utilisant les commandes RACADM, ouvrez une invite de commande et entrez les commandes suivantes dans l'invite de commande :

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1
racadm config -g cfgActiveDirectory -o cfgADType 1
racadm config -g cfgActiveDirectory -o cfgADRacName <RAC common name>
racadm config -g cfgActiveDirectory -o cfgADRacDomain < fully qualified rac domain name >
racadm config -g cfgActiveDirectory -o cfgADDomainController1 < fully qualified domain name
or IP Address of the domain controller >
racadm config -g cfgActiveDirectory -o cfgADDomainController2 < fully qualified domain name
or IP Address of the domain controller >
racadm config -g cfgActiveDirectory -o cfgADDomainController3 < fully qualified domain name
or IP Address of the domain controller >
```

REMARQUE : Vous devez définir au moins une des trois adresses. Le contrôleur CMC tente de se connecter à chacune des adresses définies l'une après l'autre jusqu'à ce qu'il établisse une connexion. Avec le schéma étendu, il s'agit du nom de domaine qualifié ou des adresses IP des contrôleurs de domaine où se trouve le périphérique iDRAC7.

Pour désactiver la validation de certificat au cours de la négociation (facultatif) :

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0
```

REMARQUE : Dans ce cas, il n'est pas nécessaire de téléverser un certificat d'autorité de certification.

Pour désactiver la validation de certificat au cours de la négociation SSL (facultatif) :

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1
```

Dans ce cas, vous devez téléverser un certificat d'autorité de certification :

```
racadm sslcertupload -t 0x2 -f < ADS root CA certificate >
```

REMARQUE : Si la validation de certificat est activée, définissez les adresses Serveur contrôleur de domaine et le nom de domaine qualifié. Vérifiez que le service DNS est correctement défini.

L'utilisation de la commanRACADM suivante peut être facultative :

```
racadm sslcertdownload -t 0x1 -f < RAC SSL certificate >
```

Configuration d'utilisateurs LDAP générique

CMC fournit une solution générique permettant de prendre en charge l'authentification LDAP (Lightweight Directory Access Protocol - Protocole léger d'accès aux annuaires). Cette fonction ne requiert aucune extension de schéma dans les services d'annuaire.

L'administrateur CMC peut désormais intégrer les connexions aux serveurs LDAP dans CMC. Cette intégration nécessite des opérations de configuration à la fois sur le serveur LDAP et sur le CMC. Sur le serveur LDAP, vous utilisez un objet de groupe standard comme groupe de rôles. Tout utilisateur possédant un accès à CMC devient membre du groupe de rôles. Les privilèges sont toujours stockés dans CMC pour l'autorisation, comme avec la configuration de schéma standard Active Directory prise en charge.

Pour autoriser l'utilisateur LDAP à accéder à une carte CMC spécifique, vous devez configurer le nom du groupe de rôles et son nom de domaine sur la carte CMC concernée. Vous pouvez configurer un maximum de cinq groupes de rôles pour chaque CMC. Il est possible d'ajouter un utilisateur à plusieurs groupes dans le service d'annuaire. Si un utilisateur est membre de plusieurs groupes, il obtient les privilèges de tous les groupes concernés.

Pour plus informations sur le niveau de privilèges des groupes de rôle et sur les paramètres par défaut de ces groupes, voir « Types d'utilisateur ».

Configuration de l'annuaire LDAP générique pour accéder à CMC

L'implémentation LDAP générique du contrôleur CMC utilise deux phases pour autoriser l'accès d'un utilisateur : authentification et autorisation.

Authentification des utilisateurs LDAP

Certains serveurs d'annuaire nécessitent une liaison pour pouvoir rechercher un serveur LDAP.

Pour authentifier un utilisateur :

1. Si vous le souhaitez, vous pouvez effectuer la liaison avec le service de répertoire. Par défaut, la liaison est anonyme.

   REMARQUE : Les serveurs de répertoire Windows ne permettent pas de se connecter de façon anonyme. Par conséquent, saisissez le nom de domaine et le mot de passe pour la liaison.

2. Recherchez l'utilisateur en fonction de ses identifiants de connexion. L'attribut par défaut est `uid`. Si plusieurs objets sont trouvés, le processus renvoie une erreur.
3. Annulez la liaison et effectuez une liaison avec le DN et le mot de passe de l'utilisateur. Si le système ne peut pas établir de liaison, la connexion échoue.
4. Si ces étapes réussissent, l'utilisateur est authentifié.

Autorisation des utilisateurs LDAP

Pour autoriser un utilisateur :

1. Recherchez le nom de domaine de l'utilisateur dans chaque groupe défini dans les attributs `member or uniqueMember`. L'administrateur peut configurer un domaine d'utilisateur.
2. Pour chaque groupe d'utilisateurs auquel l'utilisateur appartient, fournissez les droits d'accès et privilèges utilisateur appropriés.

Configuration du service d'annuaire LDAP générique à l'aide de l'interface Web CMC

Pour configurer le service d'annuaire LDAP générique :

REMARQUE : Vous devez disposer du privilège Administrateur de configuration du châssis.

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Authentification utilisateur** > **Services d'annuaire**.
2. Sélectionnez **LDAP générique**.
   Les paramètres à configurer pour le schéma standard sont affichés dans la même page.
3. Paramétrez les options suivantes :

   REMARQUE : Pour plus d'informations sur les champs, voir l'*Aide en ligne*.

   - Paramètres communs
   - Serveur à utiliser avec LDAP :
     - Serveur statique : spécifiez le nom FQDN (Fully Qualified Domain Name, nom de domaine entièrement qualifié) ou l'adresse IP, et le numéro du port LDAP.
     - Serveur DNS : spécifiez le serveur DNS afin de récupérer la liste des serveurs LDAP d'après leur enregistrement SRV dans DNS.

       La requête DNS suivante est effectuée pour les enregistrements SRV :

       ```
       _<Nom du service>._tcp.<Domaine de recherche>
       ```

       où <*Search Domain*> est le domaine racine à utiliser dans la requête et <*Service Name*> est le nom du service à utiliser dans la requête.

       Par exemple :

       ```
       _ldap._tcp.dell.com
       ```

où `ldap` est le nom de service et `dell.com` est le domaine de recherche.

4. Cliquez sur **Appliquer** pour enregistrer les paramètres.

   REMARQUE : Vous devez appliquer les paramètres avant de continuer. Si vous ne le faites pas, ils sont perdus lorsque vous passez à une autre page.

5. Dans la section **Paramètres de groupe**, cliquez sur un **Groupe de rôles**.
6. Dans la page **Définir le groupe de rôles LDAP**, spécifiez le nom de domaine de groupe et les privilèges du groupe de rôles.
7. Cliquez sur **Appliquer** pour enregistrer les paramètres de groupe de rôles, cliquez sur **Retour à la page Configuration**, puis sélectionnez **LDAP générique**.
8. Si vous avez activé l'option **Validation de certificat activée**, vous devez accéder à la section **Gérer les certificats**, spécifier le certificat de CA utilisé pour valider le certificat de serveur LDAP au cours de la reconnaissance mutuelle (handshake) SSL, puis cliquer sur **Téléverser**. Le certificat est téléversé dans CMC et ses détails sont affichés.
9. Cliquez sur **Appliquer**.
   Le service d'annuaire LDAP générique est configuré.

Configuration du service d'annuaire LDAP générique à l'aide de RACADM

Pour configurer le service d'annuaire LDAP, utilisez les objets des groupes RACADM `cfgLdap` et `cfgLdapRoleGroup`.

Il existe de nombreuses options permettant de configurer les connexions LDAP. Dans la plupart des cas, certaines options peuvent être utilisées avec leurs paramètres par défaut.

REMARQUE : Il est vivement recommandé d'utiliser la commande RACADM `testfeature -f LDAP` pour tester les paramètres LDAP lors de la configuration initiale. Cette fonctionnalité prend en charge IPv4 et IPv6.

Les modifications de propriétés requises comprennent l'activation des connexions LDAP, la configuration du nom FQDN (Fully Qualified Domain Name - Nom de domaine entièrement qualifié) ou l'adresse IP du serveur, et la configuration du DN de base du serveur LDAP.

- ```
  $ racadm config -g cfgLDAP -o cfgLDAPEnable 1
  ```
- ```
  $ racadm config -g cfgLDAP -o cfgLDAPServer 192.168.0.1
  ```
- ```
  $ racadm config -g cfgLDAP -o cfgLDAPBaseDN dc=
  company,dc=com
  ```

Le contrôleur CMC peut être configuré pour interroger un serveur DNS afin d'obtenir des enregistrements SRV. Si la propriété `cfgLDAPSRVLookupEnable` est activée, la propriété `cfgLDAPServer` est ignorée. La requête suivante est utilisée pour effectuer une recherche d'enregistrements SRV dans le serveur DNS :

```
_ldap._tcp.domainname.com
```

Dans la requête ci-dessus, `ldap` correspond à la propriété `cfgLDAPSRVLookupServiceName`.

`cfgLDAPSRVLookupDomainName` est configuré comme **nomdedomaine.com**.

Pour plus d'informations sur les commandes RACADM, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX* sur le site **dell.com/support/manuals**.
```

10

Configuration de CMC pour la connexion directe (SSO) ou la connexion par carte à puce

Cette section fournit des informations sur la configuration de CMC pour la connexion par carte à puce et pour la connexion directe (SSO) des utilisateurs Active Directory.

La connexion SSO utilise Kerberos comme méthode d'authentification des utilisateurs qui se connectent automatiquement (ou directement) aux applications, notamment Exchange. Pour la connexion directe, le contrôleur CMC utilise les références du système client mises en cache par le système d'exploitation après votre connexion à l'aide d'un compte Active Directory valide.

L'authentification à deux facteurs fournit un niveau élevé de sécurité, car les utilisateurs doivent disposer à la fois d'un mot de passe (ou code PIN) et d'une carte physique contenant une clé privée ou un certificat numérique. Kerberos utilise ce mécanisme d'authentification à deux facteurs pour permettre aux systèmes de prouver leur authenticité.

REMARQUE : Le choix d'une méthode de connexion ne définit pas les attributs de stratégie concernant les autres interfaces de connexion, comme SSH. Vous devez également définir d'autres attributs de stratégie pour ces autres interfaces. Si vous souhaitez désactiver toutes les autres interfaces de connexion, accédez à la page Services et désactivez toutes les interfaces de connexion (ou certaines).

Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7 et Windows Server 2008 peuvent utiliser Kerberos comme mécanisme d'authentification pour la connexion directe (SSO) et la connexion par carte à puce.

Pour plus d'informations sur Kerberos, visitez le site Web Microsoft.

Sujets :

Configuration système requise

Pour que vous puissiez utiliser l'authentification Kerberos, votre réseau doit inclure les éléments suivants :

- Serveur DNS
- Microsoft Active Directory Server

  REMARQUE : Si vous utilisez Active Directory sous Windows 2003, vérifiez que vous avez installé les derniers Service Packs et correctifs sur le système client. Si vous utilisez Active Directory sous Windows 2008, veillez à installer SP1 avec les correctifs suivants :

  Windows6.0-KB951191-x86.msu pour l'utilitaire KTPASS. Sans ce correctif, l'utilitaire génère des fichiers keytab incorrects.

  Windows6.0-KB957072-x86.msu pour utiliser les transactions GSS_API et SSL pendant une liaison LDAP.
- Centre de distribution de clés Kerberos (fourni avec le logiciel du serveur Active Directory Server)
- Serveur DHCP (recommandé)
- La zone inverse du serveur DNS doit comporter une entrée pour le serveur Active Directory et pour CMC

Systèmes clients

- Pour utiliser uniquement la connexion par carte à puce, votre système client doit comporter la version redistribuable de Microsoft Visual C++ 2005. Pour plus d'informations, visitez le site **www.microsoft.com/downloads/details.aspx?FamilyID=32BC1BEEA3F9-4C13-9C99-220B62A191EE&displaylang=en**.
- Pour la connexion directe ou par carte à puce, le système client doit faire partie du domaine Active Directory et du royaume Kerberos.

CMC

- Chaque CMC doit posséder un compte Active Directory.
- CMC doit faire partie du domaine Active Directory et du royaume Kerberos.

Prérequis pour la connexion directe ou par carte à puce

Les prérequis de configuration de la connexion directe (SSO) ou par carte à puce sont les suivants :

- Configurez le royaume kerberos et le KDC (Key Distribution Center, centre de distribution de clés) pour Active Directory (ksetup).
- Installez une infrastructure NTP et DNS robuste pour éviter les problèmes de dérive d'horloge et de recherche inversée.
- Configurez le CMC avec le groupe de rôles de schéma standard Active Directory, avec des membres autorisés.
- Pour la carte à puce, créez des utilisateurs Active Directory pour chaque CMC, configurés pour utiliser le cryptage DES Kerberos, mais pas la préauthentification.
- Configurez le navigateur pour la connexion directe (SSO) ou par carte à puce.
- Enregistrez les utilisateurs CMC auprès du centre de distribution de clés avec Ktpass (cela génère également une clé pour le téléversement dans le CMC).

Génération d'un fichier Keytab Kerberos

Pour prendre en charge l'authentification de connexion directe (SSO) et par carte à puce, le contrôleur CMC prend en charge le réseau Windows Kerberos. L'outil ktpass (disponible auprès de Microsoft sur le CD/DVD d'installation du serveur) permet de créer des liaisons SPN (Service Principal Name) avec un compte utilisateur et d'exporter les informations de confiance dans un fichier keytab Kerberos de type MIT. Pour plus d'informations sur l'utilitaire ktpass, voir le site Web Microsoft.

Avant de générer un fichier keytab, vous devez créer le compte utilisateur Active Directory à utiliser avec l'option **-mapuser** de la commande ktpass. Vous devez utiliser le même nom que le nom DNS du CMC vers lequel vous téléversez le fichier keytab généré.

Pour générer un fichier keytab à l'aide de l'outil ktpass :

1. Exécutez l'utilitaire *ktpass* sur le contrôleur de domaine (serveur Active Directory) où vous souhaitez associer le contrôleur CMC à un compte utilisateur dans Active Directory.
2. Utilisez la commande `ktpass` suivante pour créer le fichier keytab Kerberos :

```
ktpass -princ HTTP/cmcname.domainname.com@DOMAINNAME.COM -mapuser keytabuser -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -pass * -out c:\krbkeytab
```

REMARQUE : La valeur `cmcname.domainname.com` doit être en minuscules pour respecter la norme RFC et la valeur `@REALM_NAME` doit être en majuscules. Le contrôleur CMC prend également en charge les type de cryptage DES-CBC-MD5 et AES256–SHA1 pour l'authentification Kerberos.

Le fichier keytab est généré et vous devez le téléverser dans CMC.

REMARQUE : Le fichier keytab contient une clé de cryptage et doit être conservé en lieu sûr. Pour plus d'informations sur l'utilitaire *ktpass*, voir le site Web Microsoft.

Configuration du contrôleur CMC pour le schéma Active Directory

Pour plus d'informations sur la configuration du contrôleur CMC pour le schéma standard Active Directory, voir Configuration d'Active Directory pour les schéma étendu.

Pour plus d'informations sur la configuration du contrôleur CMC pour le schéma étendu Active Directory, voir Présentation du schéma étendu Active Directory.

Configuration du navigateur pour la connexion directe (SSO)

La connexion directe est prise en charge dans Internet Explorer versions 6.0 et ultérieures, et dans Firefox versions 3.0 et ultérieures.

REMARQUE : Les instructions suivantes s'appliquent uniquement si CMC utilise la connexion directe avec l'authentification Kerberos.

Internet Explorer

Pour configurer Internet Explorer pour la connexion directe :

1. Dans Internet Explorer, sélectionnez **Outils** > **Options Internet**.
2. Dans l'onglet **Sécurité**, sous **Cliquez sur une zone pour afficher ou modifier les paramètres de sécurité**, sélectionnez **Intranet local**.
3. Cliquez sur **Sites**.
   La boîte de dialogue **Intranet local** s'affiche.
4. Cliquez sur **Avancé**.
   La boîte de dialogue **Paramètres avancés Intranet local** s'affiche.
5. Dans **Ajouter ce site Web à la zone**, saisissez le nom de CMC et le domaine auquel il appartient, puis cliquez sur **Ajouter**.

   REMARQUE : Vous pouvez utiliser un caractère générique (*) pour spécifier tous les périphériques ou utilisateurs du domaine.

Mozilla Firefox

1. Dans Firefox, saisissez `about:config` dans la barre d'adresse.

   REMARQUE : Si le navigateur affiche l'avertissement Ceci risque d'annuler votre garantie, cliquez sur Je ferai attention, promis !.
2. Dans la zone de texte **Filtre**, entrez `negotiate`.
   Le navigateur affiche une liste des noms des préférences qui contiennent le terme negotiate uniquement.
3. Dans la liste, double-cliquez sur **network.negotiate-auth.trusted-uris**.
4. Dans la boîte de dialogue **Saisir une valeur de chaîne**, saisissez le nom de domaine CMC et cliquez sur **OK**.

Configuration du navigateur pour la connexion avec une carte à puce

Internet Explorer : vérifiez que votre navigateur Internet est configuré pour télécharger les plug-ins Active-X.

Configuration de la connexion directe ou par carte à puce CMC pour les utilisateurs Active Directory

Vous pouvez utiliser l'interface Web CMC ou RACADM pour configurer la connexion directe (SSO) CMC ou par carte à puce.

Configuration de la connexion directe ou par carte à puce CMC pour les utilisateurs Active Directory dans l'interface Web

Pour configurer la connexion directe (SSO) ou par carte à puce Active Directory pour CMC :

REMARQUE : Pour plus d'informations sur les options, voir l'*Aide en ligne*.

1. Au cours de la configuration d'Active Directory pour définir un compte d'utilisateur, réalisez les étapes supplémentaires :
   - Pour téléverser le fichier keytab :
   - Pour activer la connexion directe (SSO), sélectionnez l'option **Activer SSO**.
   - Pour activer la connexion par carte à puce, sélectionnez l'option **Activer la connexion par carte à puce**.

     REMARQUE : Si ces deux options sont sélectionnées, toutes les informations hors bande de ligne de commande, y compris SSH (Secure Shell), Telnet, Série et RACADM distant, ne changent pas.
2. Cliquez sur **Appliquer**.

   Les paramètres sont enregistrés.

   Vous pouvez tester Active Directory avec l'authentification Kerberos à l'aide de la commande RACADM suivante :

   ```
   testfeature -f adkrb -u <user>@<domain>
   ```

   où `<user>` correspond à un compte utilisateur Active Directory valide.

   L'aboutissement d'une commande indique que le contrôleur CMC parvient à acquérir les références Kerberos et à accéder au compte Active Directory de l'utilisateur. Si la commande échoue, corrigez l'erreur et exécutez-la à nouveau. Pour plus d'informations, reportez-vous au document *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX) sur le site dell.com/support/manuals.

Téléversement du fichier keytab

Le fichier keytab Kerberos fournit les références de nom d'utilisateur et de mot de passe CMC à Kerberos Data Center (KDC), qui à son tour autorise l'accès à l'annuaire Active Directory. Chaque CMC du royaume Kerberos doit être enregistré auprès de l'annuaire Active Directory et disposer d'un fichier keytab unique.

Vous pouvez téléverser un fichier keytab Kerberos généré sur le serveur Active Directory associé. Pour générer le fichier keytab Kerberos à partir du serveur Active Directory, exécutez l'utilitaire `ktpass.exe`. Ce fichier keytab établit une relation de confiance entre le serveur Active Directory et CMC.

Pour téléverser le fichier keytab :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Authentification utilisateur** > **Services d'annuaire**.
2. Sélectionnez **Microsoft Active Directory (Schéma standard)**.
3. Dans la section **Kerberos Keytab**, cliquez sur **Parcourir**, sélectionnez un fichier keytab et cliquez sur **Téléverser**.

   Une fois le téléversement terminé, un message s'affiche pour indiquer si le fichier keytab a été téléversé.

Configuration de la connexion directe CMC ou de la connexion avec une carte à puce pour les utilisateurs Active Directory à l'aide de RACADM

Outre les étapes exécutées lors de la configuration d'Active Directory, exécutez la commande suivante pour activer la connexion directe (SSO) :

```
racadm config -g cfgActiveDirectory -o cfgADSSOEnable 1
```

Outre les étapes exécutées lors de la configuration d'Active Directory, utilisez les objets suivants pour activer la connexion par carte à puce :

- `cfgSmartCardLogonEnable`
- `cfgSmartCardCRLEnable`

11

Configuration du contrôleur CMC pour utiliser des consoles de ligne de commande

Cette section fournit des informations sur les fonctions de la console de ligne de commande CMC (ou console série/Telnet/Secure Shell) et explique comment configurer le système de façon à pouvoir utiliser la console pour effectuer des actions de gestion de systèmes. Pour plus d'informations sur l'utilisation des commandes RACADM dans le CMC via la console de ligne de commande, reportez-vous au *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX*.

Sujets :

Fonctions de la console de ligne de commande CMC

Le CMC prend en charge les fonctions de console série, Telnet et SSH suivantes :

- Une connexion de client série et un maximum de quatre connexions de clients Telnet simultanées.
- Un maximum de quatre connexions de clients Secure Shell (SSH) simultanées
- Prise en charge des commandes RACADM
- Commande de connexion intégrée qui permet de se connecter à la console série des serveurs et du module d'E/S ; également disponible sous la forme `racadm connect`.
- Modification et historique de ligne de commande
- Contrôle du délai d'expiration de la session sur toutes les interfaces de console

Commandes de l'interface de ligne de commande CMC

Lorsque vous vous connectez à la ligne de commande CMC, vous pouvez entrer les commandes suivantes :

Tableau 31. Commandes de la ligne de commande CMC

Commande	Description
`racadm`	Les commandes RACADM commencent par le mot-clé `racadm`, suivi d'une sous-commande. Pour plus d'informations, reportez-vous au *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX*.
`connect`	Permet de se connecter à la console série d'un serveur ou d'un module d'E/S. Pour plus d'informations, reportez-vous à la section Connexion aux serveurs ou au module d'E/S à l'aide de la commande connect. **REMARQUE : Vous pouvez également utiliser la commande RACADM `connect`.**
`exit`, `logout` et `quit`	Toutes les commandes effectuent la même action. Elles permettent de terminer la session en cours et de revenir à une interface de ligne de commande de connexion.

Utilisation d'une console Telnet avec CMC

Vous pouvez ouvrir simultanément jusqu'à quatre sessions Telnet avec CMC.

Si la station de gestion exécute Microsoft Windows XP ou Microsoft Windows Server 2003, vous pouvez rencontrer un problème de caractères au cours d'une session Telnet CMC. Cela peut donner lieu au gel de la connexion, quand la touche Retour ne répond pas et que le message de saisie du mot de passe ne s'affiche pas.

Pour résoudre ce problème, téléchargez le hot fix 824810 depuis l'adresse **support.microsoft.com**. Pour plus d'informations, vous pouvez également consulter l'article 824810 dans la base de connaissances de Microsoft.

Depuis l'interface de ligne de commande, vous pouvez gérer les expirations de session à l'aide de la commande racadm, `racadm getconfig -g cfgSessionManagement`. Pour plus d'informations, voir le *Guide de référence de la ligne de commande PowerEdge VRTX de Dell Version Chassis Management Controller*.

Utilisation de SSH avec CMC

SSH est une session de ligne de commande qui offre les mêmes fonctionnalités qu'une session Telnet, mais avec des fonctions de négociation de session et de chiffrement qui renforcent la sécurité. Le contrôleur CMC prend en charge SSH version 2 avec authentification par mot de passe. Par défaut, SSH est activé sur le contrôleur CMC.

REMARQUE : CMC ne prend pas en charge la version 1 de SSH.

En cas d'erreur pendant la connexion à CMC, le client SSH affiche un message d'erreur. Le texte du message dépend du client et n'est pas contrôlé par le CMC. Consultez les messages RACLog pour déterminer la cause de la panne.

REMARQUE : `OpenSSH` doit être exécuté à partir d'un émulateur de terminal VT100 ou ANSI sous Windows. Vous pouvez également exécuter `OpenSSH` en utilisant `Putty.exe`. L'exécution d'`OpenSSH` sous l'invite de commande Windows n'offre pas une fonctionnalité complète, c'est-à-dire que certaines touches ne répondent pas et aucun graphique n'est affiché. Sous Linux, exécutez les services clients SSH pour vous connecter au contrôleur CMC avec n'importe quel shell.

Le système prend en charge quatre sessions SSH simultanées. Le délai d'expiration de la session est contrôlé par la propriété `cfgSsnMgtSshIdleTimeout`. Vous pouvez vérifier les diverses expirations de session à l'aide de la commande racadm `getconfig -g cfgSessionManagement`.

```
$ racadm getconfig -g cfgSessionManagement
cfgSsnMgtWebserverTimeout=1800
cfgSsnMgtTelnetIdleTimeout=1800
cfgSsnMgtSshIdleTimeout=1800
cfgSsnMgtRacadmTimeout=60
```

Pour plus d'informations sur les commandes RACADM, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX* sur le site dell.com/support/Manuals.

CMC prend également en charge l'authentification par clé publique (PKA) sur SSH. Cette méthode d'authentification améliore l'automatisation de la rédaction des scripts SSH en évitant d'intégrer ou de demander l'ID utilisateur/le mot de passe. Pour plus d'informations, consultez Configuration de l'authentification par clé publique sur SSH.

SSH est activé par défaut. Si SSH est désactivé, vous pouvez l'activer avec n'importe quelle autre interface prise en charge.

Pour configurer SSH, voir « Configuration des services ».

Schémas cryptographiques SSH pris en charge

Pour communiquer avec CMC en utilisant le protocole SSH, le système prend en charge les schémas cryptographiques répertoriés dans le tableau suivant.

Tableau 32. Schémas de cryptographie

Type de schéma	Couleurs
Cryptographie asymétrique	Spécification de bits (aléatoire) Diffie-Hellman DSA/DSS 512-1024 par NIST
Cryptographie symétrique	• AES256-CBC • RIJNDAEL256-CBC • AES192-CBC • RIJNDAEL192-CBC • AES128-CBC • RIJNDAEL128-CBC

Tableau 32. Schémas de cryptographie (suite)

Type de schéma	Couleurs
	• BLOWFISH-128-CBC • 3DES-192-CBC • ARCFOUR-128
Intégrité du message	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
Authentification	Mot de passe

Configuration de l'authentification par clé publique sur SSH

Vous pouvez configurer jusqu'à six clés publiques qui peuvent être utilisées avec le nom d'utilisateur du service via une interface SSH. Avant d'ajouter ou de supprimer des clés publiques, veillez à utiliser la commande `view` pour identifier les clés qui sont déjà configurées, afin d'éviter qu'une clé ne soit remplacée ou supprimée par inadvertance. Le nom d'utilisateur du service est un compte d'utilisateur spécial qui peut être utilisé lors de l'accès au CMC via SSH. Lorsque l'authentification par clé publique sur SSH est correctement configurée et utilisée, vous n'avez pas besoin de saisir le nom d'utilisateur ou les mots de passe pour vous connecter au CMC. Cela peut être très utile pour configurer des scripts automatisés afin d'exécuter diverses fonctions.

REMARQUE : L'interface utilisateur n'est pas prise en charge pour la gestion de cette fonction ; vous ne pouvez utiliser que RACADM.

Lors de l'ajout de nouvelles clés publiques, assurez-vous que les clés existantes ne se trouvent pas déjà sur l'index, où est ajoutée la nouvelle clé. Le contrôleur CMC n'effectue aucune vérification pour s'assurer que les anciennes clés sont supprimées avant d'en ajouter une nouvelle. Dès que vous ajoutez une nouvelle clé, elle prend automatiquement effet à condition que l'interface SSH soit activée.

Dans la clé publique, lorsque vous utilisez la section commentaire de la clé publique, n'oubliez pas que le CMC n'utilise que les 16 premiers caractères. Le commentaire de la clé publique est utilisé par le CMC pour distinguer les utilisateurs SSH lors de l'utilisation de la commande RACADM `getssninfo`, car tous les utilisateurs de l'authentification par clé publique utilisent le nom d'utilisateur du service pour se connecter.

Par exemple, si deux clés publiques sont configurées, l'une avec le commentaire PC1 et l'autre avec le commentaire PC2 :

```
racadm getssninfo
Type       User   IP Address   Login
Date/Time
SSH        PC1    x.x.x.x      06/16/2009
09:00:00
SSH        PC2    x.x.x.x      06/16/2009
09:00:00
```

Pour plus d'informations sur la commande `sshpkauth`, reportez-vous au *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX*.

Génération de clés publiques pour des systèmes exécutant Windows

Avant d'ajouter un compte, vous devez obtenir une clé publique à partir du système qui accède au CMC sur SSH. Deux méthodes permettent de générer la paire de clés publique/privée : l'utilisation de l'application PuTTY Key Generator pour les clients sous Windows ou ssh-keygen CLI pour les clients sous Linux.

Cette section propose des instructions simples permettant de générer une paire de clés publique/privée pour les deux applications. Pour une utilisation supplémentaire ou avancée de ces outils, consultez l'assistance de l'application.

Pour utiliser le générateur de clé PuTTY pour créer une clé de base pour les clients qui exécutent Windows :

1. Démarrez l'application et sélectionnez SSH-2 RSA ou SSH-2 DSA comme type de clé à générer (SSH-1 n'est pas pris en charge).
2. Saisissez le nombre de bits de la clé. Assurez-vous que la longueur de la clé RSA est comprise entre 1 024 et 4 096.

REMARQUE :

- **Il est recommandé d'utiliser une longueur de clé DSA de 1024.**
- **Le contrôleur CMC peut ne pas afficher de message si vous ajoutez des clés de moins de 1 024 bits ou de plus de 4 096 bits, mais lorsque vous essayez de vous connecter avec ces clés, la connexion échoue.**
- **Pour des clés DSA supérieures à 2 048, utilisez la commande RACADM suivante. Le CMC accepte les clés RSA avec une puissance allant jusqu'à 4096, mais la puissance recommandée est de 1024.**

```
racadm -r 192.168.8.14 -u root -p calvin sshpkauth -i svcacct -k 1 -p 0xfff -f
dsa_2048.pub
```

3. Cliquez sur **Générer**, puis déplacez la souris dans la fenêtre en suivant les instructions.

   Une fois la clé créée, vous pouvez modifier le champ Commentaire de la clé.

   Vous pouvez également saisir une phrase de passe pour sécuriser la clé. Veillez à bien enregistrer la clé privée.

4. Vous pouvez utiliser la clé publique de deux façons :
   - Enregistrer la clé publique dans un fichier à téléverser ultérieurement.
   - Copier/coller le texte de la fenêtre **Clé publique à coller** lors de l'ajout du compte à l'aide de l'option de texte.

Génération de clés publiques pour les systèmes Linux

L'application ssh-keygen pour clients Linux est un outil de ligne de commande sans interface utilisateur graphique. Ouvrez une fenêtre de terminal et entrez la commande suivante à l'invite shell :

```
ssh-keygen -t rsa -b 1024 -C testing
```

où

L'option `-t` doit être dsa ou rsa.

`-b` spécifie la taille du cryptage binaire entre 768 et 4 096.

`-c` permet de modifier le commentaire de la clé publique ; l'option est facultative.

La valeur <*passphrase*> est facultative. Une fois la commande exécutée, utilisez le fichier public pour le transmettre à RACADM afin de le téléverser.

Remarques concernant la syntaxe RACADM pour le contrôleur CMC

Lorsque vous utilisez la commande `racadm sshpkauth`, vérifiez les points suivants :

- Pour l'option `-i`, le paramètre doit être `svcacct`. Tous les autres paramètres entrés pour `-i` échouent dans le contrôleur CMC. `svcacct` désigne un compte spécial destiné à l'authentification par clé publique sur SSH dans le contrôleur CMC.
- Pour se connecter au CMC, l'utilisateur doit être un service. Les utilisateurs d'autres catégories peuvent accéder aux clés publiques entrées avec la commande `sshpkauth`.

Affichage des clés publiques

Pour afficher les clés publiques que vous avez ajoutées au CMC, entrez :

```
racadm sshpkauth -i svcacct -k all -v
```

Pour afficher une clé à la fois, remplacez l'argument `all` par un nombre compris entre 1 et 6. Par exemple, pour afficher la clé 2, entrez :

```
racadm sshpkauth -i svcacct -k 2 -v
```

Ajout de clés publiques

Pour ajouter une clé publique au contrôleur CMC en utilisant l'option `-f` de téléversement de fichier, entrez la commande suivante depuis la console d'interface de ligne de commande :

```
racadm sshpkauth -i svcacct -k 1 -p 0xfff -f <fichier de clé publique>
```

REMARQUE : Vous pouvez utiliser l'option de téléversement de fichier avec RACADM distant. Pour plus d'informations, voir le document *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX).

Pour ajouter une clé publique à l'aide de l'option de téléversement de texte, entrez :

```
racadm sshpkauth -i svcacct -k 1 -p 0xfff -t "<texte de clé publique>"
```

Suppression de clés publiques

Pour supprimer une clé publique, exécutez la commande suivante :

```
racadm sshpkauth -i svcacct -k 1 -d
```

Pour supprimer toutes les clés publiques, exécutez la commande suivante :

```
racadm sshpkauth -i svcacct -k all -d
```

Configuration du logiciel d'émulation de terminal

Le contrôleur CMC prend en charge une console texte série depuis une station de gestion exécutant l'un des types de logiciels d'émulation de terminal suivants :

- Linux Minicom
- HyperTerminal Private Edition (version 6.3) de Hilgraeve

Effectuez les tâches des sous-sections suivantes pour configurer le type de logiciel de terminal requis.

Configuration de Linux Minicom

Minicom est un utilitaire d'accès à un port série pour Linux. Les étapes suivantes s'appliquent à la configuration de Minicom 2.0. Les autres versions de Minicom peuvent être légèrement différentes, mais nécessitent les mêmes paramètres de base. Pour configurer d'autres versions de Minicom, voir les informations qui figurent dans la section des paramètres Minicom requis de ce Guide d'utilisation.

Configuration de Minicom version 2.0

REMARQUE : Pour des résultats optimaux, configurez la propriété cfgSerialConsoleColumns afin qu'elle corresponde au nombre de colonnes. Attention, l'invite consomme deux caractères. Par exemple, pour une fenêtre de terminal à 80 colonnes :

```
racadm config -g cfgSerial -o cfgSerialConsoleColumns 80.
```

1. Si vous ne possédez pas de fichier de configuration Minicom, passez à l'étape suivante. Si vous disposez d'un tel fichier, entrez `minicom<Minicom config file name>`, puis passez à l'étape 12.
2. À l'invite de commande Linux, tapez `minicom -s`.
3. Sélectionnez **Configuration du port série** et appuyez sur <Entrée>.
4. Appuyez sur <a> et sélectionnez le périphérique série approprié (par exemple, `/dev/ttyS0`).
5. Appuyez sur <e> et définissez l'option **Bits par seconde/Parité/Bits** sur **115200 8N1**.
6. Appuyez sur <f>, puis définissez **Contrôle de flux matériel** sur **Oui** et **Contrôle de flux logiciel** sur **Non**. Pour quitter le menu **Configuration des ports série**, appuyez sur <Entrée>.
7. Sélectionnez **Modem et numérotation** et appuyez sur <Entrée>.
8. Dans le menu **Configuration du modem et de la numérotation**, appuyez sur <Ret. Arr.> pour effacer les paramètres **init**, **reset**, **connect** et **hangup** afin de les laisser vides. Appuyez ensuite sur <Entrée> pour enregistrer chaque valeur vide.
9. Lorsque tous les champs indiqués ont été effacés, appuyez sur <Entrée> pour quitter le menu **Configuration de la numérotation du modem et des paramètres**.
10. Sélectionnez **Quitter Minicom** et appuyez sur <Entrée>.
11. À l'invite du shell de commandes, entrez `minicom <Minicom config file name>`.
12. Pour quitter Minicom, appuyez sur <Ctrl><a>, <x>, <Entrée>.

Vérifiez que la fenêtre Minicom affiche une invite de connexion. Si cette invite apparaît, la connexion a été établie. Vous êtes prêt à vous connecter et à accéder à l'interface de ligne de commande (CLI) CMC.

Paramètres Minicom requis

Consultez le tableau suivant pour configurer Minicom, quelle que soit la version.

Tableau 33. Paramètres Minicom

Description du paramètre	Paramètre requis
B/s/Par/Bits	115200 8N1
Contrôle du débit matériel	Oui
Contrôle du débit logiciel	Non
Émulation de terminal	ANSI
Paramètres de la numérotation du modem et des paramètres	Effacez les paramètres **init**, **reset**, **connect** et **hangup** pour qu'ils soient vides.

Connexion aux serveurs ou au module d'entrée/sortie à l'aide de la commande connect

Le contrôleur CMC peut établir une connexion pour rediriger la console série d'un serveur ou du modules d'E/S.

Pour les serveurs, vous pouvez effectuer la redirection de console série à l'aide des outils suivants :

- Interface de ligne de commande (CLI) du CMC ou commande RACADM `connect`. Pour plus d'informations sur l'exécution des commandes RACADM, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX*.
- Fonction de redirection de la console série de l'interface Web iDRAC.
- Fonction SOL (Serial Over LAN, série sur LAN) de l'iDRAC.

Dans une console série, Telnet ou SSH, le contrôleur CMC prend en charge la commande `connect` pour établir une connexion série à un serveur ou à un module d'E/S. La console série du serveur contient à la fois les écrans de démarrage et de configuration du BIOS, et la console série du système d'exploitation. Pour le module d'E/S, la console série du commutateur est disponible. Il n'y a qu'un seul module d'E/S sur le châssis.

PRÉCAUTION : Lors d'une exécution à partir de la console série du CMC, l'option `connect -b` reste connectée jusqu'à la réinitialisation du CMC. Cette connexion représente un risque de sécurité potentiel.

REMARQUE : La commande `connect` fournit l'option –b (binaire). L'option –b transmet des données binaires brutes, et `cfgSerialConsoleQuitKey` n'est pas utilisé. En outre, lorsque vous vous connectez à un serveur à l'aide de la console série du CMC, les transitions du signal DTR (par exemple, si le câble série est retiré pour connecter un débogueur) n'entraînent pas une fermeture de l'application.

REMARQUE : Si le module d'E/S ne prend pas en charge la redirection de la console, la commande `connect` affiche une console vide. Dans ce cas, pour revenir à la console CMC, saisissez la séquence d'échappement. La séquence d'échappement par défaut de la console est <Ctrl><\>.

Pour vous connecter à un module d'E/S, tapez :

```
connect switch-n
```

où `n` est une étiquette IOM A1.

Lorsque vous référencez l'IOM dans la commande connect, l'IOM est associé à un commutateur, comme indiqué dans le tableau suivant.

Tableau 34. Association de module d'E/S à des commutateurs

Étiquette de module d'E/S	Switch (Commutateur)
A1	commutateur-a1 ou commutateur-1

REMARQUE : À un moment donné, il peut exister une seule connexion IOM par châssis.

REMARQUE : Vous ne pouvez pas vous connecter aux fonctions d'intercommunication depuis la console série.

Pour vous connecter à une console série de serveurs gérés, exécutez la commande `connect server-n`, où `n` est compris entre 1 et 4. Vous pouvez également utiliser la commande `racadm connect server-n`. Lorsque vous vous connectez à un serveur à l'aide de l'option `-b`, la communication binaire est utilisée et le caractère d'échappement est désactivé. Si l'iDRAC n'est pas disponible, le message d'erreur `No route to host` s'affiche.

La commande `connect server-n` permet à l'utilisateur d'accéder au port série du serveur. Une fois la connexion établie, l'utilisateur peut voir la redirection de console du serveur via le port série du CMC, y compris la console série du BIOS et la console série du système d'exploitation.

REMARQUE : Pour afficher les écrans de démarrage du BIOS, la redirection série doit être activée dans la configuration du BIOS des serveurs. En outre, vous devez définir une valeur de 80 × 25 pour la fenêtre de l'émulateur de terminal. Dans le cas contraire, les caractères de la page ne s'afficheront pas correctement.

REMARQUE : Toutes les touches ne fonctionnent pas sur les pages de configuration du BIOS. Vous devez donc définir des raccourcis clavier appropriés pour les combinaisons utilisant les touches <Ctrl>, <Alt>, <Suppr>, etc. L'écran de redirection initial affiche les raccourcis clavier nécessaires.

Configuration du BIOS du serveur géré pour la redirection de console série

Vous pouvez utiliser une session de console distante pour vous connecter au système géré en utilisant l'interface Web iDRAC (voir le document *Guide d'utilisation d'iDRAC* sur le site **dell.com/support/manuals**).

La communication série dans le BIOS est désactivée par défaut. Pour rediriger les données de console texte de l'hôte vers SOL (Serial over LAN), vous devez activer la redirection de console via COM1. Pour modifier le paramètre BIOS :

1. Mettez le serveur géré sous tension.
2. Appuyez sur la touche <F2> pour accéder à l'utilitaire de configuration du BIOS pendant le test POST.
3. Accédez à **Communication série** et appuyez sur <Entrée>. Dans la boîte de dialogue, la liste des communications série affiche les options suivantes :
   - **désactivé**
   - **activé sans redirection de console**
   - **activé avec redirection de console via COM1**

   Pour naviguer entre ces options, appuyez sur les touches fléchées.

   REMARQUE : Vérifiez que l'option Activer avec la redirection de console via COM1 est sélectionnée.
4. Activez l'option **Redirection après démarrage** (la valeur par défaut est **Désactivé**). Cette option permet la redirection de console BIOS pour les redémarrages suivants.
5. Cette option permet d'enregistrer les modifications et de quitter.

   Le système géré redémarre.

Configuration de Windows pour la redirection de console série

Aucune configuration n'est nécessaire pour les serveurs qui exécutent Microsoft Windows Server 2003 ou supérieur. Windows reçoit les informations du BIOS et active la console SAC (Special Administration Console - Console d'administration spéciale) sur COM1.

Configuration de Linux pour la redirection de console série du serveur pendant le démarrage

Les étapes suivantes sont propres à GRUB (Linux GRand Unified Bootloader - Grand chargeur d'amorçage unifié Linux). Des modifications similaires sont nécessaires si vous utilisez un chargeur d'amorçage différent.

REMARQUE : Lorsque vous configurez la fenêtre d'émulation VT100, configurez la fenêtre ou l'application qui affiche la console redirigée en définissant 25 lignes × 80 colonnes pour afficher correctement le texte. Autrement, certains écrans texte peuvent être déformés.

Modifiez le fichier `/etc/grub.conf` comme suit :

1. Recherchez les sections relatives aux paramètres généraux dans le fichier et ajoutez les deux lignes suivantes :

```
serial --unit=1 --speed=57600 terminal --timeout=10 serial
```

2. Ajoutez deux options à la ligne du noyau :

```
noyau de la console=ttyS1,57600
```

3. Si le fichier `/etc/grub.conf` contient une instruction `splashimage`, mettez-la en commentaire pour l'exclure.

   L'exemple suivant illustre les modifications décrites dans cette procédure.

```
# grub.conf generated by anaconda # # Notez qu'il est inutile d'exécuter de nouveau grub
après modification # de ce fichier. # REMARQUE : vous n'avez pas de partition /boot. Ceci
signifie que tous # les chemins kernel et initrd sont relatifs par rapport à /, ex. : #
root (hd0,0) # kernel /boot/vmlinuz-version ro root= /dev/sda1 # initrd /boot/initrd-
version.img # #boot=/dev/sda default=0 timeout=10 #splashimage=(hd0,2)/grub/splash.xpm.gz
serial --unit=1 --speed=57600 terminal --timeout=10 serial title Red Hat Linux Advanced Server (2.4.9-
e.3smp) root (hd0,0) kernel /boot/vmlinuz-2.4.9-e.3smp ro root= /dev/sda1 hda=ide-scsi
console=ttyS0 console=ttyS1,57600 initrd /boot/initrd-2.4.9-e.3smp.img title Red Hat Linux
Advanced Server-up (2.4.9-e.3) root (hd0,00) kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/
sda1 initrd /boot/initrd-2.4.9-e.3.img
```

   Lors de la modification du fichier `/etc/grub.conf`, appliquez les consignes suivantes :

   - Désactivez l'interface graphique GRUB et utilisez l'interface texte. Sinon, l'écran GRUB ne s'affiche pas pour la redirection de console. Pour désactiver l'interface graphique, mettez en commentaire la ligne qui commence par `splashimage`.
   - Pour activer plusieurs options GRUB afin de démarrer les sessions de console via la connexion série, ajoutez la ligne suivante à toutes les options :

     ```
     console=ttyS1,57600
     ```

     Dans l'exemple, `console=ttyS1,57600` est ajouté à la première option uniquement.

Configuration de Linux pour la redirection de console série du serveur après l'amorçage

Modifiez le fichier `/etc/inittab` de la manière suivante :

Ajoutez une nouvelle ligne pour configurer `agetty` sur le port série COM2 :

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
```

L'exemple suivant montre le fichier avec la nouvelle ligne.

```
# # inittab Ce fichier explique comment le processus INIT # doit configurer le système pour
un certain # niveau d'exécution. # # Auteur : Miquel van Smoorenburg # Modifié pour RHS Linux
par Marc Ewing et # Donnie Barnes # # Niveau d'exécution par défaut. Les niveaux d'exécution
utilisés par RHS sont : # 0 - halt (Ne PAS définir initdefault sur ce niveau) # 1 - Mode
utilisateur unique # 2 - Multi-utilisateur, sans NFS (Identique à 3, si vous # n'avez pas de
mise en réseau) # 3 - Mode multi-utilisateur complet # 4 - Non utilisé # 5 - X11 # 6 -
Redémarrage (Ne PAS définir initdefault sur ce niveau) # id:3:initdefault: # Initialisation
```

```
du système. si::sysinit:/etc/rc.d/rc.sysinit l0:0:wait:/etc/rc.d/rc 0 l1:1:wait:/etc/rc.d/rc
1 l2:2:wait:/etc/rc.d/rc 2 l3:3:wait:/etc/rc.d/rc 3 l4:4:wait:/etc/rc.d/rc 4 l5:5:wait:/etc/
rc.d/rc 5 l6:6:wait:/etc/rc.d/rc 6 # Éléments à exécuter à chaque niveau d'exécution.
ud::once:/sbin/update # Interruption CTRL-ALT-SUPPR ca::ctrlaltdel:/sbin/shutdown -t3 -r now
# Lorsque l'onduleur indique une panne de courant, nous supposons qu'il reste # quelques
minutes d'alimentation. Planifiez un arrêt dans 2 minutes à partir de maintenant. # Bien
entendu, on considère ici que l'alimentation est installée, # et que l'onduleur est connecté
et fonctionne correctement. pf::powerfail:/sbin/shutdown -f -h +2 "Panne de courant ; arrêt
du système" # Si vous avez rétabli l'alimentation avant l'arrêt, annulez cet arrêt.
pr:12345:powerokwait:/sbin/shutdown -c "Alimentation restaurée ; arrêt annulé" # Exécutez
gettys avec les niveaux d'exécution standard co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1 2:2345:respawn:/sbin/mingetty tty2 3:2345:respawn:/sbin/
mingetty tty3 4:2345:respawn:/sbin/mingetty tty4 5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6 # Exécutez xdm pour le niveau d'exécution 5 # xdm est
désormais un service séparé x:5:respawn:/etc/X11/prefdm -nodaemon
```

Modifiez le fichier `/etc/securetty` de la manière suivante :

Ajoutez une nouvelle ligne avec le nom du tty série de COM2 :

```
ttyS1
```

L'exemple suivant montre un fichier avec la nouvelle ligne.

```
vc/1 vc/2 vc/3 vc/4 vc/5 vc/6 vc/7 vc/8 vc/9 vc/10 vc/11 tty1 tty2 tty3 tty4 tty5 tty6 tty7
tty8 tty9 tty10 tty11 ttyS1
```

12

Utilisation de FlexAddress et FlexAdress Plus

Cette section fournit des informations sur FlexAddress, FlexAddress Plus et leur configuration.

REMARQUE : Une licence Entreprise doit être installée sur le CMC pour l'utilisation de la fonctionnalité FlexAddress.

Sujets :

À propos de FlexAddress

Si un serveur est remplacé, la FlexAddress du logement reste la même pour le logement de serveur. Si le serveur est inséré dans un nouveau logement ou châssis, l'adresse WWN/MAC attribuée par le serveur est utilisée à moins que la fonction FlexAddress du châssis soit activée pour le nouveau logement. Si vous retirez le serveur, il réutilise l'adresse attribuée par le serveur. Vous ne devez pas reconfigurer les canevas de déploiement, les serveurs DHCP et les routeurs des différentes matrices pour identifier le nouveau serveur.

Chaque module serveur reçoit des adresses WWN et/ou MAC uniques au cours de la fabrication. Sans FlexAddress, si vous devez remplacer un serveur par un autre module serveur, les adresses WWN/MAC changent, et vous devez reconfigurer les outils de gestion de réseau Ethernet et les ressources SAN afin d'identifier le nouveau module serveur.

La fonction FlexAddress permet à CMC d'attribuer des adresses WWN/MAC à un logement et de remplacer les adresses définies en usine. Ainsi, si le module serveur est remplacé, les adresses WWN/MAC basées sur le logement restent identiques. Avec cette fonction, vous n'avez plus à reconfigurer les outils de gestion de réseau Ethernet ni les ressources SAN d'un nouveau module serveur.

En outre, ce *remplacement* se produit uniquement lorsque vous insérez un module serveur dans un châssis où la fonction FlexAddress est activée. Aucune modification permanente n'est apportée au module serveur. Si un module serveur est transféré vers un châssis qui ne prend pas en charge la fonction FlexAddress, les adresses WWN/MAC affectées en usine sont utilisées.

Le châssis CMC VRTX est fourni avec la carte SD qui prend en charge les fonctions FlexAddress, FlexAddress Plus et de stockage étendu. Si le châssis VRTX est fourni avec un deuxième contrôleur CMC en option, ce dernier dispose d'une carte SD qui prend en charge le stockage étendu.

REMARQUE :

- **Les données sur la carte SD sont cryptées et ne peuvent pas être dupliquées ou modifiées en aucune manière afin de garantir que le système et ses fonctions restent opérationnels.**
- **L'utilisation d'une carte SD est limitée à un seul châssis. Vous ne pouvez pas utiliser la même carte SD sur un autre châssis.**

La carte de fonction FlexAddress contient une plage d'adresses MAC. Avant d'installer FlexAddress, vous pouvez déterminer la plage d'adresses MAC figurant sur la carte de fonction FlexAddress en insérant la carte SD dans un lecteur de cartes mémoire USB et en affichant le fichier `pwwn_mac.xml`. Ce fichier XML en texte clair stocké sur la carte SD contient la balise XML *mac_start*, qui indique la première adresse MAC hexadécimale utilisée pour cette plage d'adresses MAC uniques. La balise *mac_count* indique le nombre total d'adresses MAC allouées par la carte SD. La plage totale d'adresses MAC allouées peut être déterminée par :

```
<mac_start> + <mac_count>  - 1 = <mac_end>
```

Par exemple :

```
(starting_mac)00188BFFDCFA + (mac_count)0xCF - 1 = (ending_mac)00188BFFDDC8
```

.

REMARQUE : Verrouillez la carte SD avant de l'insérer dans le lecteur de cartes mémoire USB pour empêcher toute modification involontaire du contenu. Vous devez déverrouiller la carte SD avant de l'insérer dans le contrôleur CMC.

À propos de FlexAddress Plus

FlexAddress Plus est une nouvelle fonction, nouveauté de la carte de fonction version 2.0. Il s'agit d'une mise à niveau de la carte de fonction FlexAddress version 1.0. FlexAddress Plus contient davantage d'adresses MAC que FlexAddress. Les deux fonctions permettent au châssis d'attribuer des adresses WWN/MAC (World Wide Name/Media Access Control - Nom universel/contrôle de l'accès aux supports) aux périphériques Fibre Channel et Ethernet. Les adresses WWN/MAC attribuées par le châssis sont uniques au niveau global et propres à un logement de serveur.

Affichage de l'état d'activation de FlexAddress

Une carte de fonction est équipée d'une ou de plusieurs des fonctionnalités suivantes : FlexAddress, FlexAddress Plus, et/ou Stockage étendu.

Pour afficher l'état FlexAddress du châssis en utilisant l'interface Web CMC, cliquez sur **Présentation du châssis** > **Configurer**.

La page **Paramètres généraux du châssis** s'affiche.

L'option **FlexAddress** est définie soit sur **Actif** soit sur **Inactif**. La valeur **Actif** indique que la fonction est installée sur le châssis et la valeur **Inactif** indique que la fonction n'est ni installée, ni en cours d'utilisation sur le châssis.

Exécutez la commande RACADM suivante pour vérifier l'état de la carte de fonction SD :

```
racadm featurecard -s
```

Le message suivant s'affiche :

```
Active CMC:
The feature card inserted is valid, serial number CN0H871T1374036T00MXA00
The feature card contains the following feature(s)
       FlexAddress: bound
       FlexAddressPlus: bound
       ExtendedStorage: bound
Standby CMC:
The feature card contains the following feature(s)
       ExtendedStorage: bound
```

REMARQUE : La console CMC secondaire est facultative, et la sortie de la console CMC de secours s'affiche uniquement si cette dernière est disponible dans le châssis.

Tableau 35. Messages d'état renvoyés par la commande featurecard -s

Message de condition	Actions
`No feature card inserted.`	Vérifiez que la carte SD est correctement insérée dans le contrôleur CMC. Dans une configuration avec CMC redondants, vérifiez que la carte de fonction SD a été insérée dans le CMC actif et non dans le CMC de secours.
`The feature card inserted is valid and contains the following feature(s) FlexAddress: bound.`	Aucune action n'est requise.
`The feature card inserted is valid and contains the following feature(s) FlexAddress: bound to another chassis, svctag=ABC1234, SD card SN = 1122334455.`	Retirez la carte SD, localisez et installez la carte SD du châssis actuel.
`The feature card inserted is valid and contains the following feature(s) FlexAddress: not bound.`	La carte de fonction peut être déplacée vers un autre châssis ou réactivée sur le châssis actuel. Pour effectuer une

Tableau 35. Messages d'état renvoyés par la commande featurecard -s (suite)

Message de condition	Actions
	réactivation sur le châssis actuel, saisissez la commande `racadm racreset` jusqu'à ce que le module CMC sur lequel est installée la carte de fonction devienne actif.

Utilisez la commande RACADM suivante pour afficher toutes les fonctionnalités activées sur le châssis :

```
racadm feature -s
```

La commande renvoie le message de condition suivant :

```
Feature Name = FlexAddress
       Date/time Activated = 05 Oct 2013 - 11:50:49
       Feature installed from SD-card serial number = CN0H871T1374036T00MXA00

       Feature Name = FlexAddressPlus
       Date/time Activated = 05 Oct 2013 - 11:50:49
       Feature installed from SD-card serial number = CN0H871T1374036T00MXA00

       Feature Name = ExtendedStorage
       Current Status = redundant, active
       Date/time Activated = 05 Oct 2013 - 11:50:58
       Feature installed from SD-card serial number = CN0H871T1374036T00MXA00
```

Si aucune fonction n'est active sur le châssis, la commande renvoie le message suivant :

```
racadm feature -s
No features active on the chassis
```

Les cartes de fonctions Dell (Dell Feature Card) peuvent contenir plusieurs fonctions. Une fois qu'une fonction incluse sur une carte de fonction Dell a été activée sur un châssis, les autres fonctions éventuellement contenues dans cette carte de fonction Dell ne peuvent pas être activées sur un autre châssis. Dans ce cas, la commande `racadm feature -s` affiche le message suivant pour les fonctions affectées :

```
ERROR: One or more features on the SD card are active on another chassis
```

Pour plus d'informations sur les commandes `feature` et `featurecard`, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX* sur le site de support.

Configuration de FlexAddress

FlexAddress est une mise à niveau facultative qui permet aux modules serveurs de remplacer l'adresse WWN/MAC définie en usine par une adresse WWN/MAC fournie par le châssis.

REMARQUE : Dans cette section, le terme FlexAddress désigne également la version FlexAddress Plus.

REMARQUE : Vous pouvez réinitialiser l'adresse Flex d'une CMC à sa configuration d'usine par défaut à l'aide de la sous-commande `racresetcfg`. Il s'agit de la configuration « désactivé ». La syntaxe RACADM est :

```
racadm racresetcfg -c flex
```

Pour en savoir plus sur les commandes RACADM liées à FlexAddress et les données concernant les autres propriétés définies en usine voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge* disponible à l'adresse dell.com/cmcmanuals.

Vous devez mettre le serveur hors tension avant de commencer la configuration. Vous pouvez activer ou désactiver FlexAddress pour chaque structure. Vous pouvez également activer ou désactiver la fonction pour chaque logement. Une fois que vous avez activé la fonction pour une structure, vous pouvez sélectionner les logements à activer. Par exemple, si la structure A est activée, FlexAddress est activé uniquement sur la structure A pour tous les logements activés. Toutes les autres structures utilisent l'adresse WWN/MAC définie en usine sur le serveur.

REMARQUE : FlexAddress ne prend effet sur un module de serveur qu'au prochain redémarrage. Lorsque la fonction FlexAddress est déployée pour la première fois sur un module de serveur donné, vous devez mettre le serveur hors tension puis le remettre sous tension pour pouvoir activer FlexAddress. Sur les périphériques Ethernet, la fonction FlexAddress est programmée par le BIOS du module serveur. Pour que le BIOS du module serveur puisse programmer l'adresse, celui-ci doit être opérationnel, ce qui signifie que le module serveur doit être mis sous tension. À la fin de la séquence de mise hors et sous tension, les adresses MAC attribuées par le châssis sont disponibles pour la fonction Wake-on-LAN (WOL).

Configuration de FlexAddress pour les structures et logements au niveau du châssis

Au niveau du châssis, vous pouvez activer ou désactiver la fonction FlexAddress pour les structures et logements. FlexAddress est activé en fonction de chaque structure, puis vous sélectionnez les logements à inclure dans la fonction. Vous devez activer à la fois des structures et des logements pour configurer correctement FlexAddress.

Configuration de FlexAddress pour les structures et logements au niveau du châssis avec l'interface Web CMC

Si un serveur est présent dans le logement, éteignez-le avant d'activer la fonction FlexAddress dans ce logement.

Pour activer ou désactiver une structure et des logements pour utiliser la fonction FlexAddress à l'aide de l'interface Web CMC :

1. Dans le volet de gauche, cliquez sur **Présentation du serveur** > **Configurer** > **FlexAddress.**.
2. Dans la page **Déployer FlexAddress**, dans la section **Sélectionner les structures du WWN/des adresses MAC affectées par le châssis**, sélectionnez le type de structure (**Structurre A** ou **iDRAC**) pour lequel vous voulez activer FlexAddress. Pour désactiver la fonction, désélectionnez l'option.
3. Sur la page **Sélectionner les structures du WWN/des adresses MAC affectées par le châssis**, sélectionnez l'option **Activé** pour le logement pour lequel vous voulez activer FlexAddress. Pour désactiver la fonction, désélectionnez l'option.

   REMARQUE : Notez les points suivants :

   - **Si vous ne sélectionnez aucun logement, FlexAddress n'est pas activé pour la structure sélectionnée.**
   - **Lorsque aucune des structures n'est sélectionnée et qu'un logement de serveur est sélectionné et appliqué, le message suivant s'affiche `No fabrics selected! FlexAddress will not be used on this chassis.` Sélectionnez à la fois le logement et la structure pour configurer FlexAddress.**
   - **La configuration de Flexaddress pour logement esclave n'est pas permise. L'option est grisée dans l'interface Web CMC. Les périphériques Ethernet associés au logement esclave du serveur héritent de la configuration des emplacements maîtres.**
4. Pour enregistrer les paramètres, cliquez sur **Appliquer**.

Configuration de FlexAddress pour les structures et logements au niveau du châssis avec RACADM

Pour activer et désactiver des structures, utilisez la commande RACADM suivante :

```
racadm setflexaddr [-f <fabricName> <state>]
```

où `<fabricName> = A or iDRAC` et `<state> = 0 or 1`

(0 = désactivé et 1 = activé).

Pour activer et désactiver des logements, utilisez la commande RACADM suivante :

```
racadm setflexaddr [-i <slot#> <state>
```

où `<slot#> = 1 or 4` et `<state> = 0 or 1`

(0 = désactivé et 1 = activé).

Pour plus d'informations sur la commande **setflexaddr**, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX*.

REMARQUE : Si vous achetez la fonction FlexAddress ou FlexAddressPlus avec votre Dell PowerEdge VRTX, la fonction est pré-installée et activée pour tous les logements et structures. Pour acheter cette fonction, contactez Dell à dell.com.

REMARQUE : Vous pouvez réinitialiser l'adresse Flex d'une CMC à sa configuration d'usine par défaut à l'aide de la sous-commande `racresetcfg`. Il s'agit de la configuration « désactivé ». La syntaxe RACADM est :

```
racadm racresetcfg -c flex
```

Pour en savoir plus sur les commandes RACADM liées à FlexAddress et les données concernant les autres propriétés définies en usine, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge* disponible à l'adresse dell.com/cmcmanuals.

Affichage des adresses WWN (World Wide Name) ou MAC (Media Access Control)

La page **Résumé WWN/MAC** affiche la configuration WWN (World Wide Name) et l'adresse MAC (Media Access Control) d'un logement présent dans le châssis.

Configuration de la structure

La section **Configuration de la structure** affiche le type de structure d'entrée/de sortie de la structure A. Une coche verte indique que la structure est activée pour FlexAddress. La fonction FlexAddress sert à déployer les adresses permanentes de logement et attribuées par le châssis WWN/MAC dans les divers logements et structures du châssis. Cette fonction est activée en fonction de chaque structure et chaque logement.

REMARQUE : Pour plus d'informations sur la fonction FlexAddress, voir À propos de FlexAddress.

Affichage des informations sur l'adresse WWN ou MAC

Vous pouvez afficher l'inventaire des adresses WWW/MAC des cartes réseau de chaque logement de serveur ou de tous les serveurs dans un châssis. L'inventaire contient les éléments suivants :

- Configuration de la structure

  REMARQUE :

  - **La structure A affiche le type de structure d'entrée/sortie installée. Si la structure A est activée, les logements non affectés affichent les adresses MAC affectées par le châssis de la structure A.**
  - **Le contrôleur de gestion iDRAC n'est pas une structure, mais sa FlexAddress est considérée correspondre à une structure.**
  - **SI la case associée à un composant est cochée, cela implique que la structure est activée pour FlexAddress ou FlexAddressPlus.**
- Protocole utilisé sur le port de la carte NIC. Par exemple, LAN, iSCSI et FCoE.
- Configuration Fibre Channel World Wide Name (WWN) et adresses MAC (Media Access Control d'un logement dans le châssis.
- Type d'attribution de l'adresse MAC et type d'adresse actif actuel : attribuée par le serveur, FlexAddress ou MAC d'identité d'E/S. Une coche noire indique le type de l'adresse active, c'est-à-dire attribuée par le serveur, attribuée par le châssis ou attribuée à distance.
- L'état des partitions NIC des périphériques prenant en charge le partitionnement.

Vous pouvez afficher l'inventaire des adresses WWN/MAC à l'aide de l'interface Web ou de l'interface de ligne de commande de RACADM. En fonction de l'interface, vous pouvez filtrer l'adresse MAC et savoir quelle adresse WWN/MAC est utilisée pour cette fonction ou partition. Si NPAR est activé sur la carte, vous pouvez afficher les partitions qui sont activées ou désactivées.

En utilisant l'interface Web, vous pouvez afficher les informations des adresses WWN/MAC pour les éléments suivants :

- Emplacements spécifiques : ouvrez la page **FlexAddress** en cliquant sur **Présentation du serveur** > **Slot <x>** > **Configuration** > **FlexAddress**.
- Tous les logements et le serveur : ouvrez la page **Récapitulatif WWN/MAC** en cliquant sur **Présentation du serveur** > **Propriétés** > **WWN/MAC**.

Dans les deux pages, vous pouvez afficher les informations des adresses WWN/MAC dans le mode de base ou dans le mode Avancé :

- **Mode de base** : dans ce mode, vous pouvez afficher le logement du serveur, la structure, le protocole, les adresses WWN/MAC et l'état de la partition. Seules les adresses MAC actives s'affichent dans la zone d'adresse WWN/MAC. Vous pouvez les filtrer à l'aide de certains des champs affichés ou de tous les champs :
- **Mode avancé** : dans ce mode, vous pouvez voir à la fois tous les champs affichés dans le mode basique et tous les types d'adresses MAC (Attribuée par le serveur, FlexAddress et Identité d'E/S). Vous pouvez les filtrer à l'aide de certains des champs affichés ou de tous les champs.

Dans le mode Basique et le mode Avancé, les informations des adresses WWN/MAC s'affichent dans un format réduit. Cliquez sur le symbole plus  en regard d'un logement, ou cliquez sur le bouton **Développer/Réduire tout** pour afficher les informations d'un logement ou de tous les logements.

Vous pouvez également exporter les informations des adresses WWN/MAC pour tous les serveurs du châssis dans un dossier local.

Pour plus d'informations sur les champs, voir l'*Aide en ligne*.

Affichage des informations sur l'adresse WWN ou MAC de base à l'aide de l'interface Web

Pour afficher les informations relatives à l'adresse WWN/MAC pour chaque logement de serveur ou tous les serveurs présents dans le châssis, en mode basique, procédez comme suit :

1. Cliquez sur **Présentation du serveur** > **Propriétés** > **WWN/MAC**.
   La page **Résumé WWN/MAC** affiche les informations des adresses WWN/MAC.

   Vous pouvez également cliquer sur **Présentation du serveur** > **Logement <x>** > **Configuration** > **FlexAddress** pour afficher les informations d'adresse WWN/MAC d'un logement de serveur. La page **FlexAddress** s'affiche.
2. Dans le tableau **Adresses WWN/MAC**, cliquez sur **Exporter** pour enregistrer les adresses WWN/MAC au niveau local.
3. Cliquez sur le symbole  correspondant à un logement, ou sur le bouton **Développer/Réduire tout** pour développer ou réduire les attributs répertoriés pour un logement spécifique ou tous les logements dans le tableau d'adresses WWN/MAC.
4. Dans le menu déroulant **Afficher**, sélectionnez **Basique**, pour afficher les attributs des adresses WWN/MAC dans la vue d'arborescence.
5. Dans le menu déroulant **Logement du serveur**, sélectionnez **Tous les serveurs,** ou un logement spécifique pour afficher les attributs des adresses WWN/MAC de tous les serveurs ou de serveurs dans des logements spécifiques uniquement.
6. Dans le menu déroulant **Structure**, sélectionnez l'un des types de structure pour afficher les détails de tous les types ou uniquement de certains types de gestion ou de structure d'E/S associés aux serveurs.
7. Dans le menu déroulant **Protocole**, sélectionnez **Tous les protocoles** ou l'un des protocoles réseau répertoriés pour afficher toutes les adresses MACS ou les adresses MAC associées au protocole sélectionné.
8. Dans le champ **Adresses WWN/MAC**, entrez l'adresse MAC partielle ou complète MAC pour afficher uniquement les logements associés à l'adresse MAC.
9. Dans le menu déroulant **Condition de partition**, sélectionnez la condition des partitions pour afficher les serveurs dotés de la condition de partition sélectionnée.

Pour plus d'informations sur les champs, voir l'*Aide en ligne*.

Affichage des informations avancées d'adresse WWN ou MAC à l'aide de l'interface Web

Pour afficher les informations d'adresse WWN/MAC de chaque logement de serveur ou de tous les serveurs présents dans le châssis, en mode avancé, procédez comme suit :

1. Cliquez sur **Présentation du serveur** > **Propriétés** > **WWN/MAC**.
   La page **Résumé WWN/MAC** affiche les informations des adresses WWN/MAC.
2. Dans le menu déroulant **Afficher**, sélectionnez **Avancé** pour afficher les attributs des adresses WWN/MAC dans une vue détaillée.

Le tableau **Adresses WWN/MAC** affiche Logement de serveur, Structure, Protocole, Adresses WWN/MAC, État de la partition et le type d'attribution de l'adresse MAC : Attribué par serveur, FlexAddress ou Identité d'E/S MAC. Une coche noire indique le type de l'adresse active, c'est-à-dire attribuée par le serveur, attribuée par le châssis ou attribuée à distance. MAC.

3. Dans le tableau **Adresses WWN/MAC**, cliquez sur **Exporter** pour enregistrer les adresses WWN/MAC au niveau local.
4. Cliquez sur le symbole + correspondant à un logement, ou sur le bouton **Développer/Réduire tout** pour développer ou réduire les attributs répertoriés pour un logement ou tous les logements dans le tableau d'adresses WWN/MAC.
5. Dans le menu déroulant **Logement du serveur**, sélectionnez **Tous les serveurs,** ou un logement spécifique pour afficher les attributs des adresses WWN/MAC de tous les serveurs ou de serveurs dans des logements spécifiques uniquement.
6. Dans le menu déroulant **Structure**, sélectionnez l'un des types de structure pour afficher les détails de tous les types ou uniquement de certains types de gestion ou de structure d'E/S associés aux serveurs.
7. Dans le menu déroulant **Protocole**, sélectionnez **Tous les protocoles** ou l'un des protocoles réseau répertoriés pour afficher toutes les adresses MACS ou les adresses MAC associées au protocole sélectionné.
8. Dans le champ **Adresses WWN/MAC**, saisissez l'adresse MAC pour afficher uniquement les emplacements associés à l'adresse MAC spécifique.
9. Dans le menu déroulant **Condition de partition**, sélectionnez la condition des partitions pour afficher les serveurs dotés de la condition de partition sélectionnée.

   Si une partition donnée est désactivé, la condition s'affiche en tant que **Désactivé** et la ligne contenant la partition est grisée.

Pour plus d'informations sur les champs, voir l'*Aide en ligne*.

Affichage des informations d'adresse WWN ou MAC à l'aide de l'interface RACADM

Pour afficher les informations d'adresse WWN/MAC de tous les serveurs ou de serveurs spécifiques à l'aide de RACADM, utilisez les sous-commandes `getflexaddr` et `getmacaddress`.

Pour afficher FlexAddress pour l'ensemble du châssis, utilisez la commande RACADM suivante :

```
racadm getflexaddr
```

Pour afficher l'état de FlexAddress pour un logement en particulier, utilisez la commande RACADM suivante :

```
racadm getflexaddr [-i <slot#>]
```

où *<slot#>* est une valeur comprise entre 1 et 4.

Pour afficher l'adresse MAC de la carte fille réseau NDC ou LOM, utilisez la commande RACADM suivante :

```
racadm getmacaddress
```

Pour afficher l'adresse MAC du châssis, utilisez la commande RACADM suivante :

```
racadm getmacaddress -m chassis
```

Pour afficher les adresses MAC iSCSI de tous les serveurs, utilisez la commande RACADM suivante :

```
racadm getmacaddress -t iscsi
```

Pour afficher les adresses MAC iSCSI d' un serveur spécifique, utilisez la commande RACADM suivante :

```
racadm getmacaddress [-m <module> [-x]] [-t iscsi]
```

Pour afficher l'adresses MAC et WWN définie par l'utilisateur, utilisez la commande RACADM suivante :

```
racadm getmacaddress -c io-identity
```

```
racadm getmacaddress -c io-identity -m server -2
```

Pour afficher l'adresse MAC/WWN attribuée par la console de toutes les cartes réseau intégrées ou des cartes mezzanine, utilisez la commande RACADM suivante :

```
racadm getmacaddress -c all
```

Pour afficher les adresses WWN/MAC attribuées par le châssis, utilisez la commande RACADM suivante :

```
racadm getmacaddress -c flexaddress
```

Pour afficher les adresses MAC/WWN de toutes les cartes réseau intégrées ou des cartes mezzanine, utilisez la commande RACADM suivante :

```
racadm getmacaddress -c factory
```

Pour afficher les adresses MAC/WWN Ethernet et iSCSI de toutes les cartes iDRAC/LOM/mezzanine, utilisez la commande RACADM suivante :

```
racadm getmacaddress -a
```

Pour plus d'informations sur les sous-commandes `getflexaddr` et `getmacaddress`, reportez-vous au *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX*.

Messages des commandes

Le tableau suivant répertorie les commandes RACADM et leurs sorties pour des problèmes FlexAddress courants.

Tableau 36. Commandes et sortie FlexAddress

Problème	Commande	Sortie
La carte SD du contrôleur CMC actif est liée à un autre numéro de service.	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)` `FlexAddress: bound to another chassis, svctag = <Service tag Number> SD card SN = <Valid flex address serial number>`
La carte SD du contrôleur CMC actif est liée au même numéro de service.	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)` `FlexAddress: bound`
La carte SD du contrôleur CMC actif n'est liée à aucun numéro de service.	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)` `FlexAddress:not bound`
La fonctionnalité FlexAddress n'est pas active sur le châssis pour une raison inconnue (Pas de carte SD insérée/carte SD corrompue/ fonctionnalité désactivée/carte SD liée à un autre châssis)	`$racadm setflexaddr [-f <fabricName> <slotState>]` `$racadm setflexaddr [-i <slot#> <slotstate>]`	`ERROR: Flexaddress feature is not active on the chassis`
L'utilisateur invité tente de définir FlexAddress sur des logements/des structures.	`$racadm setflexaddr [-f <fabricName> <slotState>]` `$racadm setflexaddr [-i <slot#> <slotstate>]`	`ERROR: Insufficient user privileges to perform operation`

Tableau 36. Commandes et sortie FlexAddress (suite)

Problème	Commande	Sortie
Désactivation de la fonctionnalité FlexAddress alors que le châssis est sous tension	`$racadm feature -d -c flexaddress`	`ERROR: Unable to deactivate the feature because the chassis is powered ON`
L'utilisateur invité essaie de désactiver la fonctionnalité sur le châssis	`$racadm feature -d -c flexaddress`	`ERROR: Insufficient user privileges to perform operation`
Modification des paramètres FlexAddress de logement/structure pendant que les modules de serveur sont sous tension.	`$racadm setflexaddr -i 1 1`	`ERROR: Unable to perform the set operation because it affects a powered ON server`
Modification des paramètres Flexaddress d'un logement ou d'une structure lorsque la licence d'entreprise CMC n'est pas installée.	`$racadm setflexaddr -i<slotnum> <status>` `$racadm setflexaddr -f<FabricName> <status>`	`ERROR: SWC0242 : A required license is missing or expired. Obtain an appropriate license and try again, or contact your service provider for additional details.` **REMARQUE : Pour résoudre ce problème, vous devez disposer d'une licence d'Activation de FlexAddress.**

CONTRAT DE LICENCE DES LOGICIELS DELL FlexAddress

Ceci est un contrat légal entre vous, l'utilisateur et Dell Products L.P. ou Dell Global B.V. (« Dell »). Cet accord couvre tous les logiciels distribués avec le produit Dell et pour lesquels il n'existe aucun contrat de licence distinct entre vous et le fabricant ou propriétaire des logiciels en question (collectivement « le logiciel »). Ce contrat ne peut donner lieu à la vente du logiciel et de toute autre propriété intellectuelle. Tous les titres et droits de propriété intellectuelle concernant le logiciel sont la propriété du fabricant ou propriétaire du logiciel. Tous les droits non expressément octroyés dans le cadre du présent contrat sont réservés au fabricant ou propriétaire du logiciel. En ouvrant le ou les emballages du logiciel, ou en brisant leur sceau de sécurité, en installant ou en téléchargeant le logiciel, ou en utilisant le logiciel préchargé ou intégré dans votre produit, vous acceptez d'être lié par les conditions du présent contrat. Si vous n'acceptez pas ces conditions, renvoyez immédiatement tous les éléments du logiciel (disques, documentation écrite et emballages), et supprimez tout le logiciel préchargé ou intégré.

Vous êtes autorisé à utiliser une seule copie du logiciel, sur un seul ordinateur à la fois. Si vous avez plusieurs licences pour le logiciel, vous pouvez utiliser simultanément autant de copies de vous avez de licences. Le terme « utiliser » désigne ici le chargement du logiciel dans la mémoire temporaire ou dans le stockage permanent de l'ordinateur. L'installation sur un serveur réseau uniquement en vue de la distribution vers d'autres ordinateurs n'est pas considérée comme une « utilisation », mais cela s'applique uniquement si vous disposez d'une licence séparée pour chacun des ordinateurs vers lesquels vous distribuez le logiciel. Vous devez vous assurer que le nombre de personnes qui utilisent le logiciel installé sur un serveur réseau ne dépasse pas celui des licences que vous possédez. Si le nombre des utilisateurs du logiciel installé sur un serveur réseau dépasse le nombre des licences, vous devez acheter des licences supplémentaires afin que le nombre des licences soit égal à celui des utilisateurs, avant d'autoriser des utilisateurs supplémentaires à utiliser le logiciel. Si vous êtes un client commercial de Dell ou une filiale Dell, vous autorisez par la présente Dell ou tout agent choisi par Dell, à effectuer un audit de votre utilisation du logiciel au cours des heures de bureau normales, vous acceptez de coopérer avec Dell pour cet audit et vous acceptez de fournir à Dell, dans les limites du raisonnable, tous les dossiers liés à votre utilisation du logiciel. L'audit se limite à la vérification de votre conformité aux conditions du présent contrat.

Le logiciel est protégé par les lois des États-Unis et les divers traités internationaux relatifs aux droits d'auteur. Vous pouvez créer une seule copie du logiciel, uniquement à des fins de sauvegarde ou d'archivage, ou le transférer vers un seul disque dur, à condition de conserver l'original uniquement pour la sauvegarde ou l'archivage. Vous ne pouvez pas louer le logiciel ni le céder en crédit-bail, ni copier les documents papier qui accompagnent le logiciel, mais vous pouvez transférer définitivement le logiciel et toute la documentation qui l'accompagne dans le cadre d'une vente ou d'un transfert du produit Dell, si vous n'en conservez aucune copie et si le destinataire accepte les conditions du présent contrat. Tout transfert doit inclure la mise à jour la plus récente et toutes les versions précédentes. Il est interdit d'effectuer l'ingénierie inverse du logiciel, de le décompiler ou de le désassembler. Si l'emballage accompagnant votre ordinateur contient des CD, ou des disques 3,5 pouces et/ou 5,25 pouces, vous ne pouvez utiliser que les disques conçus pour votre ordinateur. Vous n'avez pas le droit d'utiliser ces disques sur un autre ordinateur ou réseau, ni de les prêter, les louer, les céder en crédit-bail ou les transférer vers un autre utilisateur, sauf condition expresse du présent contrat.

GARANTIE LIMITÉE

Dell garantit que les disques du logiciel sont exempts de défaut matériel et de fabrication pour une utilisation normale pendant quatre-vingt-dix (90) jours à compter de la date où vous les recevez. Cette garantie s'applique uniquement à vous-même et n'est pas transférable. Toutes les garanties implicites sont limitées à quatre-vingt-dix (90) jours à compter de la date de réception du logiciel. Certaines juridictions n'autorisent aucune limite de durée d'une garantie implicite, si bien que cette limitation peut ne pas s'appliquer à vous. L'entière responsabilité de Dell et de ses fournisseurs, et votre seul recours, correspond (a) au remboursement du prix payé pour le logiciel ou (b) au remplacement de tout disque non conforme aux termes de la garantie, renvoyé à Dell avec un numéro d'autorisation de retour, à vos propres coûts et risques. Cette garantie limitée est nulle et non avenue si les dommages des disques résultent d'un accident, d'un abus, d'une utilisation incorrecte, d'un entretien ou d'une modification par une personne autre que Dell. Les disques de remplacement sont garantis pour la durée restante de la garantie d'origine ou pour trente (30) jours. La durée la plus longue sera appliquée.

Dell ne garantit PAS que les fonctions du logiciel répondront à vos besoins, ni que le fonctionnement du logiciel sera ininterrompu ou exempt d'erreur. Vous assumez l'entière responsabilité du choix de ce logiciel pour obtenir les résultats recherchés, ainsi que de l'utilisation et des résultats du logiciel.

DELL, EN SON PROPRE NOM ET EN CELUI DE SES FOURNISSEURS, REJETTE TOUTE AUTRE GARANTIE, EXPRESSE OU IMPLICITE, Y COMPRIS MAIS SANS S'Y LIMITER, LES GARANTIES IMPLICITES DE VALEUR MARCHANDE ET D'ADÉQUATION À UNE UTILISATION PARTICULIÈRE, POUR LE LOGICIEL ET TOUTE LA DOCUMENTATION ÉCRITE QUI L'ACCOMPAGNE. Cette garantie limitée vous donne des droits légaux spécifiques ; vous pouvez avoir d'autres droits, qui varient d'une juridiction à l'autre.

DELL OU SES FOURNISSEURS NE SAURAIENT EN AUCUN CAS ÊTRE TENUS POUR RESPONSABLE DES ÉVENTUELS DOMMAGES (Y COMPRIS, SANS S'Y LIMITER, LES DOMMAGES DE TYPE PERTE DE PROFIT, INTERRUPTION DES ACTIVITÉS, PERTE D'INFORMATIONS COMMERCIALES OU AUTRE PERTE FINANCIÈRE) DÉCOULANT DE L'UTILISATION OU DE L'IMPOSSIBILITÉ D'UTILISER LE LOGICIEL, MÊME S'ILS ONT ÉTÉ AVERTIS DE L'ÉVENTUALITÉ DE TELS DOMMAGES. Comme certaines juridictions n'autorisent pas l'exclusion ou la limitation de responsabilité pour les dommages induits ou accidentels, la limitation ci-dessus ne s'applique pas forcément à votre cas.

LOGICIEL LIBRE (Open Source)

Une partie de ce CD peut contenir des logiciels libres, que vous pouvez utiliser conformément aux termes et conditions des licences spécifiques sous lesquelles ils ont été distribués.

CE LOGICIEL OPEN SOURCE EST DISTRIBUÉ DANS L'ESPOIR QU'IL VOUS SERA UTILE, MAIS IL EST FOURNI « EN L'ÉTAT », SANS AUCUNE GARANTIE EXPRESSE OU IMPLICITE, Y COMPRIS MAIS SANS S'Y LIMITER LES GARANTIES IMPLICITES DE VALEUR MARCHANDE OU D'ADÉQUATION À UNE UTILISATION PARTICULIÈRE. DELL, LES DÉTENTEURS DES DROITS DE COPYRIGHT OU LES CONTRIBUTEURS DU LOGICIEL NE SAURAIENT EN AUCUN CAS ÊTRE TENUS POUR RESPONSABLES DES ÉVENTUELLES DOMMAGES DIRECTS, INDIRECTS, CONSÉCUTIFS, SPÉCIAUX, EXEMPLAIRES OU INDUITS (Y COMPRIS MAIS SANS S'Y LIMITER LA FOURNITURE DE BIENS OU SERVICES DE SUBSTITUTION, LA PERTE D'UTILISATION, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉS), QUELLE QU'EN SOIT LA CAUSE, NI DES ÉVENTUELLES PLAINTES, PAR ACTION OU CONTRAT, DÉLIT OU AUTRE (Y COMPRIS LA NÉGLIGENCE OU AUTRES CAUSES) DÉCOULANT DE QUELQUE MANIÈRE QUE CE SOIT DE L'UTILISATION DE CE LOGICIEL, MÊME S'ILS ONT ÉTÉ AVERTIS DE L'ÉVENTUALITÉ DE TELS DOMMAGES.

DROITS RESTREINTS DU GOUVERNEMENT DES ÉTATS-UNIS

Le logiciel et sa documentation sont des « articles commerciaux », conformément à la définition de ce terme dans le document 48 C.F.R. 2.101, comprenant d'une part un « logiciel informatique commercial » et d'autre part une « documentation de logiciel informatique commercial », conformément à la définition de ces termes dans le document 48 C.F.R. 12.212. Selon les termes des documents 48 C.F.R. 12.212 et 48 C.F.R. 227.7202-1 à 227.7202-4, tous les utilisateurs finaux appartenant au Gouvernement des États-Unis acquièrent le logiciel et sa documentation avec uniquement les droits décrits dans le présent document.

Fournisseur/Éditeur du logiciel: Dell Products, L.P., One Dell Way, Round Rock, Texas 78682.

CONSIGNES GÉNÉRALES

Cette licence reste en vigueur jusqu'à son expiration. Elle expire selon les conditions décrites ci-dessus, ou si vous ne respectez pas certaines des conditions du présent contrat. À l'expiration de la licence, vous acceptez de détruire le logiciel et les documents associés, ainsi que toutes les copies existantes. Ce contrat est régi par les lois de l'État du Texas. Chaque disposition de ce contrat est dissociable. Si une disposition n'est pas applicable, cela n'affecte en aucune manière l'applicabilité des autres dispositions, termes ou conditions du contrat. Ce contrat lie vos successeurs et délégués. Dell accepte et vous acceptez de renoncer dans les limites maximales autorisées par la loi, à tout droit de procédure juridique concernant le logiciel ou le présent contrat. Comme cette renonciation n'est pas valide dans certaines juridictions, cette clause peut ne pas s'appliquer à votre cas. Vous reconnaissez que vous avez lu le présent contrat, que vous le comprenez, que vous acceptez d'être lié par ses conditions, et qu'il s'agit de l'expression complète et exclusive de l'accord conclu entre vous et Dell concernant le logiciel.

13

Gestion des structures

Le châssis prend en charge un type de structure, la structure A. Cette structure est utilisée par le module d'E/S unique et elle est toujours connectée aux adaptateurs Ethernet intégrés de serveurs.

Le châssis ne dispose que d'un seul module d'E/S (IOM), où l'IOM est un relais ou un module de commutation. Le module d'E/S est classifié comme groupe A.

L'IOM du châssis utilise un chemin discret appelé **Structure** et il s'appelle A. La structure A prend en charge Ethernet uniquement. Chaque adaptateur d'E/S de serveur (carte mezzanine ou LOM) peut avoir deux ou quatre ports selon la fonction. Les logements de carte mezzanine sont occupés par les cartes d'extension connectées aux cartes PCIe (et non pas aux modules d'E/S). Lorsque vous déployez les réseaux Ethernet, iSCSI ou FibreChannel, étendez leurs liaisons redondantes dans les blocs 1 et 2 pour optimiser la disponibilité. L'IOM discret est identifié par un identificateur de structure.

REMARQUE : Dans l'interface CLI CMC, l'IOM s'appelle par convention, un commutateur.

Sujets :

Nouveau scénario de démarrage

Lorsque le châssis est connecté et sous tension, le module d'E/S est prioritaire sur les serveurs. Le module IOM est autorisé à se mettre sous tension avant les autres. À ce stade la vérification de leurs types de structures n'est pas exécutée.

Une fois les modules IOM sous tension, les serveurs sont mis sous tension, puis le contrôleur CMC vérifie les serveurs pour déterminer la cohérence de structure.

Vous pouvez placer un module d'intercommunication et un commutateur dans le même groupe si leur structure est identique. Cette coexistence de commutateurs et modules d'intercommunication dans un même groupe est possible même s'ils sont fabriqués par des fournisseurs différents.

Surveillance de l'intégrité des modules d'E/S (IOM)

Pour plus d'informations sur la surveillance de l'intégrité IOM, voir Affichage des informations et de l'état d'intégrité des modules IOM.

Définition des paramètres réseau pour le module IOM

Vous pouvez spécifier les paramètres réseau de l'interface utilisée pour gérer le module d'E/S (IOM). Pour les commutateurs Ethernet, le port de gestion hors bande (adresse IP) est configuré. Le port de gestion intrabande (VLAN1) n'est pas configuré avec cette interface.

Avant de définir les paramètres réseau pour le module IOM, vérifiez que ces modules sont sous tension.

Pour pouvoir définir les paramètres réseau pour le module IOM dans le groupe A, vous devez disposer des privilèges d'administrateur de structure A.

REMARQUE : Pour les commutateurs Ethernet, les adresses IP de gestion intrabande (VLAN1) et hors bande doivent être différentes et sur des réseaux différents. Par conséquent, l'adresse IP hors bande n'est pas définie. Consultez la documentation IOM pour connaître l'adresse IP de gestion intrabande par défaut.

REMARQUE : Ne configurez pas les paramètres réseau des modules d'E/S pour les commutateurs d'intercommunication Ethernet et Infiniband.

Définition des paramètres réseau du module IOM à l'aide de l'interface Web CMC

Pour définir les paramètres réseau du module d'E-S :

1. Dans le volet de gauche, cliquez sur **présentation du châssis**, **Présentation du module d'E/S** et sur **Configurer**. Pour définir les paramètres réseau du seul module d'E-S disponible **A**, cliquez sur **Gigabit Ethernet A** et sur **Configurer**.
   Sur la page **Configurer les paramètres réseau du module d'E/S**, entrez les données appropriées et cliquez sur **Appliquer**.
2. Si vous y êtes autorisé, entrez le mot de passe de l'utilisateur root, la chaîne SNMP RO Community et l'adresse IP du serveur Syslog du module IOM. Pour plus d'informations sur les champs, voir l'*Aide en ligne*.

   REMARQUE : L'adresse IP définie dans le module IOM depuis le contrôleur CMC n'est pas enregistrée dans la configuration permanente de démarrage du commutateur. Pour l'enregistrer définitivement, vous devez entrer la commande `connect switch` ou la commande RACADM `racadm connect switch` ou bien utiliser une interface directe à l'interface utilisateur graphique du module IOM pour enregistrer cette adresse dans le fichier de configuration du démarrage.

   REMARQUE : La chaîne de communauté SNMP peut comprendre des caractères ASCII de la plage de valeurs 33–125.

3. Cliquez sur **Appliquer**.
   Les paramètres réseau sont définis pour le module IOM.

   REMARQUE : Si vous y êtes autorisé, vous pouvez réinitialiser les valeurs de configuration par défaut des réseaux VLAN, des propriétés réseau et des ports d'E/S.

Définition des paramètres réseau d'un module IOM à l'aide de RACADM

Pour définir les paramètres réseau d'un module IOM en utilisant RACADM, définissez la date et l'heure. Voir la section de la commande deploy dans le document *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX).

Vous pouvez définir le nom d'utilisateur, le mot de passe et la chaîne SNMP du module IOM en utilisant la commande RACADM deploy :

```
racadm deploy -m switch -u <nom d'utilisateur> -p <mot de passe>
```

```
racadm deploy -m switch -u -p <mot de passe> -v SNMPv2 <snmpCommunityString> ro
```

```
racadm deploy -a [server|switch] -u <nom d'utilisateur> -p <mot de passe>
```

Gestion des opérations de contrôle de l'alimentation pour les modules IOM

Pour plus d'informations sur la définition des opérations de contrôle de l'alimentation pour les modules d'E/S, voir Exécution d'opérations de contrôle de l'alimentation sur un module d'E/S.

Activation ou désactivation du clignotement des LED des IOM

Pour plus d'informations sur l'activation du clignotement des voyants pour les modules d'E/S (IOM), voir Configuration des voyants pour identifier les composants du châssis.

14

Gestion et surveillance de l'alimentation

Le châssis PowerEdge VRTX est le châssis de serveurs modulaire le plus économe en énergie. Il contient des blocs d'alimentation et ventilateurs très économes en énergie, et sa structure est optimisée pour faciliter la circulation de l'air dans l'ensemble du système. Il est pourvu de composants économes en énergie. Cette conception matérielle optimisée est associée à des fonctions avancées de gestion de l'alimentation, intégrées au contrôleur CMC (Chassis Management Controller), aux blocs d'alimentation et à l'interface iDRAC pour disposer d'un environnement de serveurs encore plus économe en énergie.

Les fonctions de gestion de l'alimentation du PowerEdge VRTX aident les administrateurs à configurer le boîtier pour réduire la consommation électrique et à ajuster l'alimentation en fonction des besoins spécifiques de l'environnement.

Le châssis modulaire PowerEdge VRTX consomme du courant alternatif et distribue la charge entre tous les blocs d'alimentation internes actifs. Le système peut générer jusqu'à 4 800 watts CA alloués aux modules serveurs et à l'infrastructure de boîtier associée. Cependant, cette capacité varie en fonction de la politique de redondance que vous sélectionnez.

Le boîtier PowerEdge VRTX peut être configurée pour n'importe laquelle des deux politiques de redondance qui affectent le comportement des blocs d'alimentation et déterminent la manière dont l'état de redondance du châssis est signalé aux administrateurs.

Vous pouvez également contrôler la gestion de l'alimentation via **OpenManage Power Center (OMPC)**. Lorsque OMPC contrôle l'alimentation en externe le contrôleur CMC continue de gérer :

- Règle de redondance
- Journalisation distante de l'alimentation
- DPSE (Dynamic Power Supply Engagement)

OMPC gère alors :

- l'alimentation du serveur
- La priorité du serveur
- Capacité maximale de l'alimentation d'entrée du système
- Mode de conservation de puissance maximale

REMARQUE : La puissance de sortie réelle est basée sur la configuration et la charge de travail.

Vous pouvez utiliser l'interface Web CMC ou RACADM pour gérer et configurer le contrôle de l'alimentation sur le contrôleur CMC :

- Consulter l'allocation d'alimentation, la consommation électrique et l'état d'alimentation du châssis, des serveurs et des blocs d'alimentation
- Configurer le bilan de puissance et la stratégie de redondance du châssis
- Exécuter des opérations de contrôle de l'alimentation (mise sous tension, mise hors tension, réinitialisation du système, cycle d'alimentation) du châssis

Sujets :

Stratégies de redondance

La stratégie de redondance est un ensemble de propriétés configurable qui détermine la façon dont le CMC gère l'alimentation du châssis. Vous pouvez configurer les stratégies de redondance suivantes avec ou sans enclenchement dynamique des blocs d'alimentation :

- Redondance de réseau d'alimentation
- Redondance de l'alimentation électrique

Règle de redondance de réseau d'alimentation

L'objectif de la stratégie de redondance du réseau d'alimentation est de permettre à un système d'enceinte modulaire de fonctionner dans un mode où il peut tolérer les pannes de l'alimentation CA. Ces pannes peuvent provenir du réseau électrique CA, du câblage et de la distribution, ou du bloc d'alimentation proprement dit.

Lorsque vous configurez un système pour la redondance de l'alimentation CA, les blocs d'alimentation sont répartis dans des réseaux électriques : les blocs d'alimentation des logements 1 et 2 se trouvent dans le réseau 1 et les blocs d'alimentation des logements 3 et 4 se trouvent dans le réseau 2. Le CMC gère l'alimentation de manière à ce qu'en cas d'échec d'un des deux réseaux, le système continue de fonctionner sans dégradation. La redondance d'alimentation CA permet aussi la tolérance des pannes des blocs d'alimentation individuels.

REMARQUE : L'un des rôles de la redondance d'alimentation CA est d'assurer le fonctionnement transparent en cas de défaillance de l'ensemble d'un réseau, mais la plus grande puissance est utilisée pour maintenir la redondance d'alimentation CA lorsque les capacités des deux réseaux sont à peu près égales.

REMARQUE : La redondance d'alimentation n'est atteinte que lorsque les conditions de charge ne dépassent pas la capacité du réseau ayant la plus faible puissance.

Niveaux de redondance de l'alimentation de réseau

La configuration minimale nécessaire pour utiliser la redondance d'alimentation CA consiste à installer un bloc d'alimentation dans chaque réseau d'alimentation. Il est possible de réaliser des configurations supplémentaires avec chaque combinaison comportant au moins un bloc d'alimentation dans chaque réseau d'alimentation. Toutefois pour disposer d'un maximum de puissance, vous devez utiliser dans chaque branche un nombre total de blocs d'alimentation aussi égal que possible. La limite maximale de puissance disponible en maintenant la redondance d'alimentation CA est la puissance disponible sur le plus faible des deux réseaux d'alimentation.

Si un contrôleur CMC ne peut pas maintenir la redondance de l'alimentation CA, une alerte par e-mail et/ou SNMP est envoyée aux administrateurs si l'événement Redondance perdue est configuré pour générer des alertes.

En cas de panne d'un seul bloc d'alimentation (PSU) dans cette configuration, les unités d'alimentation restantes dans le réseau défaillant sont marquées comme étant en ligne. Dans cet état, les unités d'alimentation dans le réseau redondant, s'il n'est pas en état d'échec, aident le système à fonctionner sans interruption. En cas de défaillance d'un bloc d'alimentation, l'intégrité du châssis est marquée comme étant non critique. Si le réseau plus petit ne peut pas prendre en charge la totalité des allocations d'alimentation du châssis, l'état de redondance de réseau est **Non** et l'intégrité du châssis est **Critique**.

Stratégie de redondance des blocs d'alimentation

La stratégie de redondance des blocs d'alimentation s'avère utile lorsque vous n'avez pas de réseaux électriques d'alimentation redondants, mais que vous souhaitez protéger le système afin que l'échec d'un seul bloc d'alimentation (PSU) n'éteigne pas les serveurs dans une enceinte modulaire. Le bloc d'alimentation de capacité supérieure est gardé en réserve en ligne dans ce but. Cela crée un pool de blocs d'alimentation.

Les unités d'alimentation se trouvant au-delà de celles exigées pour la puissance et la redondance sont encore disponibles et seront ajoutées au pool en cas de défaillance.

Contrairement à la redondance de réseau d'alimentation, lorsque la redondance du bloc d'alimentation est sélectionnée, le CMC n'a pas besoin que les blocs d'alimentation soient présents dans des positions de logement spécifiques.

REMARQUE : L'engagement dynamique des blocs d'alimentation (Dynamic Power Supply Engagement ou DPSE) permet de mettre les blocs d'alimentation (PSU) en veille. Cet état de veille est un état physique : les blocs ne fournissent aucune alimentation. Lorsque vous activez DPSE, les blocs d'alimentation peuvent être mis en mode Attente pour renforcer l'efficacité et économiser l'énergie.

REMARQUE : Modifiez la règle de redondance enceinte modulaire pendant que le boîtier est mis hors tension.

Enclenchement dynamique des blocs l'alimentation

Par défaut le mode DPSE (Dynamic Power Supply Engagement) est désactivé. Ce mode économise l'énergie en optimisant l'efficacité des blocs d'alimentation électrique qui alimentent le châssis. Cela permet également d'allonger la durée de vie des blocs d'alimentation électrique et de réduire la génération de chaleur. Pour utiliser cette fonction, vous devez disposer d'une licence d'entreprise.

Le contrôleur CMC surveille l'allocation globale d'alimentation du boîtier et fait passer les blocs d'alimentation électrique en mode Veille, ce qui permet d'assurer l'allocation totale d'alimentation du châssis avec un nombre réduit de blocs d'alimentation électrique. Comme les blocs d'alimentation électrique en ligne sont plus efficaces à un taux d'utilisation élevé, cela augmente leur efficacité tout en allongeant la durée de vie des blocs d'alimentation électrique de secours.

Pour faire fonctionner les blocs d'alimentation électrique restants de manière optimale, utilisez les modes de redondance d'alimentation suivants :

- Le mode **Redondance des blocs d'alimentation** avec DPSE permet de fournir une alimentation efficace. Au moins deux blocs d'alimentation sont en ligne, un pour alimenter la configuration et l'autre pour assurer la redondance en cas de défaillance du premier bloc. Le mode de redondance des blocs d'alimentation offre une protection contre la défaillance d'un bloc d'alimentation, mais pas contre une perte de réseau électrique CA.
- Mode de **redondance de réseau d'alimentation** avec DPSE, quand au moins deux blocs d'alimentation sont actifs, un dans chaque réseau d'alimentation. La redondance de réseau d'alimentation équilibre également l'efficacité et la disponibilité maximale pour une configuration de boîtier modulaire partiellement chargée.
- La désactivation de l'enclenchement dynamique des blocs d'alimentation (DPSE) offre la plus faible efficacité étant donné que tous les six blocs d'alimentations sont actifs et partagent la charge, entraînant une plus faible utilisation de chaque bloc d'alimentation.

Le mode DPSE peut être activé pour les deux configurations de redondance d'alimentation électrique expliquées ci-dessus : **Redondance des blocs d'alimentation** et **Redondance du réseau d'alimentation**.

REMARQUE : Dans les modes de configuration à deux blocs d'alimentation, la charge du serveur peut empêcher un bloc d'alimentation électrique de passer en mode Veille.

- Dans une configuration de **redondance d'alimentation électrique**, outre les blocs d'alimentation électrique nécessaires pour alimenter le boîtier, ce dernier maintient toujours un bloc d'alimentation supplémentaire sous tension et marqué **En ligne**. L'utilisation de l'alimentation est surveillée et un bloc d'alimentation peut être passé en mode Veille en fonction de la charge totale du système. Dans une configuration à quatre blocs d'alimentation électrique, deux blocs d'alimentation minimum sont toujours sous tension.

  Comme un boîtier dans la configuration de **redondance d'alimentation** comporte toujours un bloc d'alimentation supplémentaire déclenché, le boîtier peut tolérer la perte d'un seul bloc d'alimentation en ligne et il dispose toujours d'une puissance suffisante pour les modules serveur installés. La perte du bloc d'alimentation électrique en ligne provoque la mise en ligne d'un bloc d'alimentation en veille. Si plusieurs blocs d'alimentation électrique sont défaillants simultanément, l'alimentation de certains modules serveur est coupée et les blocs d'alimentation électrique en veille sont activés.
- Dans la configuration de **redondance de réseau d'alimentation**, tous les blocs d'alimentation sont activés à la mise sous tension du châssis. La consommation électrique est surveillée. Si la configuration du système et la consommation électrique le permettent, les blocs d'alimentation passent en **Veille**. Comme l'état **En ligne** des blocs d'alimentation d'un réseau d'alimentation est le miroir de l'autre réseau, le boîtier peut supporter la perte d'alimentation de tout un réseau électrique sans que l'alimentation du boîtier soit coupée.

  Si les besoins d'alimentation de la configuration avec **Redondance de réseau d'alimentation** augmentent, des PSU sortent du mode **Veille**. Cela maintient la configuration en miroir nécessaire pour la redondance à deux réseaux d'alimentation.

  REMARQUE : Avec le mode DPSE activé, si la demande de puissance augmente dans les deux modes de redondance d'alimentation, les alimentations électriques en veille sont mises en ligne pour récupérer de la puissance.

Configuration de redondance par défaut

Comme indiqué dans le tableau ci-dessous, la configuration de redondance par défaut d'un châssis varie en fonction du nombre de blocs d'alimentation qu'il contient.

Tableau 37. Configuration de redondance par défaut

Configuration des unités d'alimentation	Stratégie de redondance par défaut	Paramètre d'engagement dynamique des blocs d'alimentation par défaut
Deux blocs d'alimentation	Redondance CC	Désactivé

Tableau 37. Configuration de redondance par défaut (suite)

Configuration des unités d'alimentation	Stratégie de redondance par défaut	Paramètre d'engagement dynamique des blocs d'alimentation par défaut
Quatre blocs d'alimentation	Redondance CC	Désactivé

Redondance de réseau d'alimentation

En mode de redondance d'alimentation avec quatre blocs d'alimentation, tous les blocs sont actifs. Deux blocs d'alimentation doivent être connectés à un réseau d'alimentation alors que les deux autres blocs d'alimentation sont connectés à l'autre réseau d'alimentation.

PRÉCAUTION : Pour éviter une panne système et pour garantir l'efficacité de la redondance de l'alimentation, il doit exister un ensemble équilibré de blocs d'alimentation sur les réseaux d'alimentation CA.

En cas de défaillance de l'un des réseaux d'alimentation CA, les blocs d'alimentation du réseau d'alimentation CA opérationnel prennent la relève sans interruption pour les serveurs ou l'infrastructure.

PRÉCAUTION : En mode de redondance CA, il doit exister des ensembles de blocs d'alimentation équilibrés (au moins un bloc dans chaque réseau). Si cette condition n'est pas remplie, la redondance CA n'est pas possible.

Redondance de l'alimentation électrique

Lorsque vous activez la redondance d'alimentation, l'un des blocs d'alimentation du châssis est conservé comme bloc de secours, ce qui garantit que la panne d'un seul bloc ne provoque pas l'arrêt des serveurs ou du châssis. Le mode de redondance de l'alimentation nécessite jusqu'à deux blocs d'alimentation. Les blocs d'alimentation supplémentaires, s'il en existe, sont utilisés pour améliorer l'efficacité du système si le mode DPSE est activé. Après la perte de la redondance, les échecs suivants peuvent provoquer l'arrêt des serveurs du châssis.

Fonction Bilan de puissance des modules matériels

Le CMC offre un service d'établissement d'un bilan de puissance qui vous permet de configurer le bilan de puissance, la redondance et l'alimentation dynamique du châssis.

Le service de gestion de l'alimentation permet d'optimiser la consommation électrique et de réattribuer de la puissance aux différents modules en fonction des besoins.

Le CMC maintient un bilan de puissance de l'enceinte qui réserve la puissance nécessaire à tous les serveurs et composants installés.

Le contrôleur CMC alloue de la puissance à l'infrastructure CMC et aux serveurs dans le châssis. L'infrastructure CMC est constituée des composants du châssis, tels que les ventilateurs, le module d'E/S, les adaptateurs de stockage, les cartes PCIe, le disque physique et la carte principale. Le châssis peut contenir jusqu'à quatre serveurs qui communiquent avec lui via un contrôleur iDRAC. Pour plus d'informations, voir le *Guide d'utilisation d'iDRAC* sur le site **dell.com/support/manuals**.

L'iDRAC fournit à CMC l'enveloppe de puissance dont il a besoin, avant d'allumer le serveur. L'enveloppe de puissance est déterminée par les niveaux de puissance minimal et maximal nécessaires pour garantir le bon fonctionnement du serveur. L'estimation initiale de l'iDRAC repose sur sa connaissance initiale des composants du serveur. Une fois le système en fonctionnement, des composants supplémentaires sont détectés, et l'iDRAC peut augmenter ou réduire les besoins d'alimentation par rapport aux valeurs initiales.

Lorsqu'un serveur est sous tension dans un boîtier, le logiciel iDRAC refait une estimation des besoins en alimentation et demande la modification de l'enveloppe de puissance en conséquence.

Le contrôleur CMC fournit l'alimentation demandée au serveur et la puissance allouée est soustraite du bilan disponible. Lorsque le serveur reçoit une demande de puissance, son logiciel iDRAC surveille en permanence la consommation électrique. En fonction des besoins de puissance, l'enveloppe de puissance iDRAC peut changer sur une période. iDRAC demande une augmentation de puissance si les serveurs utilisent complètement la puissance allouée.

Si la charge est trop importante, les performances des processeurs du serveur peuvent être dégradées pour que la consommation d'énergie reste inférieure à la limite de puissance d'entrée système configurée par l'utilisateur.

Le boîtier PowerEdge VRTX peut fournir la puissance suffisante pour les pics de performance de la plupart des configurations de serveur, mais la majorité des configurations de serveur ne consomment pas la puissance maximale que peut fournir le boîtier. Pour aider les centres de données à allouer de la puissance pour leurs boîtiers, le châssis PowerEdge VRTX permet de définir une limite de puissance d'entrée système pour que la puissance CA tirée de l'ensemble du châssis reste dans un point de seuil donné. Le contrôleur CMC vérifie qu'il existe une puissance disponible suffisante pour faire fonctionner les ventilateurs, le module d'E/S, les adaptateur de stockage, le disque physique, la carte principale et pour lui-même. Cette allocation de puissance s'appelle la puissance d'entrée allouée à l'infrastructure du châssis. Les serveurs d'un boîtier sont mis sous tension après l'infrastructure du châssis. Toute tentative de définir une limitation de puissance d'entrée

système inférieure à la charge de puissance échoue. La charge de puissance est la somme de la puissance allouée à l'infrastructure et de la puissance allouée minimale pour les serveurs alimentés.

REMARQUE : Pour pouvoir utiliser la fonction de limite de puissance, vous devez disposer d'une licence d'entreprise.

Si nécessaire, pour que le bilan de puissance total reste inférieur à la valeur *Limite de la puissance d'entrée système*, le contrôleur CMC alloue aux serveurs une puissance inférieure à la puissance maximale demandée. L'allocation de puissance aux serveurs repose sur le paramètre *Priorité des serveurs*. Les serveurs avec la priorité maximale reçoivent le maximum de puissance, les serveurs de priorité 2 sont alimentés après les serveurs de priorité 1, etc. Les serveurs à priorité basse peuvent obtenir moins de puissance que les serveurs de priorité 1, en fonction de la *capacité de puissance maximale d'entrée système* et du paramètre de *limite de puissance d'entrée système* défini par l'utilisateur.

Les modifications de configuration, telles que l'ajout d'un serveur, de disques durs partagés ou de cartes PCIe au châssis, peuvent nécessiter d'augmenter la *limite de puissance d'entrée système*. Les besoins en puissance dans un boîtier modulaire augmentent également lorsque les conditions thermiques changent et que les ventilateurs doivent fonctionner plus rapidement et consomment donc plus d'énergie. L'insertion d'un module d'E/S et de cartes de stockage, de cartes PCIe, d'un disque physique, d'une carte principale, ainsi que le nombre, le type et la configuration des blocs d'alimentations électrique augmentent également les besoins en puissance du boîtier modulaire. Une petite quantité de puissance est consommée par les serveurs, même lorsqu'ils sont arrêtés afin de maintenir actif le contrôleur de gestion.

Vous ne pouvez mettre sous tension des serveurs supplémentaires dans le boîtier modulaire que si la puissance disponible est suffisante. Vous pouvez à tout moment augmenter la *limite de puissance d'entrée système*, jusqu'à un maximum de 5 000 watts pour permettre la mise sous tension des serveurs supplémentaires.

Les changements dans l'enceinte modulaire permettant de réduire l'allocation de puissance sont :

- Serveur hors tension
- Module d'E/S hors tension
- Adaptateurs de stockage, cartes PCIe, disque physique et carte principale hors tension
- Passage du châssis à l'état hors tension

Vous pouvez redéfinir la *limite de la puissance d'entrée système* lorsque le châssis est sous ou hors tension.

Paramètres de priorité de l'alimentation des logements de serveur

Le contrôleur CMC permet de définir la priorité d'alimentation de chacun des quatre logements d'une enceinte. Les paramètres de priorité vont de 1 (le plus élevé) à 9 (le plus faible). Ces paramètres sont attribués aux logements du châssis et tout serveur inséré dans un logement hérite de la priorité du logement. Le contrôleur CMC utilise la priorité de logement pour allouer la puissance d'alimentation aux serveurs de l'enceinte dont le niveau de priorité est le plus élevé.

Avec le paramètre par défaut de priorité des logements de serveur, la puissance est répartie également entre tous les logements. La modification des priorités de logement permet aux administrateurs de hiérarchiser les serveurs auxquels donner la priorité pour l'allocation d'alimentation. Si les modules de serveur les plus critiques sont maintenus au niveau de priorité de logement par défaut (priorité 1) et si vous basculez les modules de serveur moins importants vers un niveau de priorité plus faible (2 ou plus), les modules de priorité 1 sont allumés en premier. Ces serveurs de priorité élevée obtiennent l'allocation de puissance maximale, alors que les serveurs de priorité faible risquent de recevoir une puissance insuffisante pour fonctionner avec des performances optimales. Ils peuvent même ne pas s'allumer du tout, selon la valeur de limite de puissance d'entrée système et des besoins d'alimentation des serveurs.

Si un administrateur met sous tension manuellement des modules serveur à priorité faible avant les modules à priorité élevée, les modules de priorité faible sont les premiers dont l'allocation de puissance est réduite à la valeur minimale afin de donner la préférence aux serveurs à priorité élevée. Par conséquent, une fois la puissance disponible pour l'allocation entièrement consommée, le contrôleur CMC récupère de la puissance auprès des serveurs à priorité inférieure ou égale, jusqu'à ce qu'ils atteignent leur niveau d'alimentation minimal.

REMARQUE : Le module d'E/S, les ventilateurs, la carte principale, les disques physiques et les adaptateurs de stockage reçoivent la priorité la plus élevée. Le contrôleur CMC récupère de la puissance uniquement depuis les périphériques à faible priorité pour répondre aux besoins de puissance d'un périphérique ou d'un serveur à haute priorité.

Affectation de niveaux de priorité aux serveurs

Lorsque plus de puissance est nécessaire, les niveaux de priorité des serveurs déterminent les serveurs depuis lesquels le contrôleur CMC récupère de la puissance.

REMARQUE : La priorité que vous affectez à un serveur est liée à l'emplacement du serveur et non pas au serveur lui-même. Si vous placez le serveur dans un autre logement, vous devez redéfinir la priorité du nouveau logement.

REMARQUE : Vous devez disposer du privilège Administrateur de configuration de châssis pour effectuer les tâches de gestion de l'alimentation.

Affectation de niveaux de priorité aux serveurs à l'aide de l'interface Web du contrôleur CMC

Pour définir des niveaux de priorité :

1. Dans le volet de gauche, cliquez sur **Présentation du serveur** > **Alimentation** > **Priorité**.
   La page **Priorité des serveurs** affiche tous les serveurs du châssis.
2. Dans le menu déroulant **Priorité**, sélectionnez un niveau de priorité (1–9, où 1 est la priorité la plus élevée) pour un ou plusieurs serveurs ou pour tous les serveurs. La valeur par défaut est 1. Vous pouvez affecter le même niveau de priorité à plusieurs serveurs.
3. Cliquez sur **Appliquer** pour enregistrer vos modifications.

Affectation de niveaux de priorité aux serveurs à l'aide de l'interface RACADM

Ouvrez une console texte série/Telnet/SSH d'accès à CMC, ouvrez une session et entrez :

```
racadm config -g cfgServerInfo -o cfgServer Priority -i <numéro de logement> <niveau de priorité>
```

où <*slot number*> (de 1 à 4) correspond au logement du serveur, et <*priority level*> est une valeur comprise entre 1 et 9.

Par exemple, pour définir le niveau de priorité 1 pour le serveur installé dans le logement 4, entrez la commande suivante :

```
racadm config -g cfgServerInfo -o cfgServerPriority -i 4 1
```

Affichage de la condition de la consommation électrique

CMC fournit la consommation électrique d'entrée réelle de l'ensemble du système.

Affichage de la condition de la consommation énergétique à l'aide de l'interface Web du CMC

Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Alimentation** > **Surveillance de l'alimentation**. La page Surveillance de l'alimentation affiche l'intégrité de l'alimentation, l'état de l'alimentation du système, des statistiques de puissance en temps réel et des statistiques d'énergie en temps réel. Pour plus d'informations, voir l'*Aide en ligne*.

REMARQUE : Vous pouvez également afficher l'état de la redondance d'alimentation sous Blocs d'alimentation.

Affichage de l'état de la consommation énergétique à l'aide de RACADM

Pour afficher la condition de la consommation énergétique à l'aide de RACADM :

Ouvrez une console texte série/Telnet/SSH d'accès à CMC, ouvrez une session et entrez :

```
racadm getpminfo
```

Restauration de l'alimentation secteur

Si l'alimentation secteur d'un système est interrompue, le châssis est restauré à l'état d'alimentation précédant la perte d'alimentation secteur. La restauration à l'état d'alimentation précédent est le comportement par défaut. Les facteurs suivants peuvent provoquer une interruption :

- panne de courant
- retrait des câbles d'alimentation des blocs d'alimentation (PSU)
- panne de l'unité d'alimentation (PDU)

Si l'option **Configuration du bilan/de la redondance** > **Désactiver la récupération de l'alimentation secteur** est sélectionnée, le châssis reste hors tension après la récupération en CA.

Dans ce cas, les serveurs lame ne sont pas configurés sur la mise sous tension automatique, il vous faudra peut-être les mettre sous tension manuellement.

Affichage de l'état du bilan de puissance avec l'interface Web CMC

Pour afficher l'état du bilan de puissance avec l'interface Web CMC, dans le volet de gauche accédez à **Présentation du châssis** et cliquez sur **Alimentation** > **État du bilan de puissance**. La page **État du bilan de puissance** affiche la configuration de stratégie d'alimentation du système, le bilan de puissance allouée aux modules serveur et les informations d'alimentation du châssis. Pour plus d'informations, voir l'*Aide en ligne*.

Affichage de l'état du bilan de puissance avec RACADM

Ouvrez une console texte série/Telnet/SSH d'accès à CMC, ouvrez une session et entrez :

```
racadm getpbinfo
```

Pour plus d'informations sur la commande **getpbinfo**, y compris la sortie, voir la section de la commande **getpbinfo** dans le document *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX).

Condition de la redondance et intégrité énergétique globale

L'état de redondance est un facteur qui détermine l'intégrité globale de l'alimentation. Lorsque la stratégie de redondance de l'alimentation est définie, par exemple, à la redondance du réseau d'alimentation et que l'état de redondance indique que le système fonctionne avec redondance, l'intégrité globale de l'alimentation est habituellement **OK**. Si le bloc d'alimentation installé sur un châssis est défaillant pour une raison quelconque, l'état d'intégrité globale de l'alimentation du châssis s'affiche comme **non critique**. Toutefois, si les conditions applicables au fonctionnement avec redondance du réseau d'alimentation ne peuvent pas être respectées, l'état de redondance est **non** et l'intégrité globale de l'alimentation est **critique**. Cela est dû au fait que le système ne parvient pas à fonctionner conformément à la stratégie de redondance configurée.

Le CMC actif interroge l'état d'intégrité du CMC de secours pour déterminer si le châssis est redondant. Lorsque vous déconnectez le câble réseau, un basculement de châssis se déclenche au bout de 30 secondes. Le CMC de secours s'active. En cas d'interruption du réseau, le CMC initialement actif démarre au bout d'environ trois minutes et devient un CMC de secours. La tâche de surveillance de l'intégrité sur le CMC de secours reprend au bout de cinq minutes. Les modifications de l'intégrité, le cas échéant, sur le CMC de secours ne sont traitées qu'une fois que celui-ci est stable. Le CMC actif doit attendre huit minutes et demie pour déterminer si la redondance existe. Assurez-vous que l'état de redondance est intègre avant de lancer un basculement en raison des modifications de l'intégrité.

REMARQUE : Le CMC n'effectue pas une vérification préalable de ces conditions lorsque vous modifiez la stratégie de redondance vers ou depuis la redondance du réseau d'alimentation. Par conséquent, la configuration de la stratégie de redondance peut entraîner immédiatement une perte de redondance ou une condition retrouvée.

Gestion de l'alimentation après une défaillance de bloc d'alimentation

Lorsqu'une événement d'insuffisance de puissance se produit, dans le cas d'une défaillance de bloc d'alimentation, par exemple, le contrôleur CMC réduit l'alimentation électrique vers les serveurs. Ensuite, il réévalue les besoins en puissance du châssis. Si les besoins en puissance ne sont toujours pas satisfaits, le contrôleur CMC met hors tension les serveurs à faible priorité. Cependant, cette opération est effectuée en fonction de chaque stratégie de redondance que vous définissez pour le contrôleur CMC. Un serveur redondant peut tolérer une perte de puissance sans affecter les performances des serveurs.

La puissance des serveurs à priorité élevée est restaurée par paliers, tant que les besoins en puissance restent dans le bilan alloué. Pour définir la stratégie de redondance, voir Configuration du bilan d'alimentation et de la redondance.

Gestion de l'alimentation après le retrait d'un bloc d'alimentation

Le contrôleur CMC peut commencer à économiser l'énergie lorsque vous retirez un bloc d'alimentation ou son câble CA. Il réduit l'alimentation des serveurs à priorité faible jusqu'à ce que l'allocation de puissance soit prise en charge par les blocs d'alimentation restants du châssis. Si vous retirez plusieurs blocs d'alimentation, le contrôleur CMC évalue à nouveau les besoins en puissance lors du retrait du deuxième bloc d'alimentation afin de déterminer la réponse du micrologiciel. Si les besoins en puissance ne sont toujours pas satisfaits, le contrôleur CMC peut mettre hors tension les serveurs à priorité faible.

Limites

- Le contrôleur CMC ne prend pas en charge l'arrêt *automatisé* d'un serveur à priorité inférieure afin de permettre la mise sous tension d'un serveur à priorité supérieure. Ce type d'arrêt peut néanmoins être exécuté à l'initiative d'un utilisateur.
- Les modifications de la stratégie de redondance des blocs d'alimentation sont limitées par le nombre de blocs d'alimentation du châssis. Vous pouvez sélectionner n'importe lequel des deux paramètres de configuration de redondance des blocs d'alimentation figurant dans la zone Configuration de redondance par défaut.

Règle d'engagement d'un nouveau serveur

Si un nouveau serveur sous tension dépasse la puissance disponible pour le châssis, le CMC peut réduire la puissance des serveurs de priorité inférieure. Cela peut se produire si l'administrateur a configuré pour le châssis une limite de puissance inférieure à la puissance nécessaire pour permettre une allocation de puissance totale aux serveurs, ou si la puissance disponible est insuffisante pour couvrir les besoins d'alimentation plus élevés de tous les serveurs du châssis. Si l'alimentation libérée en réduisant l'alimentation allouée aux serveurs de priorité inférieure est insuffisante, le nouveau serveur ne peut pas être alimenté.

Cette situation existe si l'administrateur a défini une limite de puissance pour le châssis, qui est inférieure à l'allocation de puissance totale des serveurs ou qu'une puissance insuffisante est disponible pour les serveurs nécessitant plus de puissance.

Le tableau suivant indique les actions qu'exécute le contrôleur CMC lorsqu'un nouveau serveur est mis sous tension selon le scénario décrit plus haut.

Tableau 38. Réponse de CMC lors de la tentative d'allumage d'un serveur

L'alimentation du cas le plus défavorable est disponible	Prise en charge par CMC	Allumage du serveur
Oui	La préservation de l'alimentation n'est pas nécessaire	Autorisé
Non	Passage en mode d'économie d'énergie : • L'alimentation nécessaire au nouveau serveur est disponible • L'alimentation nécessaire au nouveau serveur n'est pas disponible.	Autorisé Non autorisé

Si un bloc d'alimentation ne fonctionne plus, le système passe à l'état d'erreur d'intégrité non critique et un événement d'échec de bloc d'alimentation est généré. Le retrait d'un bloc d'alimentation provoque un événement de retrait de bloc.

Si l'un ou l'autre des événements provoque une perte de redondance, selon les allocations d'alimentation, un événement de *perte de redondance* est généré.

Si la capacité de puissance ultérieure ou la capacité de puissance de l'utilisateur est supérieure à celle des allocations de serveur, les serveurs risquent d'afficher une dégradation de performances, voire, dans le pire des cas, d'être désactivés. Les deux conditions suivent l'ordre inverse des priorités. Autrement dit, les serveurs de faible priorité sont mis hors tension en premier.

Le tableau suivant répertoire la réponse du firmware en cas de mise hors tension ou du retrait d'un bloc d'alimentation dans le cadre de différentes configurations de redondance de blocs d'alimentation.

Tableau 39. Impact de l'échec ou du retrait d'un bloc d'alimentation sur le châssis

Configuration des blocs d'alimentation	Engagement dynamique des blocs d'alimentation	Prise en charge par le firmware
Redondance de réseau d'alimentation	Désactivé	Le contrôleur CMC signale la perte de la redondance de réseau d'alimentation.
Redondance des blocs d'alimentation	Désactivé	Le contrôleur CMC signale la perte de la redondance de l'alimentation électrique.
Redondance de réseau d'alimentation	Activé	Le contrôleur CMC signale la perte de la redondance de réseau d'alimentation. Les blocs d'alimentation en mode veille (s'il y en a) sont allumés pour compenser la perte de bilan d'alimentation due à l'échec ou au retrait d'un bloc d'alimentation.
Redondance des blocs d'alimentation	Activé	CMC vous avertit de la perte de la redondance des blocs d'alimentation (PSU). Les PSU en mode veille (s'il y en a) sont allumés pour compenser la perte de bilan d'alimentation dû à l'échec ou au retrait d'un PSU.

Modifications d'alimentation et de la règle de redondance dans le journal des événements système

Les changements d'état des blocs d'alimentation et de stratégie de redondance de l'alimentation sont enregistrés en tant qu'événements. Les événements liés à l'alimentation qui journalisent des entrées dans le journal des événements système (SEL) sont l'insertion et le retrait d'un bloc d'alimentation, l'insertion et le retrait d'une entrée d'alimentation, et la confirmation ou la déconfirmation de la sortie d'alimentation.

Le tableau suivant répertorie les entrées de journal SEL liées aux modifications des blocs d'alimentation :

Tableau 40. Événements du journal SEL relatifs aux modifications des blocs d'alimentation

Événement d'alimentation	Entrée du journal des événements système (SEL)
Insertion	Alimentation électrique présente.
Retrait	Alimentation absente.
Alimentation alternative reçue	L'entrée de l'alimentation a été restaurée.
perte de l'alimentation alternative	L'entrée de l'alimentation est perdue
sortie CC produite	L'alimentation électrique fonctionne correctement.
Perte de sortie en CC	Défaillance de l'alimentation électrique.

Les événements liés aux changements de l'état de redondance de l'alimentation qui enregistrent des entrées dans le journal SEL sont la perte de redondance et le rétablissement de la redondance pour un boîtier modulaire configuré avec la stratégie d'alimentation **Redondance de réseau d'alimentation** ou **Redondance des blocs d'alimentation**. Le tableau suivant répertorie les entrées SEL liées aux modifications de la condition de la redondance d'alimentation.

Tableau 41. Événements du journal SEL relatifs aux modifications de la condition de la redondance d'alimentation

Événement de stratégie d'alimentation	Entrée du journal des événements système (SEL)
Perte de la redondance	Power supply redundancy is lost. (Perte de la redondance du bloc d'alimentation.)

Tableau 41. Événements du journal SEL relatifs aux modifications de la condition de la redondance d'alimentation (suite)

Événement de stratégie d'alimentation	Entrée du journal des événements système (SEL)
Regain de la redondance	The power supplies are not redundant. (Les blocs d'alimentation ne sont pas redondants.)

Configuration du bilan d'alimentation et de la redondance

Vous pouvez configurer le bilan d'alimentation, la redondance et l'alimentation dynamique de l'ensemble du châssis (châssis, serveurs, module d'E/S, KVM, CMC et blocs d'alimentation) qui utilise quatre blocs d'alimentation. Le service de gestion de l'alimentation optimise la consommation d'électricité et réalloue l'alimentation aux différents modules en fonction des besoins.

Vous pouvez configurer les paramètres suivants :

- Limite de la puissance d'entrée système
- Règle de redondance
- Activer l'enclenchement dynamique des blocs d'alimentation
- Désactiver le bouton d'alimentation du châssis
- Mode d'économie d'énergie maximum
- Journalisation distante de l'alimentation
- Intervalle de journalisation distante de l'alimentation
- Gestion de l'alimentation basée sur le serveur
- Désactiver la récupération de l'alimentation secteur

Économie d'énergie et bilan de puissance

Le contrôleur CMC réalise des économies d'énergie lorsque le système atteint la limite de puissance maximale définie par l'utilisateur. Lorsque la demande de puissance dépasse la valeur limite de la puissance d'entrée système définie par l'utilisateur, le contrôleur CMC réduit l'alimentation des serveurs dans l'ordre inverse des priorités pour libérer de la puissance pour les serveurs et autres modules à priorité élevée installés dans le châssis.

Si tous ou plusieurs logements du châssis sont configurés avec le même niveau de priorité, le contrôleur CMC réduit l'alimentation des serveurs dans l'ordre croissant des numéros de logement. Par exemple, si les serveurs des logements 1 et 2 ont le même niveau de priorité, l'alimentation du serveur du logement 1 est réduite avant celle du serveur du logement 2.

REMARQUE : Vous pouvez attribuer un niveau de priorité à chaque serveur du châssis, en associant les numéros 1 à 9 à chaque serveur. Le niveau de priorité par défaut pour tous les serveurs est 1. Plus le numéro est faible, plus le niveau de priorité est élevé.

Le bilan de puissance est limité à un maximum égal à la puissance de l'ensemble de deux blocs d'alimentation le plus faible. Si vous tentez de définir une valeur de bilan de puissance CA dépassant la valeur de *limite de puissance d'entrée système*, le contrôleur CMC affiche un message d'erreur. Le bilan de puissance est limité à 4 800 watts.

Mode de conservation de puissance maximale

Ceci est activé pour la redondance de réseau d'alimentation ou les modes de redondance des PSU. CMC assure la conservation de la puissance maximale lorsque :

- Le mode de conservation de puissance maximale est activé.
- Un script de ligne de commande automatisé, émis par un onduleur, sélectionne le mode de conservation maximale.

En mode de conservation de puissance maximale, tous les serveurs commencent à fonctionner avec leur niveau de puissance minimal et toute demande d'allocation supplémentaire de puissance aux serveurs est refusée. Dans ce mode, les performances des serveurs allumés peuvent être dégradées. Il est impossible d'allumer des serveurs supplémentaires, quelle que soit leur priorité.

Le système revient à ses performances optimales lorsque vous désactivez le mode de conservation de puissance maximale.

REMARQUE : Si le mode Conservation maximale de puissance (MPCM) est activé sur le châssis, toutes les demandes d'alimentation à partir d'un serveur lame sont refusées. Le serveur lame serveur n'est pas sous tension s'il n'y a une action dans le iDRAC ou sur un serveur lame exigeant que l'hôte démarre le cycle d'alimentation.

Réduction de l'alimentation des serveurs afin de préserver le bilan d'alimentation

Le contrôleur CMC réduit l'allocation de puissance des serveurs à priorité basse lorsqu'une plus grande puissance est nécessaire pour maintenir la consommation électrique du système sous la *limite de puissance d'entrée du système* définie par l'utilisateur. Par exemple, lors de la mise en place d'un nouveau serveur, le contrôleur CMC peut réduire l'alimentation des serveurs à priorité basse pour en attribuer davantage au nouveau serveur. Si la puissance d'alimentation reste insuffisante après réduction de l'allocation de puissance des serveurs à priorité basse, le contrôleur CMC réduit les performances des serveurs jusqu'à libération de suffisamment de puissance pour alimenter le nouveau serveur.

CMC réduit l'allocation d'alimentation des serveurs dans deux cas :

- La consommation électrique globale dépasse la *limite de puissance d'entrée système* configurable.
- Une panne d'alimentation survient dans le cadre d'une configuration non redondante

Fonctionnement de l'alimentation CA des blocs d'alimentation (PSU) 110 V

Par défaut, la fonction CA de bloc d'alimentation 110 V est disponible. Cependant, vous ne pouvez pas utiliser le mode 110 V et 220 V simultanément. Si le contrôleur CMC détecte que les deux tensions sont utilisées, une valeur de tension est sélectionnée et les blocs d'alimentation connectés utilisant l'autre tension d'alimentation sont mis hors tension et le système indique qu'ils ne fonctionnent pas.

Journalisation à distance

Vous pouvez générer un rapport de la consommation électrique sur un serveur syslog distant. Il est possible de journaliser la consommation électrique totale du châssis, ainsi que les consommations minimale, maximale et moyenne sur une période donnée. Pour plus d'informations sur l'activation de cette fonction et sur la configuration de la fréquence de la collecte/journalisation, voir Gestion et surveillance de l'alimentation.

Gestion d'alimentation externe

La gestion de l'alimentation CMC est contrôlée éventuellement par OpenManage Power Center (OMPC). Pour plus d'informations, voir le *Guide d'utilisation d'OMPC*.

Lorsque la gestion d'alimentation externe est activée, OMPC gère les éléments suivants :

- Alimentation des serveurs VRTX pris en charge
- Priorité des serveurs VRTX pris en charge
- Capacité maximale de l'alimentation d'entrée du système
- Mode de conservation de puissance maximale

Le CMC continue à maintenir et à gérer :

- Règle de redondance
- Journalisation distante de l'alimentation
- Performance du serveur contre redondance de l'alimentation
- Enclenchement dynamique des blocs l'alimentation

OPMC gère ensuite les niveaux de priorité et l'alimentation des nœuds de serveurs VRTX du châssis à partir du bilan de puissance disponible après l'allocation de puissance à l'infrastructure de châssis et les nœuds de serveur des générations précédentes. La journalisation de l'alimentation à distance n'est pas affectée par la gestion d'alimentation externe.

Après l'activation du mode de gestion de l'alimentation basée sur le serveur, le châssis est préparé pour la gestion PM3. Toutes les priorités de serveurs VRTX12 sont fixées sur 1 (Élevé). PM3 gère directement l'alimentation et le niveau de priorité des serveurs. Comme PM3 contrôle l'allocation de puissance des serveurs compatibles, le contrôleur CMC ne contrôle plus le mode de conservation de puissance maximale. Par conséquent, cette option est désactivée.

Lorsque vous activez le mode **Conservation de puissance maximale**, le contrôleur CMC définit la capacité de puissance d'entrée maximale du système que le châssis peut gérer. Il interdit tout dépassement de la capacité de puissance maximale. Toutefois, PM3 gère toutes les autres limitations de capacité de puissance.

Lorsque la gestion de l'alimentation PM3 est désactivée, le CMC revient à l'état des paramètres de priorité du serveur avant l'activation de la gestion externe.

REMARQUE : Si vous désactivez la gestion PM3, le CMC ne revient pas au paramètre de puissance de châssis maximale précédent. Ouvrez le journal CMC pour connaître le paramètre précédent et restaurer manuellement cette valeur.

Configuration du bilan de puissance et de la redondance avec l'interface Web CMC

REMARQUE : Vous devez disposer du privilège Administrateur de configuration du châssis pour pouvoir exécuter les tâches de gestion de l'alimentation.

Pour configurer le bilan de puissance :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Alimentation** > **Configuration**.
2. Dans la page **Configuration du bilan/de la redondance**, sélectionnez certaines ou toutes les propriétés suivantes en fonction des besoins. Pour plus d'informations sur les champs, voir l'*aide en ligne*.
   - **Activer la gestion de l'alimentation basée sur le serveur**
   - **Limite de la puissance d'entrée système**
   - **Règle de redondance**
   - **Activer l'enclenchement dynamique des blocs d'alimentation**
   - **Désactiver le bouton d'alimentation du châssis**
   - **Mode d'économie d'énergie maximum**
   - **Activation de la journalisation de l'alimentation à distance**
   - **Intervalle de journalisation distante de l'alimentation**
3. Cliquez sur **Appliquer** pour enregistrer les modifications.

Configuration du bilan de puissance et de la redondance à l'aide de RACADM

REMARQUE : Vous devez disposer du privilège d'administration de configuration du châssis pour pouvoir exécuter les tâches de gestion de l'alimentation.

Pour activer la redondance et définir la règle de redondance :

1. Ouvrez une console série/Telnet/SSH d'accès à CMC, puis ouvrez une session.
2. Définissez les propriétés selon vos besoins :
   - Pour sélectionner une règle de redondance, entrez la commande :

     ```
     racadm config -g cfgChassisPower -o
     cfgChassisRedundancyPolicy <value>
     ```

     où <*value*> correspond à 1 (Redondance de réseau d'alimentation) et 2 (Redondance des blocs d'alimentation). La valeur par défaut est 2.

     Par exemple, la commande suivante définit la stratégie de redondance sur 1 :

     ```
     racadm config -g cfgChassisPower -o
     cfgChassisRedundancyPolicy 1
     ```

   - Pour définir la valeur de bilan de puissance, entrez :

     ```
     racadm config -g cfgChassisPower -o
     cfgChassisPowerCap <value>
     ```

où <*value*> est un nombre compris entre 938 W et 4 800 W, qui représente la limite d'alimentation maximale en watts. La valeur par défaut est 4800.

Par exemple, la commande suivante définit 4 800 watts comme bilan de puissance maximal :

```
racadm config -g cfgChassisPower -o
cfgChassisPowerCap 4800
```

- Pour activer ou désactiver l'engagement dynamique des unités d'alimentation, entrez la commande :

```
racadm config -g cfgChassisPower -o
cfgChassisDynamicPSUEngagementEnable <value>
```

où <*valeur*> est 0 (désactiver), 1 (activer). La valeur par défaut est 0.

Par exemple, la commande suivante désactive l'engagement dynamique des blocs d'alimentation (PSU) :

```
racadm config -g cfgChassisPower -o
cfgChassisDynamicPSUEngagementEnable 0
```

- Pour activer le mode de consommation électrique maximale, entrez :

```
racadm config -g cfgChassisPower -o
cfgChassisMaxPowerConservationMode 1
```

- Pour rétablir le fonctionnement normal, entrez :

```
racadm config -g cfgChassisPower -o
cfgChassisMaxPowerConservationMode 0
```

- Pour activer la fonctionnalité de journalisation de l'alimentation distante, entrez la commande suivante :

```
racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogPowerLoggingEnabled 1
```

- Pour spécifier l'intervalle de journalisation de votre choix, entrez la commande suivante :

```
racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogPowerLoggingInterval n
```

où *n* correspond à 1 à 1 440 minutes.

- Pour déterminer si la fonction de journalisation de l'alimentation distante est activée, entrez la commande suivante :

```
racadm getconfig -g cfgRemoteHosts -o
cfgRhostsSyslogPowerLoggingEnabled
```

- Pour déterminer l'intervalle de journalisation à distance de l'alimentation, entrez la commande suivante :

```
racadm getconfig -g cfgRemoteHosts -o
cfgRhostsSyslogPowerLoggingInterval
```

La fonction de journalisation à distance de l'alimentation dépend des hôtes syslog distants qui ont été précédemment configurés. La connexion à un ou plusieurs hôtes syslog distants doit être activée ; dans le cas contraire, la consommation électrique est consignée dans le journal. Pour cela, vous pouvez utiliser l'interface Web ou l'interface de ligne de commande (CLI) RACADM. Pour plus d'informations, reportez-vous aux instructions de configuration des hôtes syslog distants.

- Pour activer la gestion de l'alimentation distante par OPMC (Open Manage Power Center), entrez :

```
racadm config -g cfgChassisPower -o
cfgChassisServerBasedPowerMgmtMode 1
```

- Pour restaurer la gestion de l'alimentation CMC, entrez :

```
racadm config -g cfgChassisPower -o
cfgChassisServerBasedPowerMgmtMode 0
```

Pour plus d'informations sur les commandes RACADM relatives à l'alimentation du châssis, voir les sections **config**, **getconfig**, **getpbinfo** et **cfgChassisPower** dans le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX*.

Exécution d'opérations de contrôle de l'alimentation

Vous pouvez exécuter l'opération de contrôle de l'alimentation suivante pour le châssis, les serveurs et l'IOM.

REMARQUE : Les opérations de contrôle de l'alimentation affectent l'intégralité du châssis.

Exécution d'opérations de contrôle de l'alimentation sur le châssis

Le contrôleur CMC permet d'exécuter à distance plusieurs opérations de gestion de l'alimentation, telles qu'une séquence d'arrêt propre dans l'ensemble du châssis (châssis, serveurs, module IOM, KVM et blocs d'alimentation).

REMARQUE : Vous devez disposer du privilège d'Administrateur de configuration du châssis pour exécuter les tâches de gestion de l'alimentation.

Exécution d'opérations de contrôle de l'alimentation sur le châssis avec l'interface Web

Pour exécuter des opérations de contrôle de l'alimentation sur le châssis en utilisant l'interface Web CMC :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Alimentation** > **Contrôle**.
   La page **Contrôle de l'alimentation du châssis** s'affiche.
2. Sélectionnez l'une des opérations de contrôle de l'alimentation suivantes.
   Pour plus d'informations sur chaque option, voir l'*Aide en ligne*.
   - **Mettre le système sous tension**
   - **Arrêter le système**
   - **Exécuter un cycle d'alimentation du système (démarrage à froid)**
   - **Réinitialiser CMC (amorçage à chaud)**
   - **Arrêt anormal**
3. Cliquez sur **Appliquer**.
   Une boîte de dialogue demande de confirmer.
4. Cliquez sur **OK** pour lancer la tâche de gestion de l'alimentation (réinitialisation du système, par exemple).

Exécution d'opérations de contrôle de l'alimentation sur le châssis avec RACADM

Ouvrez une console texte série/Telnet/SSH d'accès à CMC, ouvrez une session et entrez :

```
racadm chassisaction -m chassis <action>
```

où <*action*> a la valeur powerup, powerdown, powercycle, nongraceshutdown ou reset.

Exécution d'opérations de contrôle de l'alimentation sur un serveur

Vous pouvez exécuter à distance des opérations de gestion de l'alimentation pour plusieurs serveurs simultanément ou pour un seul serveur d'un châssis.

REMARQUE : Les serveurs lames modulaires sont dans un état ralenti au cours du redémarrage ou du basculement du CMC.

REMARQUE : Vous devez disposer du privilège Administrateur de configuration du châssis pour pouvoir exécuter les tâches de gestion de l'alimentation.

Exécution d'opérations de contrôle de l'alimentation sur plusieurs serveurs avec l'interface Web CMC

Pour exécuter des opérations de contrôle de l'alimentation pour plusieurs serveurs avec l'interface Web :

1. Dans le volet de gauche, cliquez sur **Présentation du serveur** > **Alimentation**.
   La page **Contrôle de l'alimentation** s'affiche.
2. Dans la colonne **Opérations**, sélectionnez, dans le menu déroulant, l'une des opérations suivantes de contrôle de l'alimentation pour les serveurs appropriés :
   - **Aucune opération**
   - **Mettre le serveur sous tension**
   - **Mettre le serveur hors tension**
   - **Arrêt normal**
   - **Réinitialiser le serveur (redémarrage à chaud)**
   - **Exécuter un cycle d'alimentation sur le serveur (redémarrage à froid)**

   Pour plus d'informations sur les options, voir l'*Aide en ligne*.
3. Cliquez sur **Appliquer**.
   Une boîte de dialogue demande de confirmer l'opération.
4. Cliquez sur **OK** pour exécuter l'action de gestion de l'alimentation (par exemple, réinitialiser le serveur).

Exécution d'opérations de contrôle de l'alimentation sur le module IOM

Vous pouvez réinitialiser ou mettre sous tension un module IOM.

REMARQUE : Vous devez disposer du privilège Administrateur de configuration du châssis pour pouvoir exécuter les tâches de gestion de l'alimentation.

Exécution d'opérations de contrôle de l'alimentation sur le module IOM à l'aide de l'interface Web CMC

Pour exécuter des opérations de contrôle de l'alimentation sur le module d'E/S :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Présentation du module d'E/S** > **Alimentation**.
2. Sur la page **Contrôle de l'alimentation**, pour le module IOM, dans le menu déroulant, sélectionnez l'opération à exécuter (cycle d'alimentation).
3. Cliquez sur **Appliquer**.

Exécution d'opérations de contrôle de l'alimentation sur le module IOM à l'aide de RACADM

Pour exécuter des opérations de contrôle de l'alimentation sur le module IOM à l'aide de RACADM, ouvrez une console texte série/Telnet/SSH sur le contrôleur CMC, connectez-vous et entrez :

```
racadm chassisaction -m switch-<n><action>
```

, où <*action*> indique l'opération à exécuter : cycle d'alimentation.

15

Gestion du stockage du châssis

Sur le Dell PowerEdge VRTX, vous pouvez exécuter les opérations suivantes :

- Afficher l'état des disques durs physiques et des contrôleurs de stockage
- Afficher les propriétés des contrôleurs, des disques durs physiques, des disques virtuels et des boîtiers
- Configurer les contrôleurs, les disques durs physiques et les disques virtuels
- Affecter des adaptateurs virtuels
- Dépanner le contrôleur, les disques durs physiques et les disques virtuels
- Mettre à jour les composants de stockage
- Utilisez les contrôleurs de stockage partagé en mode de tolérance des pannes
- Activation ou désactivation de PERC8 partagé (intégré 2)

REMARQUE : L'initialisation rapide ou complète n'apparaît pas lorsque les disques virtuels sont initialement créés.

Sujets :

Affichage de la condition des composants de stockage

Pour afficher la condition des composants de stockage :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Stockage** > **Propriétés** > **Présentation du stockage**.
2. Sur la page **Présentation du stockage**, vous pouvez :
   - Afficher le résumé graphique des disques physiques installés dans le châssis et leur état.
   - Afficher le résumé de tous les composants de stockage avec des liens vers leurs pages respectives.
   - Afficher la capacité utilisée et la capacité totale du stockage.
   - Afficher les informations de contrôleur

     REMARQUE : Dans le cas d'un contrôleur tolérant les pannes, le format de nom est : Shared <*PERC numéro*> (Integrated <numéro>). Par exemple, le contrôleur actif est Shared PERC8 (Integrated 1) et le contrôleur homologue est Shared PERC8 (Integrated 2).

     REMARQUE : Si le second PERC est désactivé, le nom s'affiche sous la forme PERC désactivé (intégré 2).
   - Afficher les événements de stockage récemment journalisés

REMARQUE : Reportez-vous à *l'Aide en ligne* pour plus d'informations.

Affichage de la topologie de stockage

Pour afficher la topologie de stockage :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Stockage** > **Propriétés** > **Topologie**.
2. Dans la page **Topologie**, cliquez sur **<nom du contrôleur>** pour afficher les pages correspondantes.

   REMARQUE : Vous pouvez afficher le nom du contrôleur actif en contrôlant les périphériques de stockage associés à ce CMC et également le contrôleur passif agissant en tant que contrôleur de secours.
3. Sous chacun des contrôleurs installés, cliquez sur les liens **Afficher les disques virtuels <nom d'enceinte>** et **Afficher les disques physiques** pour ouvrir les pages correspondantes.

Affichage des informations de dépannage de tolérance des pannes de SPERC à l'aide de l'interface Web CMC

Pour afficher les attributs qui indiquent le bon fonctionnement de la fonctionnalité de tolérance des pannes d'un SPERC.

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Stockage** > **Dépannage** > **Configuration du dépannage**. La page **Dépannage de la configuration du stockage** s'affiche.
2. Sur la page **Dépannage de la configuration du stockage** , vous pouvez :
   - Cliquez sur + pour afficher les attributs suivants lorsque le contrôleur intégré est en mode de tolérance de panne :
     - Deux PERC partagés détectés.
     - Deux modules d'extension détectés
     - PERC partagés et modules d'extension correctement câblés
     - Micrologiciel correct sur les PERC partagés
     - Micrologiciel correct sur les modules d'extension
     - Micrologiciel correct sur l'infrastructure du châssis
     - Les PERC partagés ont les mêmes paramètres : indique si les SPERC ont les mêmes paramètres.
   - Cliquez sur + pour afficher les attributs suivants lorsque le contrôleur intégré n'est pas en mode de tolérance de panne :
     - Un PERC partagé détecté

- Un module d'extension détecté
- PERC partagés et modules d'extension correctement câblés

- Cliquez sur + pour afficher les attributs suivants lorsque le contrôleur externe est en mode de tolérance de panne :
  - Deux Shared PERC détectés
  - Les Shared PERC sont installés sur des structures distinctes
  - Les Shared PERC et les EMM sont correctement connectés
  - Micrologiciel correct sur les Shared PERC
  - Les Shared PERC ont les mêmes paramètres
- Cliquez sur + pour afficher les attributs suivants lorsque le contrôleur externe n'est pas en mode de tolérance de panne :
  - Un PERC partagé détecté
  - Un module d'extension détecté
  - PERC partagés et modules d'extension correctement câblés
- Afficher l'état de chaque attribut qui indique si les critères de tolérance des pannes sont respectés.

  REMARQUE : Si l'attribut dans un environnement tolérant des pannes ne correspond pas au critère, l'option Mettre à jour maintenant s'affiche pour cet attribut.

REMARQUE : Une option Savoir comment s'affiche par rapport à certaines des attributs. Pour plus d'informations concernant l'attribut, cliquez sur Savoir comment.

3. Pour répondre à un critère pour un attribut, cliquez sur **Mettre à jour maintenant**.
   La page **Mise à jour des composants de stockage** s'affiche, ce qui vous permet de mettre à jour le composant de stockage requis pour respecter le critère de l'attribut.

Affectation d'adaptateurs virtuels à des logements à l'aide de l'interface Web CMC

La fonction d'adaptateur virtuel vous permet de partager le stockage installé avec les quatre serveurs. Pour adresser un disque virtuel à un logement de serveur, vous pouvez commencer par adresser un disque virtuel à un adaptateur virtuel (VA), puis adresser un adaptateur virtuel à un logement de serveur.

- Avant d'affecter un VA à un logement de serveur, vérifiez que :
  - Le logement du serveur est vide ou que le serveur dans le logement est hors tension.
  - Le VA est désadressé d'un serveur ou d'un logement.
  - Tous les serveurs affectés sont mis hors tension.
- Des disques virtuels sont créés et attribués en tant qu'**Adaptateur virtuel 1**, **Adaptateur virtuel 2**, **Adaptateur virtuel 3** ou **Adaptateur virtuel 4**. Pour plus d'informations, reportez-vous à la section Application d'une stratégie d'accès d'adaptateur virtuel à des disques virtuels.

REMARQUE :

- **Vous pouvez adresser uniquement un adaptateur virtuel à un serveur à la fois.**
- **Sans licence appropriée, vous pouvez uniquement supprimer l'adressage d'un serveur-VA, ou adresser le VA au serveur par défaut.**
- **L'adressage par défaut est VA1-Logement de serveur 1, VA2 Logement de serveur 2, VA3-Logement de serveur 3 et VA4 - Logement de serveur 4.**
- **Si un serveur de hauteur standard est inséré, le VA est adressé au logement supérieur. Le logement inférieur, quant à lui, est indiqué comme non adressé. Par exemple, pour un serveur de hauteur standard dans le logement 1, le VA1 est attribué au logement 1 et le VA3 n'est toujours pas adressé.**
- **Si le système dispose d'une licence Enterprise, vous pouvez attribuer l'un des quatre VA à un logement de serveur. Vous ne pouvez cependant adresser qu'un adaptateur virtuel à un seul serveur à la fois.**
- **Les règles de l'adaptateur virtuel sont appliquées aux cartes de stockage partagé externe et intégré.**

Pour adresser un adaptateur virtuel à un logement de serveur ou l'en désadresser :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Stockage** > **Configurer** > **Virtualisation**.
   La page **Virtualisation du stockage** s'affiche.

2. Pour sélectionner le type d'affectation requis, dans le tableau **Mode d'attribution : disques virtuels à adaptateurs virtuels** , sélectionnez :
   - **Attribution simple** : permet d'attribuer un disque virtuel à un adaptateur virtuel.
   - **Attribution multiple** : sélectionnez cette option pour attribuer un disque virtuel à plusieurs adaptateurs virtuels. Lisez les instructions à l'écran avant de sélectionner cette option.

   REMARQUE : Sélectionnez le mode Attribution multiple uniquement si les services de cluster sont installés sur les serveurs. L'utilisation de ce mode sans les services de cluster peut entraîner une corruption ou une perte de données.

   REMARQUE : Vous pouvez attribuer un disque virtuel à plusieurs adaptateurs virtuels depuis la CLI du CMC, même lorsque le Mode d'attribution est défini sur Attribution unique dans l'interface Web du CMC.

3. Dans le tableau **Adaptateurs virtuels adressés**, à partir du menu déroulant **Action**, sélectionnez l'une des options suivantes, puis cliquez sur **Appliquer**.
   - **<# logement>** : sélectionnez l'emplacement auquel le VA doit être attribué.
   - **Désadresser** : sélectionnez cette option pour supprimer l'affectation de VA à un logement.

   Le VA est adressé ou non adressé depuis le logement de serveur sélectionné, en fonction de l'action sélectionnée.

   REMARQUE : Prenons par exemple un VA attribué au serveur dans le logement inférieur (3 ou 4). Lorsqu'un serveur demi-hauteur (logement 3 ou 4) est remplacé par un serveur de hauteur standard, ce dernier ne peut pas accéder au VA attribué aux logements inférieurs. Une réinsertion du serveur demi-hauteur permet d'accéder au VA.

   Adresser ou supprimer l'adressage d'un contrôleur virtuel PERC au serveur lame :
   - Chaque carte Shared PERC 8 externe dispose de quatre adaptateurs virtuels (VA). Si une ou deux cartes Shared PERC 8 externes sont présentes dans le système, vous pouvez adresser ou supprimer l'adressage de l'un des quatre adaptateurs virtuels en mode partagé.
   - Si un logement PCIE externe est occupé par un adaptateur partagé, l'adressage de l'adaptateur virtuel peut obtenir les détails ou informations actuelles pour l'adressage du VA du pool VA du stockage partagé.
   - Le périphérique partagé n'est pas pris en charge lorsque le logement PCIE externe est occupé par un adaptateur partagé. L'adaptateur partagé permet la prise en charge d'un périphérique partagé en modifiant le pool de VA du stockage partagé.

Tolérance des pannes dans les contrôleurs de stockage

L'option de stockage Haute disponibilité (HA) permet la disponibilité de plusieurs composants intégrés et plusieurs points d'accès aux ressources de stockage. Dans le cas où un composant de stockage arrête de fonctionner, le serveur est pris en charge par un deuxième composant stratégique ou chemin d'accès aux données disponibles. La Haute disponibilité réduit le temps d'inactivité en restaurant les services en coulisse, dans la plupart des cas, avant que le non fonctionnement soit visible, mais ne permet pas d'éliminer les temps d'inactivité. La tolérance de panne (FT) permet d'utiliser des composants redondants au sein d'un système de stockage, qui sont configurés pour se comporter comme des composants de sauvegarde et restent en mode de secours. Les contrôleurs de stockage en mode de tolérance de panne préviennent toute interruption des services de stockage et prennent automatiquement la relève des services d'un composant qui a cessé de fonctionner. Les performances restent cohérentes tout au long de ce processus de basculement car les composant redondants (contrôleurs) ne sont pas utilisés dans des conditions de fonctionnement ordinaires.

La Haute disponibilité avec tolérance des pannes offre les avantages suivants :

- Fournit une disponibilité de toutes les applications de stockage même si un contrôleur ne fonctionne plus.
- Fournit l'accès aux fonctions essentielles du châssis à tout moment.
- Permet au serveur de gérer les situations lorsque le contrôleur arrête de fonctionner ou qu'il est défectueux.
- Utilise la redondance des composants

À l'aide de la fonction de tolérance des pannes, vous pouvez gérer les taches associées au stockage partagé effectuées grâce à un contrôleur actif et passif (homologue). Le contrôleur actif est le contrôleur qui est actif et surveille tous les processus liés au stockage. L'état de fonctionnement des deux contrôleurs est communiqué entre ces derniers, de sorte que lorsqu'un contrôleur actif cesse de fonctionner, le contrôleur passif agissant comme un homologue de secours prend le relais, sans aucune interruption.

REMARQUE : Le CMC affiche les données de tolérance des pannes des Shared PERC 8 avec micrologiciel SR-IOV activé. Si une carte non SR-IOV est connectée aux logements de stockage partagé, la carte ne se met pas sous tension et une alerte est générée.

REMARQUE : Les opérations qui réinitialisent la configuration du CMC telles que la réinitialisation du CMC, réinitialisent la configuration de tolérance aux pannes externe. Par conséquent, le mode PERC passe en « Mode sans échec ». Désactivez la tolérance aux pannes dans le PERC externe.

Non-correspondance de clé de sécurité

Vous pouvez créer une clé de sécurité sur un contrôleur à l'aide d'une **ID de clé de chiffrement** et d'une **Phrase de passe**. Le contrôleur compare uniquement la **Phrase de passe** utilisée lors de la création de la clé de sécurité pour identifier si les deux contrôleurs ont les mêmes clés de sécurité. Par conséquent, deux contrôleurs rejoignant un cluster disposent de la tolérance des pannes même si leurs **ID de clé de chiffrement** sont différentes, tant qu'ils ont la même phrase de passe.

Si une non-correspondance de clés de sécurité est détectée entre deux contrôleurs homologues, le mode de tolérance des pannes devient « Dégradé ». Une alerte critique est affichée sur la page **Intégrité du châssis** et la surveillance peut ne pas afficher une bonne association des lecteurs.

Si une non-correspondance des clés de sécurité est détectée, résolvez la non-correspondance des clés en créant, modifiant ou supprimant la clé de sécurité d'un des contrôleurs avant d'effectuer toute autre opération de sécurité du stockage sur le contrôleur. Éteignez et rallumez le châssis après avoir résolu la non-correspondance. Avant de combiner deux contrôleurs n'étant pas à haute disponibilité, modifiez les clés afin qu'elles se correspondent. Cette action facilite l'importation de lecteurs sécurisés associés à chaque contrôleur rejoignant le cluster.

Pour les contrôleurs externes, modifiez leurs clés afin qu'elles se correspondent avant de les câbler à des fins de tolérance aux pannes. La modification des clés de sécurité facilite l'importation de lecteurs sécurisés associés à chaque contrôleur rejoignant le cluster.

Résolution de la non-correspondance des clés de sécurité à l'aide de l'interface Web CMC

Pour résoudre la non-correspondance des clés de sécurité à l'aide de l'interface Web CMC :

1. Mettez tous les modules serveur hors tension.
2. Cliquez sur **Présentation du serveur** > **Alimentation** > **Contrôle** > **Mise hors tension du serveur**.
3. Modifiez la clé de sécurité sur l'un ou les deux contrôleurs non tolérants aux pannes existants de sorte que les clés correspondent.
4. Éteignez et rallumez le châssis.
5. Vérifiez si les clés des contrôleurs correspondent.

Affichage des propriétés des contrôleurs à l'aide de l'interface Web CMC

Pour afficher les propriétés générales des contrôleurs :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Contrôleur.**
2. Dans la page **Contrôleurs**, dans la section **Contrôleurs**, figurent les propriétés du contrôleur. Pour afficher les propriétés avancées, cliquez sur l'  .

   REMARQUE : Si les contrôleurs sont en mode de tolérance des pannes, les informations suivantes concernant l'état et le mode de la tolérance des pannes sont également affichées :

   - **Mode de tolérance des pannes : Partagé, Actif/Passif**
   - **État de la tolérance des pannes : Intègre/Normal, ou Perdu/Dégradé**
   - **Contrôleur homologue : indique le nom du contrôleur qui fait office d'homologue (secours) lorsque le mode de tolérance de panne est pris en charge par deux contrôleurs.**

   REMARQUE : Si le contrôleur homologue est désactivé, le nom s'affiche comme PERC désactivé (Intégré 2) ou PERC désactivé (Logement SPERC 6) et l'état s'affiche comme Inconnu, ce qui signifie que le contrôleur homologue est hors tension.

   Pour en savoir plus sur les contrôleurs, voir l'*Aide en ligne*.

Affichage des propriétés de contrôleur à l'aide de RACADM

Pour afficher les propriétés de contrôleur en utilisant RACADM, exécutez la commande `racadm raid get controllers -o`

Pour plus d'informations, voir le document *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX).

Importer ou effacer une configuration étrangère

Un disque externe doit être inséré dans le châssis.

Pour importer ou effacer la configuration étrangère :

1. Dans le volet de gauche, cliquez sur **Tour d'horizon du châssis** > **Stockage** > **Contrôleurs** > **Configuration**.
2. Sur la page **Configuration du contrôleur**, dans la section **Configuration étrangère** du contrôleur concerné, cliquez sur :
   - **Supprimer la configuration étrangère** pour effacer la configuration existante du disque.
   - **Importer/Récupérer** pour importer le disque avec la configuration étrangère.

   REMARQUE : Lorsque vous retirez les disques d'un disque virtuel particulier, réinitialisez le contrôleur et réinsérez les lecteurs un par un. Plusieurs instances de disques virtuels de différentes tailles et aux états différents s'affichent sur la page Configuration étrangère. L'activité d'étape et la taille correctes du disque virtuel s'affichent une fois que l'activité d'importation est terminée.

Configuration des paramètres du contrôleur de stockage

Vous pouvez modifier les propriétés d'un contrôleur de stockage, ou configurer les propriétés d'un contrôleur de stockage nouvellement installé.

Configuration des paramètres du contrôleur de stockage à l'aide de l'interface Web CMC

Assurez-vous qu'au moins un contrôleur de stockage est installé dans le châssis.

Pour configurer les paramètres du contrôleur de stockage :

1. Dans l'interface Web CMC, accédez à **Présentation du châssis** > **Stockage** > **Contrôleurs** > **Configurer**.
2. Sur la page de **Configuration du contrôleur**, à partir du menu déroulant **Contrôleur**, sélectionnez le contrôleur.

   REMARQUE : Notez les points suivants :

   - **Si les contrôleurs de stockage sont en mode de tolérance de panne et si les deux sont dotés de la même version de micrologiciel, ils s'affichent comme un seul périphérique dans le menu déroulant. Par exemple, Shared PERC8 (Intégré 1) ou Shared PERC8 (Intégré 2) ou Shared PERC8 (Logement SPERC 5) ou Shared PERC8 (Logement SPERC 6). Si les paramètres de deux contrôleurs sont différents, le message Paramètres incompatibles s'affiche. Vous pouvez définir les propriétés des contrôleurs à tolérance de panne de sorte que les propriétés soient identiques sur les deux contrôleurs. Les contrôleurs dans ce mode ne peuvent pas avoir des propriétés distinctes.**
   - **Si un deuxième contrôleur de stockage, doté d'une version différente de micrologiciel est installé, les contrôleurs s'affichent sous forme de deux composants différents dans le menu déroulant. Par exemple, Shared PERC8 (Intégré 1), Shared PERC8 (Intégré 2), Shared PERC8 (Logement SPERC 5) et Shared PERC8 (Logement SPERC 6).**

   Les valeurs d'attribut du contrôleur sélectionné sont mises à jour dans le tableau.
3. Entrez ou sélectionnez les données appropriées, puis cliquez sur **Appliquer**.

REMARQUE : Pour en savoir plus sur les attributs et les autres champs, voir l'*Aide en ligne*.

Les propriétés nouvellement définies sont appliquées aux contrôleurs sélectionnés et le champ **Valeur actuelle** affiche les valeurs mises à jour des attributs.

Configuration des paramètres du contrôleur de stockage à l'aide de RACADM

Pour configurer le contrôleur de stockage à l'aide d'une commande, utilisez la syntaxe suivante.

```
racadm raid ctrlprop:RAID.ChassisIntegrated.1-1 [-rebuild <value>] [-bgi <value>] [-
reconstruct <value>] [-checkconsistency <value>] [-ccmode {abortonerror | normal}] [-
copybackmode {off | on | onwithsmart}] [-lb {auto | disabled}] [-prunconfigured {yes | no}]
```

Pour plus d'informations, voir le document *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX).

Contrôleurs PERC partagé

Dans le cas des systèmes sur lesquels deux Shared PERC intégrés sont installés, vous pouvez modifier le mode de fonctionnement de **Tolérant de panne** à **Non tolérant de panne**, ou vice-versa à l'aide de l'interface Web ou de la CLI RACADM en activant ou désactivant le deuxième contrôleur PERC 8 partagé interne.

Vous pouvez désactiver le deuxième contrôleur intégré du contrôleur PERC8 partagé interne. Après la désactivation du deuxième contrôleur intégré, le premier contrôleur intégré n'est pas en mode de tolérance de panne. Lorsque le deuxième contrôleur intégré est activé, par défaut les deux contrôleurs intégrés sont en mode de tolérance de panne. Le deuxième contrôleur intégré peut être désactivé à l'aide de la commande `racadm raid disableperc:RAID.ChassisIntegrated.2-1`.

Dans le cas des enceintes externes, les cartes Shared PERC 8 externes dans les logements 5 et 6 peuvent être désactivées respectivement à l'aide des commandes `racadm raid disableperc: RAID.ChassisSlot.5-1 and racadm raid disableperc: RAID.ChassisSlot.6-1`.

Dans l'interface de ligne de commande RACADM, exécutez la commande `racadm raid get controllers` pour répertorier le nombre de contrôleurs Shared PERC du système. Si la commande indique uniquement `RAID.ChassisIntegrated.1-1`, le système est équipé d'un seul contrôleur Shared PERC. Si la commande indique `RAID.ChassisIntegrated.1-1`, `RAID.ChassisIntegrated.2-1`, le système est équipé de deux contrôleurs Shared PERC.

Les deuxièmes cartes Shared PERC 8 intégré et Shared PERC 8 externe dans les logements 5 et 6 peuvent être activées ou désactivées.

Pour modifier le mode de fonctionnement à l'aide de l'interface Web CMC, accédez à la page **Dépannage des contrôleurs** en accédant à **Présentation du châssis** > **Stockage Contrôleurs** dans le volet de gauche, puis sélectionnez l'option **Désactiver le contrôleur RAID** ou **Activer le contrôleur RAID**.

Pour modifier le mode opérationnel à l'aide de l'interface RACADM :

- Exécutez la commande `racadm raid enableperc:RAID.ChassisIntegrated.2-1` pour activer le **PERC 8 partagé intégré 2** et le mode **Tolérance de panne**, si le deuxième PERC8 partagé intégré est désactivé.
- Exécutez la commande `racadm raid enableperc:RAID.ChassisSlot.6-1` pour activer le **Shared PERC8 externe** dans le logement 6.
- Exécutez la commande `racadm raid disableperc:RAID.ChassisIntegrated.2-1` pour désactiver le **deuxième Shared PERC8 intégré** et le mode de **Tolérance de panne**.

REMARQUE :

- **Le châssis doit être sous tension, et tous les modules serveur doivent être mis hors tension avant d'exécuter les commandes d'activation ou de désactivation. Le châssis exécuté automatiquement un cycle d'alimentation dans le cadre de cette opération. Après avoir modifié le mode de fonction du PERC partagé, il est recommandé de réinitialiser le contrôleur CMC à l'aide de la page Dépannage ou de la commande `racadm racreset`.**
- **Par défaut, si des deuxièmes cartes PERC 8 intégré sont détectées, le mode s'affiche comme haute disponibilité.**
- **L'activation du SPERC dans des emplacements externes n'active pas la tolérance de panne.**
- **Pour activer le mode Tolérance de panne du Shared PERC8 externe, reportez-vous à la section *Activer ou désactiver la tolérance de panne du contrôleur RAID externe à l'aide de RACADM*.**

Activation ou désactivation du contrôleur RAID à l'aide de l'interface Web CMC

Pour un châssis VRTX avec deux contrôleurs PERC8 partagés, l'adaptateur PERC 2 intégré peut être activé ou désactivé lorsque l'adaptateur PERC 1 intégré est actif et que tous les modules serveur sont hors tension. Les deux adaptateurs doivent être activés pour la tolérance de panne. La page **Dépannage des contrôleurs** permet d'activer ou de désactiver le contrôleur homologue.

REMARQUE : Pour éviter la perte de données, avant de procéder à des opérations d'activation ou de désactivation de contrôleur :

- **Effectuez toutes les opérations de données, telles que la reconstruction ou la recopie.**
- **Assurez-vous que les volumes de données fonctionnent de manière optimale.**

REMARQUE : Un message d'avertissement s'affiche lors de l'activation du deuxième adaptateur PERC et l'état de tolérance de panne est Dégradé dans les cas suivants :

- **Les paramètres de l'adaptateur PERC sont modifiés.**
- **Le micrologiciel est mis à jour.**

Assurez-vous que le micrologiciel et les paramètres du PERC partagé correspondent pour configurer le système sur le mode de tolérance de Tolérance de panne.

Vous pouvez désactiver un contrôleur homologue uniquement dans les cas suivants :

- Tous les serveurs insérés dans le châssis sont hors tension.
- L'Integrated 1 PERC est actuellement le contrôleur actif.

  REMARQUE : Si l'Integrated 1 PERC n'est actuellement pas le contrôleur actif, effectuez un cycle d'alimentation du châssis pour que ce contrôleur devienne le contrôleur actif.
- Les deux contrôleurs CMC utilisent la même version de micrologiciel qui prend en charge cette fonctionnalité.

REMARQUE : Après avoir désactivé l'adaptateur PERC 2 intégré, pour remplacer une carte CMC, il est recommandé de mettre à jour la carte CMC avec la version de micrologiciel version 1.35 ou ultérieure avant que la carte soit désignée comme contrôleur CMC actif dans le système. Un message d'avertissement s'affiche avant cette action.

Pour activer ou désactiver un contrôleur homologue en mode de tolérance de panne à l'aide de l'interface Web CMC :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Stockage** > **Contrôleurs** > **Dépannage**.
2. Sur la page **Dépannage du contrôleur**, dans le menu déroulant **Actions** du PERC 2 intégré, sélectionnez l'une des options suivantes, puis cliquez sur **Appliquer**.
   - **Désactiver le contrôleur RAID** : désactive le contrôleur homologue en mode de tolérance de panne.
   - **Activer le contrôleur RAID** : active le contrôleur homologue en mode de tolérance de panne. Si le PERC 2 intégré est déjà désactivé, l'option **Activer le contrôleur RAID** est disponible dans le menu déroulant.
   - Pour activer ou désactiver les contrôleurs de carte Shared PERC 8 externes :
     - Dans la page **Dépannage du contrôleur**, à partir du menu déroulant **Actions** de la carte Shared PERC 8 externe dans le logement 5 ou 6, sélectionnez l'une des options suivantes, puis cliquez sur **Appliquer**.
       - **Désactiver le contrôleur RAID** : désactive le contrôleur RAID.
       - **Activer le contrôleur RAID** : active le contrôleur RAID. Si le PERC 2 est déjà désactivé, l'option **Activer le contrôleur RAID** est disponible dans le menu déroulant.
   - **Redéfinir la configuration** : sélectionnez cette option pour supprimer des disques virtuels et annuler l'attribution de tous les disques de secours connectés au contrôleur. Toutefois, cette opération supprime uniquement les disques de la configuration et ne supprime aucune des données. REMARQUE : redéfinir la configuration ne supprime aucune des configurations étrangères. Utilisez Effacer la configuration étrangère pour redéfinir.
   - **Exporter le journal TTY** : sélectionnez cette option pour exporter le journal TTY sur le système local. REMARQUE : le journal TTY collecté auprès du contrôleur ne contient aucune des données des disques. Toutefois, il peut contenir des données telles que des adresses SAS.
   - **Activer la tolérance de panne** : sélectionnez cette option pour activer le mode Tolérance de panne du SPERC externe. Cette action réinitialise également la carte Shared PERC8 externe.
   - **Activer la tolérance de panne** : sélectionnez cette option pour désactiver le mode Tolérance de panne du SPERC externe. Cette action réinitialise également la carte Shared PERC8 externe.

     REMARQUE :

- **Pour un PERC désactivé, aucune des autres options Réinitialiser la configuration, Exporter le journal TTY, Effacer le cache persistant et Désactiver le contrôleur RAID sont disponibles dans le menu déroulant.**
- **Par défaut, les deux adaptateurs de stockage partagé intégré sont détectés avec le mode haute disponibilité.**
- **Vous devez activer le mode Tolérance de panne sur le contrôleur externe partagé une fois qu'il est câblé.**
- **Les options Activer la tolérance de panne et Désactiver la tolérance de panne s'affichent uniquement pour les cartes Shared PERC 8 externe. Le mode par défaut des cartes Shared PERC 8 externe est le mode sans tolérance de panne.**

REMARQUE : L'activation ou la désactivation d'un contrôleur homologue lance un cycle d'alimentation du châssis. Les modifications ne sont répercutées qu'une fois le cycle d'alimentation terminé.

Activation ou désactivation du contrôleur RAID à l'aide de RACADM

Pour activer un contrôleur homologue en utilisant l'interface RACADM, ouvrez une console texte série/Telnet/SSH vers CMC, ouvrez une session et entrez :

```
racadm raid enableperc:<AdapterFQDD>
```

Pour désactiver un contrôleur homologue, entrez :

```
racadm raid disableperc:<AdapterFQDD>
```

REMARQUE : Pour obtenir plus d'informations sur cette fonction en utilisant l'interface RACADM, voir le *Guide de référence de la ligne de commande RACADM pour iDRAC et CMC*.

Activation ou désactivation de la tolérance de panne du contrôleur RAID externe à l'aide de RACADM

Pour activer la tolérance de panne :

```
racadm raid controllers: <FQDD of External Shared PERC8> -p HighAvailabilityMode ha
```

Pour désactiver la tolérance de panne :

```
racadm raid set controllers: <FQDD of External Shared PERC8> -p HighAvailabilityMode None
```

Affichage des propriétés des disques physiques à l'aide de l'interface Web CMC

Vérifiez que les disques physiques sont installés dans le châssis.

Pour afficher les propriétés des disques physiques :

1. Dans le volet de gauche, accédez à **Présentation du châssis** > **Stockage** > **Disques physiques**.
   La fenêtre **Propriétés** s'affiche.
2. Pour afficher les propriétés de tous les disques physiques, sous **Disques physiques**, cliquez sur le .

   REMARQUE : Les attributs suivants s'affichent pour le mode de tolérance de panne des cartes partagées intégrées :
   - **Contrôleur actif : Shared PERC8 (Intégré 1)**
   - **Contrôleur redondant/de basculement : Shared PERC8 (Intégré 2)**

Les attributs suivants s'affichent en mode de tolérance de panne des cartes partagées externes :

- **Contrôleur actif : Shared PERC8 (Logement SPERC 5)**
- **Contrôleur redondant/de basculement : Shared PERC8 (Logement SPERC 6)**

Vous pouvez également utiliser les filtres suivants pour afficher les propriétés d'un disque physique donné :

- Sous l'option **Filtre de disques physiques de base**, dans le menu déroulant **Regrouper par**, sélectionnez **Disque virtuel**, **Contrôleur** ou **Boîtier**, puis cliquez sur **Appliquer**.
- Cliquez sur **Filtre avancé**, sélectionnez les valeurs des attributs et cliquez sur **Appliquer**.

Affichage des propriétés des disques durs physiques à l'aide de RACADM

Pour afficher les propriétés des disques durs physiques à l'aide de RACADM, exécutez la commande `racadm raid get pdisks –o`

Pour plus d'informations, voir le document *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX).

Identification des disques physiques et des disques virtuels

Pour plus d'informations sur l'activation ou la désactivation du clignotement des voyants, voir :

- Configuration du clignotement des LED avec l'interface Web CMC
- Configuration du clignotement des LED avec RACADM

Affectation de disques de rechange globaux à l'aide de l'interface Web CMC

Pour affecter ou désaffecter un disque de rechange global :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Stockage** > **Disque physique** > **Configuration**.
   La page **Configuration des disques physiques** s'affiche.
2. Dans la section **Configuration des disques physiques**, dans le menu déroulant **Actions relatives aux disques physiques**, sélectionnez **Non attribué** ou **Rechange global** pour chacun des disques durs physiques, puis cliquez sur **Appliquer**.

REMARQUE : L'affectation d'un disque de rechange global est autorisée uniquement si au moins un disque virtuel est présent sur le contrôleur correspondant.

Affectation de disques de rechange globaux à l'aide de RACADM

Pour affecter un disque de rechange global à l'aide de RACADM, exécutez la commande `racadm raid hotspare: -assign yes -type ghs`.

Pour plus d'informations sur l'utilisation des commandes RACADM, voir le document *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX).

Récupération de disques physiques

Pour récupérer un disque physique :

1. Dans l'interface Web CMC, accédez à **Présentation du châssis** > **Stockage** > **Disques physiques** > **Configurer**.

2. Sur la page **Configurer**, dans la section **Récupérer des disques physiques**, sélectionnez le disque physique qui doit être restauré, puis, à partir du menu déroulant, sélectionnez **Reconstruire le lecteur**, **Annuler la recréation** ou **Forcer en ligne**, puis cliquez sur **Appliquer**.

Affichage des propriétés des disques virtuels à l'aide de l'interface Web CMC

Vérifiez que vous avez créé les disques virtuels.

Pour afficher les propriétés des disques virtuels :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Stockage** > **Disques virtuels** > **Propriétés**.
2. Dans la page **Propriétés**, dans la section **Disques virtuels**, cliquez sur le . Vous pouvez également utiliser les filtres suivants pour afficher des propriétés de disque spécifiques :
   - Dans la section **Filtre de disques virtuels de base**, dans le menu déroulant **Contrôleur**, sélectionnez le nom du contrôleur et cliquez sur **Appliquer**.
   - Cliquez sur **Filtre avancé**, sélectionnez les valeurs des attributs et cliquez sur **Appliquer**.

Affichage des propriétés de disque virtuel à l'aide de RACADM

Pour afficher les propriétés de disque virtuel à l'aide de RACADM, exécutez la commande `racadm raid get vdisks -o`

Pour plus d'informations, voir le document *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX).

Création d'un disque virtuel à l'aide de l'interface Web CMC

Par défaut, CMC crée des disques virtuels sans les initialiser. Cependant, vous pouvez choisir l'option d'initialisation rapide pour les disques virtuels créés sans initialisation. Le processus d'initialisation rapide efface les premiers et derniers 8 Mo du disque virtuel, ce qui supprime tous les enregistrements d'amorçage et les informations sur les partitions. Vous devez disposer des privilèges d'**Administrateur de configuration du châssis** pour effectuer l'initialisation rapide.

Vérifiez que le disque physique est installé dans le châssis.

REMARQUE : La suppression d'un disque virtuel supprime le disque virtuel de la configuration du contrôleur.

Pour créer un disque virtuel CacheCade :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Stockage** > **Disques virtuels** > **Créer**.
2. Dans la page **Création de disque virtuel**, à la section **Niveau de RAID**, sélectionnez le niveau de RAID.
3. Dans la section **Sélectionner les disques physiques**, sélectionnez le nombre de disques physiques en fonction du niveau de RAID sélectionné.
4. Dans la section **Configurer les paramètres**, entrez les données appropriées, sélectionnez les options **Initialiser** et **Chiffrer le disque virtuel**, puis cliquez sur **Création de disque virtuel**.

   CMC fournit une nouvelle option, l'initialisation, lors de la création de disques virtuels. Cette option vous permet de créer un disque virtuel sans initialisation rapide. Par défaut, le disque virtuel est créé avec l'initialisation rapide.

   L'option **Initialiser** vous permet de créer des disques virtuels sans initialisation. Cette option annule le comportement par défaut où un processus d'initialisation rapide est lancé lors de la création d'un disque virtuel.

   L'option **Chiffrer le disque virtuel** vous permet de créer des disques virtuels sécurisés sur des disques autocryptables (Self-Encryption Drives, SED).

   REMARQUE : L'option Chiffrer le disque virtuel est activée uniquement si la clé de chiffrement est configurée pour le contrôleur spécifique, sur la page Paramètres du contrôleur.

Gestion des clés de chiffrement

Une clé de sécurité ou de chiffrement, créée sur un contrôleur, est utilisée pour verrouiller ou déverrouiller l'accès à des disques virtuels sécurisés créés sur les disques SED. Vous ne pouvez créer qu'une seule clé de chiffrement pour un contrôleur doté de la capacité de chiffrement. Vous pouvez créer des clés de chiffrement en entrant un identifiant de clé de chiffrement et une phrase de passe sur la page **Configuration du contrôleur**. CMC vous permet également de modifier des phrases de passe de clés de chiffrement et de supprimer des clés de chiffrement.

Création d'une clé de chiffrement à l'aide de l'interface Web CMC

Vous pouvez créer des clés de chiffrement ou de sécurité pour les contrôleurs si la clé de chiffrement est **Non configurée**.

Pour créer une clé de chiffrement :

1. Dans le volet de gauche, accédez à **Stockage** > **Contrôleurs** > **Configuration**.
2. Dans la liste déroulante **Clé de sécurité**, sélectionnez **Créer une clé de sécurité**.
   Une fenêtre pop-up s'affiche.
3. Entrez la clé de sécurité et le mot de passe, puis cliquez sur **OK**.
4. Dans la page **Configuration du contrôleur**, cliquez sur **Appliquer**.
   Une fois que la clé de chiffrement est créée, le statut de la **Clé de sécurité** passe à **Activée**.

Création d'une clé de chiffrement à l'aide de RACADM

Pour créer une clé de chiffrement à l'aide d'une commande RACADM, utilisez la syntaxe suivante :

```
racadm raid createsecuritykey:RAID.ChassisIntegrated.1-1 -key <Key id> -passwd <passphrase>
```

Pour plus d'informations, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX*.

Modification de l'identifiant d'une clé de chiffrement à l'aide de l'interface Web CMC

Vous pouvez modifier l'identifiant et la phrase de passe d'une clé de chiffrement pour les contrôleurs.

Pour modifier l'identifiant et la phrase de passe d'une clé de chiffrement :

1. Dans le volet de gauche, accédez à **Stockage** > **Contrôleurs** > **Configuration**.
2. Dans la liste déroulante **Clé de sécurité**, sélectionnez **Modifier clé de sécurité**.
   Une fenêtre pop-up s'affiche.
3. Saisissez l'identifiant de la nouvelle clé de chiffrement et les phrases de passe nouvelle et existante, puis cliquez sur **OK**.
4. Dans la page **Configuration du contrôleur**, cliquez sur **Appliquer**.

Modification de l'ID d'une clé de chiffrement à l'aide de RACADM

Pour modifier l'ID et la phrase de passe d'une clé de chiffrement à l'aide d'une commande RACADM, utilisez la syntaxe suivante :

```
racadm raid modifysecuritykey:RAID.ChassisIntegrated.1-1 -key <Key id> -oldpasswd
<oldpassphrase> -newpasswd <newpassphrase>
```

Pour plus d'informations, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX*.

Suppression d'une clé de chiffrement à l'aide de l'interface Web CMC

Vous pouvez uniquement supprimer des clés de chiffrement d'un contrôleur lorsqu'aucun disque virtuel sécurisé ne lui est associé.

Pour supprimer une clé de chiffrement :

1. Dans le volet de gauche, accédez à **Stockage** > **Contrôleurs** > **Configuration**.
2. Dans la liste déroulante **Clé de sécurité**, sélectionnez **Supprimer la clé de sécurité**.
   Un message de confirmation s'affiche.
3. Cliquez sur **OK** pour continuer.

   Une fois la clé de chiffrement supprimée, tous les disques SED qui ne font pas partie des disques virtuels sont effacés de façon sécurisée. Pour plus d'informations, reportez-vous à l'*Aide en ligne*.

Suppression d'une clé de chiffrement à l'aide de RACADM

Pour supprimer une clé de chiffrement à l'aide d'une commande RACADM, utilisez la syntaxe suivante :

```
racadm raid deletesecuritykey:RAID.ChassisIntegrated.1-1
```

Pour plus d'informations, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX*.

Cryptage de disques virtuels

Vous pouvez chiffrer des disques virtuels créés sur des disques SED après avoir configuré une clé de chiffrement sur le contrôleur. Lorsque vous effectuez un chiffrement, un message est enregistré dans le `Journal CMC`. Vous pouvez chiffrer des disques virtuels :

- La clé de sécurité est configurée sur le contrôleur.
- Tous les disques sur le disque virtuel sont des disques SED.

Le chiffrement d'un seul disque virtuel permet le chiffrement sur tous les disques virtuels du même groupe de disques.

Vous devez disposer des privilèges d'**Administrateur de configuration du châssis** pour le chiffrement de disques virtuels.

Chiffrement de disques virtuels à l'aide de l'interface Web CMC

Pour chiffrer un disque virtuel existant :

1. Dans le volet de gauche, cliquez sur **Stockage** > **Disques virtuels** > **Gérer**.
2. Dans la liste déroulante **Actions virtuelles**, sélectionnez **Chiffrer le disque virtuel** et cliquez sur **Appliquer**.

REMARQUE : L'option Chiffrer le disque virtuel est disponible uniquement si des disques virtuels non sécurisés sont configurés dans le SED.

Chiffrement de disques virtuels à l'aide de RACADM

Pour chiffrer des disques virtuels à l'aide d'une commande RACADM, utilisez la syntaxe suivante :

```
racadm raid encryptvd:Disk.Virtual.0:RAID.ChassisIntegrated.1-1
```

Pour plus d'informations, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX*.

Déverrouillage d'une configuration étrangère

Les lecteurs qui font partie de lecteurs virtuels sécurisés sont des lecteurs sécurisés. Les lecteurs sécurisés peuvent être migrés d'un contrôleur vers un autre contrôleur. Si une autre clé de sécurité ou de cryptage est configurée pour le contrôleur de destination, l'état de sécurité de ces lecteurs est « locked » (verrouillé) et ne peut pas être considéré comme faisant partie de « preview foreign config » (aperçu des configurations étrangères). L'option « Import foreign config » (Importation des configurations étrangères) ne détecte pas ces lecteurs étrangers.

Lors de l'exécution de la commande de déverrouillage, fournissez l'ID de clé et la phrase secrète du contrôleur source pour ces lecteurs. Même après déverrouillage, l'option « foreign controller key » (clé de contrôleur étranger) sécurise toujours ces lecteurs. Cependant, vous pouvez voir ces lecteurs lors de la recherche de lecteurs étrangers dans l'option « preview foreign config » (aperçu des configurations étrangères) existante. Vous pouvez importer ou effacer la configuration étrangère sur ces lecteurs sécurisés.

Si des lecteurs étrangers avec des clés de sécurité différentes sont migrés à partir de plusieurs contrôleurs, déverrouillez et importez ou effacez l'ensemble des lecteurs à partir d'un contrôleur étranger avant de déverrouiller les lecteurs migrés à partir d'un autre contrôleur. Cette action assure que le déverrouillage n'est pas autorisé sur un contrôleur, si le contrôleur possède des lecteurs déverrouillés, mais non importés ou effacés.

Une fois que les disques sont déverrouillés, vous pouvez importer la configuration étrangère à l'aide de l'interface Web CMC ou de RACADM.

Si le contrôleur est éteint et rallumé après le déverrouillage et avant l'importation, les disques sont à nouveau verrouillés.

Si le système dispose de plusieurs configurations étrangères, déverrouillez et importez chaque configuration étrangère avant de déverrouiller la configuration étrangère.

L'ID de clé utilisé pour le déblocage vise uniquement à identifier les lecteurs avec l'ID de clé correspondant. Une fois les lecteurs correspondants trouvés, la phrase secrète est utilisée pour déverrouiller les lecteurs.

Déverrouillage d'une configuration étrangère à l'aide de l'interface Web du CMC

Pour verrouiller la configuration étrangère :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Stockage** > **Contrôleurs** > **Configuration**.
2. Accédez à la page **Configuration**.
3. Cliquez sur **Cliquer ici pour déverrouiller**.
   La page **Disques physiques** s'affiche.
4. Sélectionnez les disques physiques que vous souhaitez déverrouiller.
5. Vérifiez que le disque physique est associé à l'ID de clé.
6. À partir du menu déroulant **Actions**, sélectionnez **Déverrouiller le lecteur.**
   Une boîte de dialogue vous invite à saisir la phrase de la clé de sécurité.
7. Saisissez une phrase secrète dans la zone de texte **Phrase secrète de la clé de sécurité**.
8. Saisissez de nouveau la phrase secrète, puis cliquez sur **Déverrouiller**.
   Le disque physique est déverrouillé et le lecteur ne s'apparaît pas dans la liste **Récupérer des disques physiques**.

Déverrouillage d'une configuration étrangère à l'aide de RACADM

Pour déverrouiller une configuration étrangère à l'aide d'une commande RACADM, utilisez la syntaxe suivante :

```
racadm raid unlock:<Controller FQDD> -key <Key id> -passwd <passphrase>
```

Pour plus d'informations, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX*.

Effacement cryptographique

Vous pouvez utiliser l'option d'effacement cryptographique pour effacer en toute sécurité les données présentes sur les disques SED sécurisés. Les données sécurisées continuent d'exister sur les disques même après la suppression des disques virtuels, et sont donc exposées aux menaces. L'effacement cryptographique peut être utilisé dans les conditions suivantes :

- Pour effacer les données afin de mettre hors service/réutiliser des disques sécurisés.
- Pour effacer en toute sécurité des données si vous n'avez pas besoin d'importer une configuration étrangère verrouillée sécurisée.
- Pour récupérer des disques verrouillés si la phrase de passe est perdue.

Vous pouvez effectuer l'effacement cryptographique sur un ou plusieurs disques physiques SED.

PRÉCAUTION : L'exécution de la tâche d'effacement cryptographique supprime toutes les données du disque physique.

Exécution de l'effacement cryptographique

Si le disque physique fait partie d'un disque virtuel, retirez-le du disque virtuel avant d'exécuter l'effacement cryptographique.

Pour réaliser un effacement cryptographique :

1. Dans le volet de gauche, accédez à **Stockage** > **Disques physiques** > **Configuration**.
   La page **Configuration des disques physiques** s'affiche.
2. Sélectionnez le disque physique duquel vous souhaitez effacer les données.
3. Dans la liste déroulante **Actions relatives aux disques physiques**, sélectionnez **Effacement cryptographique** et cliquez sur **Appliquer**.
   Un message s'affiche pour confirmer l'action.
4. Cliquez sur **Oui** pour continuer.
   Toutes les données du disque physique sélectionné sont supprimées.

Application d'une stratégie d'accès d'adaptateur virtuel aux disques virtuels

Vérifiez que les disques physiques sont installés et que les disques virtuels ont été créés.

Pour appliquer la stratégie d'accès d'adaptateur virtuel :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Stockage** > **Disques virtuels** > **Affecter**.
2. Sur la page **Affecter des disques virtuels**, dans la section **Stratégie d'accès pour les adaptateurs virtuels**, dans le menu déroulant **Adaptateur virtuel <number>**, sélectionnez **Accès complet** pour chaque disque physique.
3. Cliquez sur **Appliquer**.

Maintenant, vous pouvez affecter des adaptateurs virtuels aux logements des serveurs. Pour plus d'informations, voir Affectation d'adaptateurs virtuels aux logements dans le Guide d'utilisation.

Modification des propriétés des disques virtuels à l'aide de l'interface Web CMC

Pour modifier les propriétés des disques virtuels :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Stockage** > **Disques virtuels** > **Gérer**.
2. Sur la page **Gérer les disques virtuels**, dans le menu déroulant **Actions de disque virtuel**, sélectionnez l'une des actions suivantes et cliquez sur **Appliquer**.
   - **Renommer**
   - **Supprimer**

REMARQUE : Si vous sélectionnez Supprimer, le message suivant s'affiche pour indiquer que la suppression d'un disque virtuel va supprimer définitivement les données qu'il contient.

```
Deleting the virtual disk removes the virtual disk from the controller's configuration.
Initializing the virtual disk permanently erases data from the virtual disk.
```

- **Modifier la stratégie : cache en lecture**
- **Modifier la stratégie : cache en écriture**
- **Modifier la stratégie : cache de disque**
- **Initialiser : rapide**
- **Initialiser : plein**
- **Crypter le disque virtuel**

Module de gestion d'enceinte (EMM)

Le module de gestion d'enceinte (EMM) fournit le chemin d'accès aux données et aux tâches de gestion de l'enceinte. Le module EMM surveille et contrôle les composants de l'enceinte et l'accès aux lecteurs.

Le module EMM communique les attributs et les états de l'enceinte au serveur hôte. Les modules EMM surveillent les composants suivants de l'enceinte :

- Ventilateurs
- Blocs d'alimentation
- Capteurs de température
- Insertion ou retrait d'un disque physique
- Voyants LED sur l'enceinte

Affichage des attributs et de l'état du module EMM

L'état du module EMM affiche l'état d'intégrité du module EMM. Les modules EMM contiennent une valeur d'état unique à l'enceinte. Vous pouvez avoir jusqu'à deux modules EMM. Le micrologiciel de l'enceinte crée un état pour chaque module EMM.

Affichage de l'état et des attributs du module EMM à l'aide de l'interface Web

Pour afficher l'état et les attributs du module EMM :

Cliquez sur **Présentation du châssis** → **Stockage** → **Enceintes** → **Propriétés**. La **page Enceintes** fournit l'état et les attributs du module EMM des enceintes du châssis. Développez l'enceinte intégrée ou les enceintes externes pour afficher l'état et les attributs du module EMM. Pour en savoir plus, voir l'*Aide en ligne de CMC*.

Affichage des attributs et de l'état du module EMM à l'aide de l'interface RACADM

Pour afficher l'état du module EMM, utilisez la commande `racadm raid get emms -o -p Status`.

Pour afficher les attributs du module EMM, utilisez la commande `racadm raid get emms -o`.

Pour en savoir plus, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX* disponible sur le site **dell.com/support/manuals**.

Affichage des attributs et de l'état de l'enceinte

Le CMC affiche l'état d'intégrité de l'enceinte en fonction des composants physiques. Les données des enceintes connectées au stockage partagé s'affichent dans le CMC, mais les enceintes externes connectées à quelques cartes PCIe s'affichent pas. Vous devez disposer des privilèges de connexion au CMC pour afficher l'état et les attributs des enceintes.

Affichage de l'état et des attributs de l'enceinte à l'aide de l'interface Web

Pour afficher l'état et les attributs de l'enceinte :

Cliquez sur **Tour d'horizon du châssis** → **Stockage** → **Boîtiers** → **Propriétés**. La **page Boîtiers** indique l'état d'intégrité des boîtiers dans le châssis. Pour plus d'informations, voir l'*Aide en ligne CMC*.

REMARQUE : L'état rollup du boîtier devient critique lorsque le module EMM, le PSU ou le ventilateur est retiré mais que l'état principal reste inchangé. Une fois que le CMC ou le châssis est passé en cycle de marche/arrêt, l'état principal passe également à critique.

Affichage de l’état et des attributs du boîtier à l’aide de RACADM

Pour afficher l’état du boîtier, utilisez la commande `racadm raid get enclosures –o –p Status`.

Pour afficher les attributs du boîtier, utilisez la commande `racadm raid get enclosures –o`.

Pour en savoir plus, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX* disponible sur le site **dell.com/support/manuals**.

Rapports de jusqu'à deux enceintes par connecteur

Chaque carte Shared PERC 8 externe prend en charge jusqu'à deux enceintes par connecteur. Cependant, il existe deux configurations différentes qui comportent des restrictions différentes. Dans une configuration à un seul PERC (sans tolérance de pannes), vous pouvez connecter jusqu'à deux enceintes par carte. Comme le câblage est redondant, une solution de carte Shared PERC 8 externe avec tolérance de panne prend en charge jusqu'à deux enceintes par paire avec tolérance de panne.

Si plus de deux enceintes sont détectées sur n'importe quel connecteur, un message d'avertissement est consigné dans le journal du châssis. Ceci affecte l'intégrité du châssis et génère une alerte active ou une entrée dans le journal du châssis.

Définition du numéro d'inventaire et du nom d'inventaire de l'enceinte

Pour identifier les enceintes, définissez le nom d'inventaire et le numéro d'inventaire des enceintes.

REMARQUE :

- **Un message d'erreur s'affiche si vous entrez une valeur non valide.**
- **Initialement, la valeur enregistrée dans le micrologiciel s'affiche .**
- **Vous devez disposer des privilèges de configuration de châssis pour définir le numéro d'inventaire et le nom d'inventaire de l'enceinte.**
- **Vous pouvez définir le numéro d'inventaire et le nom d'inventaire uniquement pour les enceintes externes.**

Définition du numéro d'inventaire et du nom d'inventaire de l'enceinte à l'aide de l'interface Web

Pour définir le numéro d'inventaire et le nom d'inventaire de l'enceinte, cliquez sur **Présentation du châssis** → **Stockage** → **Enceintes** → **Configurer**. Entrez le **Numéro d'inventaire** et le **Nom d'inventaire** dans les champs appropriés, puis cliquez sur **Appliquer**. Pour en savoir plus, voir l'*Aide en ligne de CMC*.

Définition du numéro d’inventaire et du nom d’inventaire du boîtier à l’aide de l’interface RACADM

Pour définir le numéro d’inventaire du boîtier, utilisez la commande `racadm raid set enclosures: Enclosure.External.0-0:RAID.ChassisSlot.5-1 –p AssetTag <value>`.

Pour définir le nom d’inventaire du boîtier, utilisez la commande `racadm raid set enclosures: Enclosure.External.0-0:RAID.ChassisSlot.5-1 –p AssetName <value>`.

Pour en savoir plus, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX* disponible sur le site **dell.com/support/manuals**.

Affichage de l'état et des attributs du capteur de température de l'enceinte

L'état du capteur de température affiche l'état des capteurs de température de l'enceinte. Les capteurs contiennent une valeur d'état unique pour l'enceinte. Vous pouvez avoir jusqu'à quatre capteurs de température et le micrologiciel de l'enceinte crée un état pour chaque capteur. Vous devez disposer des privilèges de connexion au CMC pour afficher l'état du capteur.

Affichage de l'état et des attributs du capteur de température de l'enceinte à l'aide de l'interface Web

Pour afficher l'état et les attributs du capteur de température de l'enceinte :

Cliquez sur **Présentation du châssis** → **Stockage** → **Enceintes** → **Propriétés**. La page **Enceintes** indique l'état d'intégrité et les attributs du capteur de température de l'enceinte dans le châssis. Développez l'enceinte externe pour afficher l'état du bloc d'alimentation des enceintes. Pour en savoir plus, voir l'*Aide en ligne de CMC*.

Affichage des attributs du capteur de température du boîtier à l'aide de l'interface RACADM

Pour afficher les attributs du capteur de température du boîtier, utilisez la commande `racadm raid get tempprobes -o`. Pour plus d'informations, reportez-vous au *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX* disponible à l'adresse **dell.com/cmcmanuals**.

Définition du seuil d'avertissement de température de l'enceinte

L'option Seuil d'avertissement de température vous permet de modifier le seuil à partir duquel une température d'enceinte est rapportée avec un avertissement.

REMARQUE :

- **Un message d'erreur s'affiche si vous entrez une valeur non valide.**
- **Initialement, la valeur enregistrée dans le micrologiciel s'affiche .**
- **Vous devez disposer des privilèges de configuration de châssis pour définir le numéro d'inventaire et le nom d'inventaire de l'enceinte.**

Définition du seuil d'avertissement de température de l'enceinte à l'aide de l'interface Web

Pour définir le seuil d'avertissement de température de l'enceinte :

Cliquez sur **Présentation du châssis** → **Stockage** → **Enceintes** → **Configurer**. Sélectionnez l'enceinte à partir du menu déroulant **Enceinte**, puis entrez les valeurs appropriées pour les températures minimale et maximale du seuil d'avertissement de capteur de température 2 et 3. Entrez le **Numéro d'inventaire** et le **Nom d'inventaire** dans les champs appropriés, puis cliquez sur **Appliquer**. Pour en savoir plus, voir l'*Aide en ligne de CMC*.

Définition du seuil d'avertissement de température du boîtier à l'aide de RACADM

Pour définir le seuil minimal d'avertissement du capteur de température dans le boîtier, utilisez la commande `racadm raid set tempprobes:TempSensor.Embedded.0:Enclosure.External.1-0:RAID.ChassisSlot.6-1 -p MinimumWarningThreshold <value>`.

Pour définir le seuil maximal d'avertissement du capteur de température dans le boîtier, utilisez la commande `racadm raid set tempprobes:TempSensor.Embedded.0:Enclosure.External.1-0:RAID.ChassisSlot.6-1 -p MaximumWarningThreshold <value>`.

Pour en savoir plus, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX* disponible sur le site **dell.com/support/manuals**.

Affichage de l'état et des attributs du ventilateur de l'enceinte

L'option d'état du ventilateur et d'attributs permet d'afficher l'état du ventilateur de l'enceinte et contient une valeur d'état unique à l'enceinte. Vous pouvez avoir jusqu'à deux ventilateurs, et le micrologiciel de l'enceinte crée un état pour chaque ventilateur. Vous devez disposer des privilèges de connexion à CMC pour afficher l'état du ventilateur.

REMARQUE : S'il manque un bloc d'alimentation, le ventilateur correspondant du bloc d'alimentation affiche un état critique.

Affichage de l'état et des attributs du ventilateur de l'enceinte à l'aide de l'interface Web

Pour afficher l'état et les attributs du bloc d'alimentation :

Cliquez sur **Présentation du châssis** → **Stockage** → **Enceintes** → **Propriétés**. La page **Enceinte** indique l'état d'intégrité et les attributs du ventilateur de l'enceinte. Développez l'enceinte externe pour afficher l'état du ventilateur de l'enceinte. Pour en savoir plus, voir l'*Aide en ligne de CMC*.

Affichage de l'état et des attributs du ventilateur du boîtier à l'aide de RACADM

Pour afficher l'état du ventilateur, utilisez la commande `racadm raid get fans -o -p Status`.

Pour afficher les attributs du ventilateur, utilisez la commande `racadm raid get fans -o`.

Pour en savoir plus, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX* disponible sur le site **dell.com/support/manuals**.

Affichage des propriétés du boîtier à l'aide de l'interface Web CMC

Pour afficher les propriétés du boîtier :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Stockage** > **Boîtiers** > **Propriété**.
2. Sur la page **Propriétés**, dans la section **Boîtier**, cliquez sur le pour afficher la vue graphique des disques physiques et leur état, le résumé des logements de disque physique et les propriétés avancées.

16

Gestion des logements PCIe

Par défaut, tous les logements ne sont pas associés. Vous pouvez :

- Afficher l'état de tous les logements PCIe dans le châssis.
- Attribuer ou supprimer des serveurs un logement PCIe.

Tenez compte des points suivants avant d'affecter un logement PCIe à un serveur :

- Vous ne pouvez pas affecter un logement PCIe à un serveur sous tension.
- Un logement PCIe avec un adaptateur affecté à un serveur ne peut pas être affecté à un autre serveur si le serveur affecté d'un adaptateur (source) est sous tension.
- Un logement PCIe avec un adaptateur affecté à un serveur ne peut pas être affecté à un autre serveur (cible) sous tension.

Considérez ce qui suit avant de retirer d'un serveur un logement PCIe attribué :

- Si un logement PCIe est vide, le logement ne peut pas être désaffecté d'un serveur, même si le serveur est sous tension.
- Si un logement PCIe contient un adaptateur et qu'il n'est pas sous tension, il ne peut pas être désaffecté du serveur, même si ce dernier est sous tension. Cette situation existe lorsqu'un logement est vide, que le serveur affecté du logement est sous tension et que l'utilisateur insère un adaptateur dans le logement vide.

Adresser ou supprimer l'adressage de l'adaptateur PCIe externe au serveur lame :

- L'adaptateur est toujours sous tension en tant que périphérique non partagé. Désormais, l'adaptateur est adressé à un serveur.
- Si un logement PCIE externe est occupé par un adaptateur partagé, l'adressage antérieur à l'insertion de l'adaptateur reste inchangée.
- Si un logement PCIE externe est occupé par un adaptateur partagé, le logement PCIE ne peut ni adresser ni supprimer l'adressage depuis/vers vers un serveur lame. Si un utilisateur tente d'adresser ou de supprimer l'adressage d'un adaptateur partagé, un message EEMI est consigné.

Pour plus d'informations sur l'attribution à des serveurs et le retrait de serveurs d'un logement PCIe, voir l' *Aide en ligne*.

REMARQUE :

- **Sans licence, vous pouvez attribuer un maximum de quatre logements PCIe à un serveur pleine hauteur, deux au logement supérieur et deux au logement d'extension, ou deux périphériques PCIe à un serveur mi-hauteur.**
- **Vous pouvez distinguer les propriétés des logements PCIE avec des périphériques de carte Shared PERC 8 externes de périphériques dédiés. Ces périphériques partagés ont des propriétés différentes de celles des périphériques dédiés.**
- **Dans le cas des SPERC externes, l'état Partagé s'affiche. Les options d'adressage et de suppression d'adressage du Shared PERC 8 externe ne sont pas disponibles.**

Sujets :

Affichage des propriétés des logements PCIe à l'aide de l'interface Web CMC

- Pour afficher les informations relatives aux huit logements PCIe, dans le volet de gauche, cliquez sur **Présentation du châssis** > **Présentation de PCIe**. Cliquez sur le + pour afficher toutes les propriétés du logement approprié.
- Pour afficher les informations d'un logement PCIe, cliquez sur **Présentation du châssis** > **Logement PCIe <numéro>** > **Propriétés** > **Condition**.

REMARQUE : L'interface utilisateur différencie les logements PCIe externes qui contiennent des périphériques SPERC (ou tout périphérique partagé) des logements PCIE munis d'adaptateurs dédiés, car ces périphériques partagés ont des propriétés différentes.

Affectation de logements PCIe aux serveurs à l'aide de l'interface Web de CMC

Pour affecter des logements PCIe aux serveurs :

- Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Présentation de PCIe** > **Configurer** > **Adressage de logements PCIe aux logements de serveur**. Dans la page **Adressage de logements PCIe aux logements de serveur**, dans la colonne **Action**, dans le menu déroulant **Action**, sélectionnez le nom de serveur approprié et cliquez sur **Appliquer**.

Notez les points suivants :

- Sans licence, le nombre maximal de logements PCIe qui peuvent être adressés à un serveur mi-hauteur est de deux. Si un serveur pleine hauteur est installé, vous pouvez adresser deux logements PCIe au logement supérieur du serveur et au logement inférieur (étendu) du serveur, pour un total de quatre logements PCIe par serveur pleine hauteur**.**
- Vous pouvez adresser les logements de serveur à n'importe lesquels des 8 logements PCIe.
- Les mezzanines supérieure et inférieure d'un serveur pleine hauteur sont remplies. Si ce n'est pas le cas, l'auto-test de démarrage s'arrête lorsque <F1> ou <F2> s'affiche sur la page pour que vous appuyiez sur l'une de ces clés.
- Dans le cas de serveurs standard, vous pouvez adresser un maximum de deux logements PCIE à la mezzanine supérieure, et de deux logements à la mezzanine inférieure. Par défaut, tous les adressages PCIe au logement de serveur 3 vont aux mezzanines inférieures.
- Le numéro de logement du serveur s'affiche comme Slot (logement) 01, Slot 02, etc. Pour un serveur pleine hauteur, le nom de logement apparaît comme Ext. de Slot 01, Ext. de Slot 02, et ainsi de suite.
- Si vous sélectionnez le nom d'hôte, celui-ci s'affiche au lieu du nom du logement.
- CMC fournit la possibilité d'alerte via le Journal des événements système (SEL), SNMP et les interfaces de courrier électronique.

Pour plus d'informations sur l'affectation de périphériques PCIe à un serveur, voir l'*Aide en ligne*.

Gestion des logements PCIe à l'aide de RACADM

Vous pouvez affecter ou désaffecter un logement PCIe à un serveur en utilisant les commandes RACADM. Certaines commandes sont fournies ici. Pour plus d'informations sur les commandes RACADM, voir le document *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX) sur le site dell.com/support/Manuals.

- Pour afficher l'affectation en cours des périphériques PCIe aux serveurs, exécutez la commande suivante :

```
racadm getpiecfg -a
```

- Pour afficher les propriétés des périphériques PCIe en utilisant le nom de domaine qualifié, exécutez la commande suivante :

```
racadm getpciecfg [-c <FQDD>]
```

  Par exemple, pour afficher les propriétés du périphérique PCIe 1, exécutez la commande suivante.

```
racadm getpciecfg -c PCIE.ChassisSlot.1
```

- Pour affecter un logement d'adaptateur PCIe à un logement de serveur, exécutez la commande suivante :

```
racadm setpciecfg assign [-c <FQDD>] [i <server slot>]
```

- Par exemple, pour affecter le logement PCIe 5 au logement de serveur 2, exécutez la commande suivante :

```
racadm setpciecfg assign -c PCIE.ChassisSlot.5 -i 2
```

- Pour désaffecter le logement PCIe 3 d'un serveur, exécutez la commande suivante :

```
racadm setpciecfg unassign -c pcie.chassisslot.3
```

Ride de puissance PCIe immédiate

récemment attribué cartes PCIe dans CMC VRTX doivent être découverts et l'initialisation du système avant d'un nœud de serveur est sous tension. Le processus d'initialisation et de la détection implique les opérations suivantes :

- Inventaire et détection des cartes de la configuration de
- Préparation d'une carte PCIe de l'exposition à un module serveur
- Préparation de plusieurs cartes pour être configurés par le BIOS du serveur
- Initialisation de toutes les cartes préalablement à la mise sous tension d'un nœud de serveur lame

Tous ces processus devaient quelques secondes pour terminer ce qui entraîne un retard de l'initialisation des cartes PCIe. La fonctionnalité à PCIe Ride dans CMC VRTX ce processus permet de réduire la durée du cycle. Le PCIe Ride fonctionnalité permet à ce qui suit :

- Les nœuds de serveur sont allumés rapidement, ce qui permet de mettre sous tension les cartes PCIe rapidement.
- L'état des cartes PCIe alimenté est étendue pour une période de temps prédéfinis dans les scénarios suivants :
  - Une fois que le serveur est hors tension.
  - Une fois que la détection de cartes est terminée.
- L'état de préparation de la mise sous tension des cartes est valable pour une durée prédéfinie une fois le processus de découverte. Cela vous évite les retards extension pour les types d'effectuer un cycle d'alimentation sur des scénarios. Les cartes continuent à être dans l'état « Prêt » en attente et la mise sous tension de l'affectation des nœuds. Les cartes mise sous tension après le délai expiré.

.

REMARQUE : À la fin de la période, les cartes PCIe sont mises hors tension. Toutes les cartes en mode Ride-through sont également mises hors tension dès que la trappe du châssis est ouverte.

REMARQUE :

- **Si le contrôleur CMC ne dispose pas de suffisamment de puissance, il met hors tension toutes les cartes en mode Ride-through pour libérer l'ensemble de l'alimentation qui leur est allouée. Si l'alimentation est rétablie, l'alimentation est réattribuée aux logements PCIe. Ainsi, les cartes sont prêtes pour l'allocation serveur sans délai.**
- **Tous les adaptateurs PCIE externes sous tension en mode partagé sont exclus des processus Ride-through. Après la mise sous tension d'un adaptateur partagé en tant que périphérique partagé, il reste sous tension jusqu'à ce que le châssis soit hors tension.**

Affichage des propriétés PCIe Ride-through à l'aide de l'interface Web CMC

Pour afficher les propriétés PCIe Ride-through, dans le volet de gauche, cliquez sur **Présentation du châssis** > **Présentation de PCIe**. La page **Condition PCIe** s'affiche. La section **Paramètres généraux** affiche les propriétés PCIe Ride-through suivantes :

- **État Ridethrough** : Activé ou Désactivé
- **Délai d'expiration Ridethrough** : indique la période pendant laquelle la fonction Ride-through est activée

Affichage de l'état des propriétés PCIe Ridethrough à l'aide de RACADM

Pour afficher les informations sur les propriétés ridethrough de puissance PCIe, entrez la commande suivante :

```
racadm getpciecfg -r
```

Pour plus d'informations, voir le document *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX).

Configuration des propriétés PCIe Ride-through à l'aide de l'interface Web CMC

Pour configurer les propriétés PCIe Ride-through pour CMC VRTX :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Configurer** > **Ridethrough**.
   La page des **Paramètres PCIe Ridethrough** s'affiche.
2. Pour activer ou désactiver la fonctionnalité PCIe Ride-through, sélectionnez ou désélectionnez l'option **Activer PCIe Ridethrough**.

   REMARQUE : Par défaut, la fonctionnalité Ride-through est activée et la période définie est de 300 secondes.

3. Dans le champ **Délai d'attente**, entrez la durée pendant laquelle la fonctionnalité Ride-through doit être activée.
   Entrez zéro (0) ou une valeur allant de 60 à 1800 secondes. Zéro indique un délai d'expiration infini.
4. Cliquez sur **Appliquer**.

Configuration de l'état des propriétés PCIe Ride-through à l'aide de RACADM

Vous pouvez configurer les propriétés de puissance PCIe Ride-through, en exécutant les commandes suivantes :

- Pour désactiver la fonctionnalité Ride-through, exécutez la commande `racadm setpciecfg ridethru -d`
- Pour activer la fonctionnalité Ride-through, exécutez la commande `racadm setpciecfg ridethru -e`
- Pour réinitialiser la propriété de délai d'expiration Ride-through, exécutez la commande `racadm setpciecfg ridethru -t <timeout>`
- Pour définir la plage de délai d'attente acceptable, exécutez la commande `racadm setpciecfg help ridethru`

Pour plus d'informations, voir le document *Chassis Management Controller for PowerEdge VRTX RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX).

17

Dépannage et restauration

Cette section explique comment exécuter les tâches de récupération et de résolution des problèmes sur le système distant en utilisant l'interface Web CMC.

- Affichage des informations sur le châssis
- Affichage des journaux d'événements
- Collecte des informations de configuration, d'état d'erreur et des journaux d'erreurs
- Utilisation de la console de diagnostic
- Gestion de l'alimentation d'un système distant
- Gestion des tâches Lifecycle Controller sur un système distant.
- Réinitialisation des composants
- Dépannage des problèmes de protocole de temps du réseau (NTP)
- Dépannage des problèmes de réseau
- Dépannage des problèmes d'alerte
- Réinitialisation de mot de passe administrateur oublié
- Enregistrement et restauration des certificats et paramètres de configuration du châssis.
- Affichage de journaux et codes d'erreur

REMARQUE : La prise en charge WinRM pour Microsoft n'est plus disponible pour le client Windows 10 : utilisez Power Shell au lieu de WinRM.

Sujets :

Réinitialisation de mot de passe administrateur oublié

Vous devez disposer des informations d'identification de l'utilisateur disposant de privilèges d'**administrateur** pour effectuer des tâches de gestion. Le logiciel CMC dispose d'une fonctionnalité de sécurité du mot de passe du compte d'utilisateur pouvant être désactivée en cas d'oubli du mot de passe du compte d'administrateur. En cas d'oubli du mot de passe du compte d'administrateur, vous pouvez le restaurer à l'aide du cavalier J_PWORD sur la carte CMC.

La carte CMC dispose d'un connecteur à deux broches de réinitialisation du mot de passe comme indiqué dans la figure suivante. Si un cavalier est installé sur le connecteur de réinitialisation, le compte administrateur et le mot de passe par défaut sont activés et définis sur les valeurs par défaut `username: root` et `password: calvin`.

Tableau 42. Paramètres du cavalier de mot de passe CMC

Commande du cavalier	Image du cavalier	État du cavalier	État de réinitialisation du cavalier
J_PWORD		(par défaut)	La fonction de réinitialisation du mot de passe est désactivée.
			La fonction de réinitialisation du mot de passe est activée.

REMARQUE : Assurez-vous que le module CMC est en mode passif avant de démarrer.

Lors de l'installation du cavalier J_PWORD est installé, le compte d'administrateur et le mot de passe par défaut sont activés et définis sur les valeurs par défaut suivantes :

```
username: root
password: calvin
```

Le compte administrateur est réinitialisé, même si le compte d'administrateur a été supprimé ou si le mot de passe a été changé.

REMARQUE : Lorsque le cavalier J_PWORD est installé, une configuration console en série par défaut est utilisée (plutôt que les valeurs de propriété de configuration), comme suit :

```
cfgSerialBaudRate=115200
cfgSerialConsoleEnable=1
cfgSerialConsoleQuitKey=^\
cfgSerialConsoleIdleTimeout=0
cfgSerialConsoleNoAuth=0
cfgSerialConsoleCommand=""
cfgSerialConsoleColumns=0
```

La procédure suivante explique comment réinitialiser le mot de passe administrateur oublié :

1. Appuyez sur le loquet de déverrouillage du CMC situé sur la poignée et tirez sur le panneau avant du module. Faites glisser le module CMC hors du boîtier.
   REMARQUE : Les événements liés aux décharges électrostatiques (ESD) peuvent endommager le CMC. Dans certains cas, de l'électricité statique peut s'accumuler sur votre corps ou un objet, tel qu'un appareil, puis se décharger dans le CMC. Pour éviter tout dommage lié aux décharges électrostatiques, veillez à décharger l'électricité statique de votre corps lors de la manipulation et de l'accès au CMC, à l'extérieur du châssis.
2. Court-circuitez les broches d'en-tête **Récupération de mot de passe** à l'aide d'un cavalier.
3. Retirez la fiche du cavalier du connecteur de réinitialisation du mot de passe, puis insérez un cavalier à 2 broches pour activer le compte administrateur par défaut. Pour localiser le cavalier de mot de passe sur la carte CMC, consultez la figure suivante.
4. Faites glisser le module CMC dans le boîtier. Rebranchez tous les câbles qui ont été déconnectés.
   REMARQUE : Assurez-vous que le module CMC est actif jusqu'à la fin des étapes restantes.
5. Attendez que le CMC ait fini de redémarrer. Dans l'interface Web, dans l'arborescence système, accédez à **Présentation du châssis** et cliquez sur **Alimentation** > **Contrôle**, sélectionnez **Réinitialiser le CMC (redémarrage à chaud)**, puis cliquez sur **Appliquer**.
6. Connectez-vous au CMC actif en utilisant le nom d'utilisateur administrateur : root et le mot de passe: calvin par défaut, puis restaurez les paramètres de compte d'utilisateur nécessaires. Les comptes et mots de passe existants ne sont pas désactivés et sont toujours actifs.
7. Effectuez les opérations de gestion requises, y compris la création d'un mot de passe administrateur.
8. Appuyez sur le loquet de déverrouillage du CMC situé sur la poignée et tirez sur le panneau avant du module. Faites glisser le module CMC hors du boîtier.
9. Retirez le cavalier 2 broches de l'en-tête **Récupération de mot de passe** et remettez en place la fiche de cavalier.
10. Faites glisser le module CMC dans le boîtier. Rebranchez tous les câbles qui ont été déconnectés. Répétez l'étape 4 pour que le module CMC sans cavalier soit le contrôleur CMC actif.

Collecte des informations de configuration, de l'état du châssis et des journaux à l'aide de RACADM

La sous-commande `racdump` fournit une commande unique d'obtention de la condition complète du châssis, des informations sur l'état de configuration et des journaux.

La sous-commande `racdump` affiche les informations suivantes :

- informations générales sur le système/RAC
- informations sur CMC
- informations sur le châssis
- Informations sur les sessions
- Informations du capteur
- informations sur le numéro du micrologiciel

Interfaces prises en charge

- CLI RACADM
- Interface RACADM distante
- RACADM Telnet

`racdump` inclut les sous-systèmes suivants et regroupe les commandes RACADM suivantes. Pour plus d'informations sur `racdump`, reportez-vous au *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX*.

Tableau 43. Commandes racadm pour les sous-systèmes

Sous-système	Commande RACADM
Informations générales sur le système/RAC	`getsysinfo`
Informations sur les sessions	`getssninfo`
Informations du capteur	`getsensorinfo`
Informations du commutateur (module d'E/S)	`getioinfo`
Informations de la carte mezzanine (carte fille)	`getdcinfo`
Informations de tous les modules	`getmodinfo`
Informations du bilan de puissance	`getpbinfo`
Informations KVM	`getkvminfo`
Informations de NIC (module CMC)	`getniccfg`
Informations de redondance	`getredundancymode`
Information du journal de suivi	`gettracelog`
Journal des événements RAC	`getraclog`
Journal des événements système	`getsel`

Téléchargement du fichier MIB (Management Information Base) SNMP

Le fichier MIB (Management Information Base) SNMP du contrôleur CMC définit les types de châssis, les événements et les indicateurs. Le contrôleur CMC vous permet de télécharger le fichier MIB à l'aide de l'interface Web.

Pour télécharger le fichier MIB SNMP du contrôleur CMC à l'aide de l'interface Web du CMC :

1. Dans le volet gauche, cliquez sur **Présentation du châssis** > **Réseaux** > **Services** > **SNMP**.

2. Dans la section **Configuration SNMP**, cliquez sur **Enregistrer** pour télécharger le fichier `MIB` du CMC vers le système local.

   Pour plus d'informations sur le fichier `MIB` SNMP, reportez-vous au *Guide de référence SNMP de Dell OpenManage Server Administrator* sur le site **dell.com/support/manuals**.

Premières étapes de dépannage d'un système distant

Les questions suivantes permettent de résoudre les problèmes généraux dans le système géré :

- Le système est-il sous tension ou hors tension ?
- S'il est sous tension, le système d'exploitation fonctionne-t-il, répond-il ou est-il arrêté ?
- S'il est hors tension, l'alimentation électrique a-t-elle été coupée soudainement ?

Dépannage de l'alimentation

Les informations suivantes vous aident à dépanner le bloc d'alimentation et à résoudre des problèmes d'alimentation :

- **Problème :** j'ai configuré la **Stratégie de redondance de l'alimentation** sur **Redondance de réseau d'alimentation** et un événement de Perte de redondance des blocs d'alimentation est survenu.
  - **Solution A :** cette configuration nécessite au moins un bloc d'alimentation côté 1 (les deux logements de gauche) et un bloc d'alimentation, côté 2 (les deux logements de droite), installés et fonctionnels dans le boîtier modulaire. De plus, la capacité de chaque côté doit être suffisante pour prendre en charge le total d'allocation de puissance nécessaire pour maintenir la **Redondance de réseau d'alimentation** du châssis. (Pour une redondance du réseau d'alimentation complète, vérifiez que vous disposez d'une configuration complète de 4 blocs d'alimentation.)
  - **Solution B :** vérifiez que tous les blocs d'alimentation sont correctement connectés aux deux réseaux d'alimentation CA ; les blocs d'alimentation côté 1 doivent être connectés à l'un des réseaux d'alimentation CA, et ceux du côté 2 doivent être raccordés à l'autre réseau d'alimentation, et les deux réseaux CA doivent fonctionner. La **Redondance d'alimentation** est perdue si l'un des réseaux d'alimentation CA ne fonctionne pas.
- **Problème :** l'état des blocs d'alimentation (PSU) est **En échec (Pas d'alimentation CA)**, même lorsqu'un cordon secteur est connecté et que l'unité de distribution électrique produit une sortie CA satisfaisante.
  - **Solution A :** vérifiez et remplacez le cordon d'alimentation secteur. Vérifiez que l'unité de distribution électrique (PDU) qui alimente le bloc d'alimentation fonctionne comme prévu. Si le problème persiste, contactez le service clientèle Dell pour obtenir un bloc d'alimentation de rechange.
  - **Solution B :** vérifiez que le bloc d'alimentation (PSU) est connecté avec la même tension que les autres blocs. Si CMC détecte un bloc d'alimentation avec une tension différente, le PSU est éteint et marqué comme En échec.
- **Problème :** l'enclenchement dynamique des blocs d'alimentation est activé, mais aucun des blocs d'alimentation ne s'affiche à l'état **Veille**.
  - **Solution A :** puissance excédentaire insuffisante. Un ou plusieurs blocs d'alimentation sont placés à l'état En attente uniquement lorsque le surplus de puissance disponible dans l'enceinte dépasse la capacité d'au moins un bloc d'alimentation.
  - **Solution B :** il est impossible de prendre entièrement en charge le mode DPSE (Dynamic Power Supply Engagement) avec les blocs d'alimentation présents dans l'enceinte. Pour vérifier si tel est le cas, utilisez l'interface Web pour désactiver la fonction DPSE, puis réactivez-la. Un message s'affiche si le système ne prend pas entièrement en charge DPSE.
- **Problème :** un nouveau serveur a été inséré dans l'enceinte contenant assez de blocs d'alimentation, mais la mise sous tension du serveur ne peut s'effectuer.
  - **Solution A :** vérifiez le paramètre de limite de puissance d'entrée système ; il se peut qu'il soit affecté d'un niveau trop faible pour permettre la mise sous tension de serveurs supplémentaires.
  - **Solution B :** vérifiez le paramètre maximal d'économie d'énergie. S'il est défini, se problème apparaît. Pour plus d'informations, voir les paramètres de configuration de l'alimentation.
  - **Solution D :** vérifiez la priorité de puissance du logement associé au nouveau serveur inséré et veillez à ce qu'elle soit supérieure ou égale à toutes les autres priorités de puissance de logement de serveur.
- **Problème :** la puissance disponible ne cesse d'évoluer, même lorsque la configuration de l'enceinte modulaire n'a pas changé.
  - **Solution :** la gestion dynamique de l'alimentation des ventilateurs du contrôleur CMC réduit brièvement la puissance allouée aux serveurs si le boîtier fonctionne à un niveau proche du seuil de puissance maximale configuré par l'utilisateur ; cela permet d'allouer de la puissance aux ventilateurs en réduisant les performances des serveurs afin de maintenir la consommation d'énergie en dessous de la **limite de puissance d'entrée système** définie. Ce comportement est normal.
- **Problème :** le <nombre> W est signalé pour le paramètre **Surplus pour un pic de performance**.

- **Solution :** l'enceinte dispose de <nombre> W de puissance excédentaire disponible dans la configuration actuelle, et la **limite de puissance d'entrée système** peut être réduite en toute sécurité en fonction de cette quantité signalée sans affecter les performances des serveurs.

- **Problème :** un sous-ensemble de serveurs a perdu son alimentation suite à une panne du réseau d'alimentation CA, alors que le châssis fonctionnait en mode de configuration de la **Redondance d'alimentation** avec quatre blocs d'alimentation.
  - **Solution :** cette situation peut se produire si les blocs d'alimentation sont mal connectés aux réseaux d'alimentation CA redondants au moment de la panne de réseau CA. La stratégie de **Redondance de l'alimentation** exige que les deux blocs d'alimentation de gauche soient connectés à un autre réseau d'alimentation CA. Si deux blocs d'alimentation sont mal connectés, par exemple si le bloc 3 et le bloc 4 sont connectés aux mauvais réseaux d'alimentation CA, une panne de circuit CA provoque la perte d'alimentation des serveurs de moindre priorité.
- **Problème :** les serveurs de priorité inférieure ne sont plus alimentés, suite à la panne d'un bloc d'alimentation (PSU).
  - **Solution** : pour éviter toute panne future de bloc d'alimentation entraînant la mise hors tension des serveurs, veillez à ce que le châssis dispose d'au moins trois blocs d'alimentation et soit configuré pour la stratégie **Redondance du bloc d'alimentation** afin d'empêcher la panne de bloc d'alimentation d'affecter le fonctionnement des serveurs.
- **Problème :** les performances globales du serveur diminuent lorsque la température ambiante augmente dans le centre de données.
  - **Solution :** cela peut se produire si vous avez défini l'option **Limite de la puissance d'entrée système** sur une valeur qui provoque une augmentation des besoins d'alimentation des ventilateurs, qui doit être compensée par une réduction de la puissance allouée aux serveurs. L'utilisateur peut configurer l'option **Limite de la puissance d'entrée système** sur une valeur plus élevée, qui permet d'allouer de la puissance supplémentaire aux ventilateurs sans aucun impact sur les performances des serveurs.

Dépannage des alertes

Utilisez le journal CMC et le journal de trace pour résoudre les alertes CMC. La réussite ou l'échec de chaque tentative de distribution par e-mail et/ou interruption SNMP sont consignés dans le journal CMC. Des informations supplémentaires concernant chaque erreur sont journalisées dans le journal de trace. Toutefois, comme SNMP ne confirme pas la distribution des interruptions, utilisez un analyseur de réseau ou un outil tel que l'utilitaire snmputil de Microsoft pour suivre les paquets sur le système géré.

Affichage des journaux d'événements

Vous pouvez afficher les journaux du matériel et du contrôleur CMC pour en savoir plus sur les événements critiques qui se produisent sur le système géré.

Affichage du journal du matériel

Le contrôleur CMC génère un journal du matériel pour les événements qui se produisent sur le châssis. Vous pouvez afficher ce journal avec l'interface Web ou avec RACADM distant.

REMARQUE : Vous devez disposer du privilège Administrateur d'effacement des journaux pour effacer le journal du matériel.

REMARQUE : Vous pouvez configurer le contrôleur CMC pour envoyer un e-mail ou une interruption SNMP lorsque des événements spécifiques se produisent. Pour plus d'informations sur la configuration du contrôleur CMC pour l'envoi d'alertes, voir Configuration du contrôleur CMC pour envoyer des alertes.

Exemples d'entrées du journal du matériel

```
critical System Software event: redundancy lost
Wed May 09 15:26:28 2007 normal System Software
event: log cleared was asserted
Wed May 09 16:06:00 2007 warning System Software
event: predictive failure was asserted
Wed May 09 15:26:31 2007 critical System Software
event: log full was asserted
Wed May 09 15:47:23 2007 unknown System Software
event: unknown event
```

Affichage des journaux du matériel avec l'interface Web CMC

Vous pouvez afficher, enregistrer et effacer le journal du matériel. Vous pouvez trier les entrées de journal sur la base des champs Gravité, Date/Heure ou Description, en cliquant sur l'en-tête de colonne approprié. Un autre clic sur l'en-tête choisi inverse le tri.

Pour afficher les journaux du matériel à l'aide de l'interface Web CMC, dans le volet de gauche, cliquez sur **Présentation du châssis** > **Jounaux**. La page **Journal du matériel** s'affiche. Pour enregistrer une copie du journal du matériel sur la station gérée ou le réseau, cliquez sur **Enregistrer le journal**, puis définissez l'emplacement d'un fichier texte du journal.

REMARQUE : Comme le journal est enregistré dans un fichier texte, les images graphiques utilisées pour indiquer la gravité dans l'interface utilisateur ne s'affichent pas. Dans le fichier texte, la gravité est signalée par les mentions OK, Informatif, Inconnu, Avertissement et Grave. Les entrées de date et d'heure sont triées dans l'ordre croissant. Si la mention <AMORÇAGE SYSTÈME> apparaît dans la colonne Date/Heure, cela signifie que l'événement s'est produit pendant la mise sous tension ou hors tension des modules, lorsque l'heure et la date n'étaient pas disponibles.

Pour effacer le journal du matériel, cliquez sur **Effacer le journal**.

REMARQUE : CMC crée une nouvelle entrée du journal qui indique que celui-ci a été effacé.

REMARQUE : Pour effacer le journal du matériel, vous devez disposer du privilège d'Administrateur d'effacement des journaux.

Affichage des journaux du matériel avec RACADM

Pour afficher le journal du matériel avec RACADM, ouvrez une console texte série, Telnet ou SSH sur le CMC, connectez-vous, puis entrez :

```
racadm getsel
```

Pour effacer le journal du matériel, entrez :

```
racadm clrsel
```

Affichage du journal du châssis

CMC génère un journal des événements liés au châssis. CMC fournit la possibilité d'alertes via le Journal des événements système (SEL), SNMP, et les Interfaces de courrier électronique.

SPERC est inséré alors que un ou plusieurs serveurs PowerEdge sont sous tension.

REMARQUE :

- **Pour effacer le journal du châssis, vous devez disposer de droits d'Administrateur d'effacement des journaux.**

Affichage des journaux du châssis à l'aide de RACADM

Pour afficher les informations du journal du châssis à l'aide de RACADM, ouvrez une console texte série, Telnet ou SSH sur le contrôleur CMC, connectez-vous, puis entrez :

```
racadm chassislog view
```

Cette commande affiche les 25 dernières entrées du journal du châssis.

Pour afficher les options disponibles pour afficher les journaux du châssis, exécutez la commande suivante :

```
racadm chassislog help view
```

Affichage des journaux du châssis à l'aide de l'interface Web

Vous pouvez afficher, enregistrer et effacer le journal du châssis. Vous pouvez filtrer les journaux en fonction du type et du filtre de journal. En outre, vous pouvez exécuter une recherche en fonction d'un mot clé et afficher le journal pour certains jours.

Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Journaux** > **Journal du châssis**. La page du **journal du châssis** s'affiche.

Pour enregistrer une copie du journal du châssis sur la station ou le réseau géré, cliquez sur **Enregistrer le journal**, puis spécifiez l'emplacement d'enregistrement du fichier journal.

Utilisation de la console de diagnostic

Vous pouvez diagnostiquer les problèmes liés au matériel du châssis à l'aide de commandes CLI si vous êtes un utilisateur expert ou que vous suivez les instructions du support technique.

REMARQUE : Pour pouvoir modifier ces paramètres, vous devez disposer du privilège d'Administrateur de commande de débogage.

Pour accéder à la console des diagnostics :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Dépannage** > **Diagnostics**.
   La page **Console de diagnostic** s'affiche.
2. Dans la zone de texte **Commande**, entrez une commande et cliquez sur **Envoyer**.

   Pour plus d'informations sur les commandes, voir l'*Aide en ligne*.

   La page Résultats des diagnostics apparaît.

Réinitialisation des composants

Vous pouvez réinitialiser le contrôleur CMC actif ou réinstaller virtuellement les serveurs afin qu'ils fonctionnent comme s'ils avaient été retirés et réinsérés. Si le châssis contient un contrôleur CMC de secours, la réinitialisation du contrôleur CMC actif provoque un basculement et le contrôleur CMC de secours devient actif.

REMARQUE : Pour réinitialiser les composants, vous devez disposer du privilège Administrateur de commandes de débogage.

Pour réinitialiser les composants avec l'interface Web CMC

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Dépannage** > **Réinitialiser les composants**.
   La page **Réinitialiser les composants** s'affiche.
2. Pour réinitialiser le contrôleur actif CMC, dans la section **État du contrôleur CMC**, cliquez sur **Réinitialiser/Basculer le contrôleur CMC**. S'il existe un contrôleur CMC de secours et que le châssis est complètement redondant, un basculement a lieu et le contrôleur de secours CMC devient actif. Cependant, si aucun contrôleur CMC de secours n'est présent, le contrôleur CMC disponible est redémarré.
3. Pour réinstaller virtuellement le serveur, dans la section **Repositionnement virtuel du serveur**, sélectionnez le serveur voulu, puis cliquez sur **Appliquer les sélections**.

   Reportez-vous à l'*Aide en ligne* pour plus d'informations.

   Cette opération oblige les serveurs à se comporter comme s'ils avaient été retirés et réinsérés.

Enregistrement ou restauration de la configuration de châssis

Il s'agit d'une fonction sous licence. Pour enregistrer ou restaurer une sauvegarde de la configuration du châssis en utilisant l'interface Web CMC :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Configurer** > **Sauvegarde du châssis**. La page **Sauvegarde du châssis** s'affiche. Pour enregistrer la configuration du châssis, cliquez sur **Enregistrer**. Remplacez le chemin de fichier par défaut (facultatif) et cliquez sur **OK** pour enregistrer le fichier. Le nom de fichier de sauvegarde par défaut contient le numéro de service du châssis. Ce fichier de sauvegarde peut être utilisé plus tard pour restaurer les paramètres et les certificats de châssis uniquement.
2. Pour restaurer la configuration du châssis, dans la section « Restaurer », cliquez sur **Parcourir**, définissez le fichier de sauvegarde, puis cliquez sur **Restaurer**.

   REMARQUE :

   - **CMC ne se réinitialise pas lors de la restauration de la configuration, mais il faut parfois un certain temps aux services CMC pour imposer un changement ou une nouvelle configuration. Une fois l'opération terminée avec succès, toutes les sessions en cours sont fermées.**
   - **Les informations FlexAddress, les profils de serveur et le stockage étendu ne sont pas enregistrés ou restaurés avec la configuration du châssis.**

Résolution des erreurs de protocole de temps du réseau

Après la configuration du CMC pour qu'il synchronise son horloge avec un serveur de temps distant sur le réseau, il peut s'écouler 2 à 3 minutes avant que la date et l'heure ne soient modifiées. Si aucun changement ne s'est produit après ce délai, il existe peut-être un problème que vous devez corriger. Le CMC peut ne pas synchroniser son horloge pour les raisons suivantes :

- Problème des paramètres Network Time Protocol (NTP) Server 1 (Serveur NTP 1), NTP Server 2 (Serveur NTP 2) et NTP Server 3 (Serveur NTP 3).
- Nom d'hôte ou adresse IP non valide entré par erreur.
- Problème de connexion réseau qui empêche le CMC de communiquer avec l'un des serveurs NTP configurés.
- Problème DNS, qui empêche la résolution des noms d'hôte de serveur NTP.

Pour résoudre les problèmes liés au NTP, consultez les informations du journal de suivi du CMC. Ce journal contient un message d'erreur pour les échecs liés au NTP. Si le CMC ne peut se synchroniser avec aucun des serveurs NTP distants configurés, l'horloge du CMC est synchronisée avec l'horloge système locale et le journal de suivi stocke une entrée semblable à celle-ci :

```
Jan 8 20:02:40 cmc ntpd[1423]: synchronized to LOCAL(0), stratum 10
```

Vous pouvez également vérifier la condition ntpd en tapant la commande RACADM suivante :

```
racadm getractime -n
```

Le résultat de cette commande contient des statistiques NTP détaillées qui peuvent faciliter le débogage du problème.

Si vous tentez de configurer un serveur NTP Windows, il peut s'avérer utile d'augmenter le paramètre `MaxDist` correspondant à `ntpd`. Avant de modifier ce paramètre, vérifiez bien tout ce qu'il implique, car le paramètre par défaut doit être suffisant pour fonctionner avec la plupart des serveurs NTP.

Pour modifier le paramètre, entrez la commande suivante :

```
racadm config -g cfgRemoteHosts -o cfgRhostsNtpMaxDist 32
```

Une fois la modification effectuée, désactivez NTP, attendez 5-10 secondes, puis réactivez NTP :

REMARQUE : Il faut jusqu'à trois minutes supplémentaires pour que NTP se resynchronise.

Pour désactiver NTP, entrez :

```
racadm config -g cfgRemoteHosts -o cfgRhostsNtpEnable 0
```

Pour activer NTP, entrez :

```
racadm config -g cfgRemoteHosts -o cfgRhostsNtpEnable 1
```

Si les serveurs NTP sont correctement configurés et que cette entrée est présente dans le journal de suivi, cela confirme que le CMC est incapable de se synchroniser avec l'un des serveurs NTP configurés.

Si l'adresse IP du serveur NTP n'est pas configurée, vous pouvez voir une entrée semblable à la suivante dans le journal de suivi :

```
Jan 8 19:59:24 cmc ntpd[1423]: Cannot find existing interface for address 1.2.3.4 Jan 8
19:59:24 cmc ntpd[1423]: configuration of 1.2.3.4 failed
```

Si un paramètre de serveur NTP a été configuré avec un nom d'hôte non valide, l'entrée de journal de suivi suivante risque de s'afficher :

```
Aug 21 14:34:27 cmc ntpd_initres[1298]: host name not found: blabla Aug 21 14:34:27 cmc
ntpd_initres[1298]: couldn't resolve `blabla', giving up on it
```

Pour plus d'informations sur la saisie de la commande `gettracelog` afin de vérifier le journal de suivi à l'aide de l'interface Web CMC, voir Utilisation de la console de diagnostic.

Interprétation des couleurs des LED et séquences de clignotement

Les voyants du châssis fournissent l'état suivant d'un composant :

- Des LED vertes allumées en continu indiquent que le composant est sous tension. Si la LED verte clignote, cela indique un événement critique mais courant pendant lequel l'unité n'est pas opérationnelle. Cela n'indique pas de panne.
- Une LED orange clignotant sur un module indique une panne de ce module.
- Les LED bleues clignotantes peuvent être configurées par l'utilisateur et utilisées à des fins d'identification. Pour plus d'informations sur la configuration, reportez-vous à la section Configuration des voyants LED pour identifier les composants du châssis.

Tableau 44. Couleur des LED et séquences de clignotement

Composant	Couleur de la LED, séquence de clignotement	État
CMC	Vert, continu	Sous tension
	Bleu, continu	firmware en cours de téléversement Mise à jour du firmware réussie
	Hors tension	Mise à jour du firmware en cours
	Vert, foncé	Hors tension
	Bleu, continu	Actif
	Bleu, clignotant	ID d'un module activé par l'utilisateur
	Orange, continu	Inutilisé
	Orange, clignotant	Panne
	Bleu, foncé	Mode veille
Serveur	Vert, continu	Sous tension
	Vert, clignotant	firmware en cours de téléversement
	Vert, foncé	Hors tension
	Bleu, continu	Normal
	Bleu, clignotant	ID d'un module activé par l'utilisateur
	Orange, continu	Inutilisé
	Orange, clignotant	Panne
	Bleu, foncé	Pas de panne
Module d'E/S (courant)	Vert, continu	Sous tension
	Vert, clignotant	firmware en cours de téléversement
	Vert, foncé	Hors tension
	Bleu, continu	Normal/maître de la pile
	Bleu, clignotant	ID d'un module activé par l'utilisateur
	Orange, continu	Inutilisé
	Orange, clignotant	Panne
	Bleu, foncé	Pas de panne/esclave de la pile
Module d'E/S (transfert)	Vert, continu	Sous tension
	Vert, clignotant	Inutilisé
	Vert, foncé	Hors tension

Tableau 44. Couleur des LED et séquences de clignotement (suite)

Composant	Couleur de la LED, séquence de clignotement	État
	Bleu, continu	Normal
	Bleu, clignotant	ID d'un module activé par l'utilisateur
	Orange, continu	Inutilisé
	Orange, clignotant	Panne
	Bleu, foncé	Pas de panne
Pulseur	Vert, continu	Ventilateur en marche
	Vert, clignotant	Inutilisé
	Vert, foncé	Hors tension
	Orange, continu	Type de ventilateur non reconnu ; mettre à jour le firmware CMC
	Orange, clignotant	Défaillance du ventilateur ; tachymètre hors de portée
	Orange, foncé	Inutilisé
Bloc d'alimentation	(Ovale) Vert, continu	Alimentation en courant alternatif OK
	(Ovale) Vert, clignotant	Inutilisé
	(Ovale) Vert, foncé	Alimentation en courant alternatif défaillante
	Orange, continu	Inutilisé
	Orange, clignotant	Panne
	Orange, foncé	Pas de panne
	(Cercle) Vert, continu	Alimentation en courant continu OK
	(Cercle) Vert, foncé	Alimentation en courant continu défaillante
Boîtier	Bleu	Lorsque le serveur hôte identifie le boîtier
	Orange	Mis sous tension ou Réinitialisation, état de défaillance

Dépannage d'un contrôleur CMC qui ne répond pas

Si vous ne pouvez pas vous connecter au contrôleur CMC via l'une des interfaces (interface Web, Telnet, SSH, RACADM distant ou série), vous pouvez vérifier le fonctionnement du contrôleur CMC en observant ses voyants.

REMARQUE : Il est impossible de se connecter sur le contrôleur CMC de secours à l'aide d'une console série.

Observation des LED afin d'isoler le problème

Deux voyants se trouvent sur le côté gauche de la carte :

- Voyant supérieur gauche : indique l'état de l'alimentation. S'il est allumé :
  - Vérifiez qu'une alimentation secteur est présente sur au moins l'un des blocs d'alimentation.
  - Vérifiez que la carte CMC est correctement insérée. Vous pouvez libérer ou tirer le levier d'éjection, retirer le contrôleur CMC, puis le réinstaller en vous assurant que la carte est bien poussée à fond et que le loquet se ferme correctement.
- Voyant gauche inférieur : il s'agit d'un voyant multicolore. Lorsque le contrôleur CMC est actif et en cours d'exécution et qu'il n'existe aucun problème, le voyant inférieur est bleu. S'il est orange, cela implique qu'une erreur s'est produite correspondant à l'un des trois événements suivants :
  - Échec du noyau. Vous devez alors remplacer la carte CMC.
  - Échec de l'auto-test. Vous devez alors remplacer la carte CMC.
  - Corruption de l'image. Dans ce cas, téléversez l'image du micrologiciel CMC pour restaurer le CMC.

REMARQUE : Au cours d'un démarrage CMC ou d'une réinitialisation normaux, le contrôleur CMC prend plus d'une minute pour s'amorcer entièrement dans son système d'exploitation avant d'être disponible pour la connexion. Le voyant bleu est allumé lorsque le contrôleur CMC est actif. Dans une configuration redondante à deux contrôleurs CMC, seul le voyant supérieur vert est allumé sur le contrôleur CMC de secours.

Dépannage des problèmes de réseau

Le journal de suivi intégré du CMC vous permet de déboguer les alertes et la gestion de réseau du CMC. Vous pouvez accéder au journal de suivi à l'aide de l'interface Web du CMC ou de RACADM. Reportez-vous à la section de la commande `gettracelog` dans le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge VRTX*.

Le journal de suivi enregistre les informations suivantes :

- DHCP : effectue le suivi des paquets envoyés à un serveur DHCP et reçus de celui-ci.
- DDNS : effectue le suivi des requêtes et des réponses de mise à jour du DNS.
- Modifications de configuration apportées aux interfaces réseau.

Le journal de suivi peut en outre contenir des codes d'erreur spécifiques au firmware CMC qui correspondent au firmware CMC intégré et non pas au système d'exploitation du système géré.

Résolution des problèmes d'un contrôleur

Pour résoudre les problèmes d'un contrôleur :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Stockage** > **Contrôleurs** > **Dépannage**.
2. Sur la page **Dépannage du contrôleur**, dans la liste déroulante **Actions** du contrôleur, sélectionnez l'une des options suivantes et cliquez sur **Appliquer**.
   - **Réinitialiser la configuration** : supprime les disques virtuels et les disques de rechange. Cependant, les données des disques ne sont pas effacées.
     REMARQUE : La réinitialisation de la configuration PERC supprime le cache persistant, le cas échéant, sur le contrôleur PERC.
   - **Exporter le journal TTY** : le journal de débogage TTY du contrôleur de stockage est exporté vers le système local.
   - **Supprimer le cache persistant** : supprime les données stockées dans le cache du contrôleur RAID.
     REMARQUE : S'il existe un cache persistant, l'option permettant de l'effacer est présente. Dans le cas contraire, cette option ne s'affiche pas.
   - **Désactiver le contrôleur RAID** : désactive le contrôleur homologue. Cette option est disponible dans le menu déroulant uniquement pour le Shared PERC8 (Integré 2) et Shared PERC8 externe.
   - **Activer le contrôleur RAID** : active le contrôleur homologue. L'option **Activer le contrôleur RAID** est disponible dans le menu déroulant.
     REMARQUE :

     Pour un PERC désactivé, aucune des autres options Réinitialiser la configuration, Exporter le journal TTY, Effacer le cache persistant et Désactiver le contrôleur RAID sont disponibles dans le menu déroulant.
   - **Activer la tolérance de panne** : active le mode tolérance de panne de la carte Shared PERC 8 externe.
   - **Désactiver la tolérance de panne** : désactive le mode tolérance de panne de la carte Shared PERC 8 externe.
     REMARQUE : Les options Activer la tolérance de panne et Désactiver la tolérance de panne s'affichent uniquement pour les cartes Shared PERC 8 externes. Le mode par défaut des cartes Shared PERC 8 externes est le mode sans tolérance de panne.

REMARQUE :

- **Affiche un message d'erreur si les lames sont sous tension.**
- **La commande échoue si les lames sont sous tension.**

Enfichage à chaud d'enceintes dans un châssis avec tolérance des pannes

1. Assurez-vous que les logements 5 et 6 du châssis ne disposent pas de la tolérance des pannes.
2. Débranchez les enceintes.
3. Modifiez l'état des logements 5 et 6 au mode de tolérance aux pannes.
4. Rebranchez les enceintes avec des câbles tolérants aux pannes.

Éteignez et rallumez le châssis après avoir déconnecté les enceintes et avant de les reconnecter, étant donné que les lecteurs conservent la réservation SCSI-3 précédente jusqu'à ce que le que le châssis soit éteint et rallumé.

18

Utilisation de l'interface de l'écran LCD

Vous pouvez utiliser l'écran LCD du châssis pour procéder à la configuration et aux diagnostics, et pour obtenir des informations sur l'état du châssis et de son contenu.

La figure suivante illustre l'écran LCD. Cet écran affiche des menus, des icônes, des images et des messages.

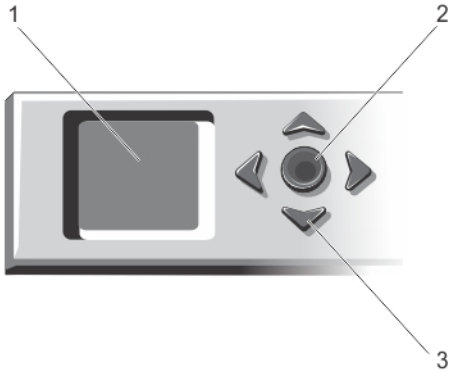


Figure 4. Affichage LCD

1. Écran LCD
2. Bouton de sélection (vérification)
3. Boutons de défilement (4)

Sujets :

Navigation sur l'écran LCD

Le côté droit de l'écran LCD comporte cinq boutons : quatre boutons flèche (haut, bas, gauche et droite) ainsi qu'un bouton central.

- *Pour passer d'un écran à l'autre, utilisez les boutons fléchés droite (suivant) et gauche (précédent). À tout moment, lorsque vous utilisez le panneau, vous pouvez revenir à un écran précédent.*
- *Pour faire défiler les options d'un écran, utilisez les touches fléchées Bas et Haut.*
- *Pour sélectionner et enregistrer un élément d'écran, et passer à l'écran suivant, utilisez le bouton central.*

Les flèches directionnelles modifient les éléments ou les icônes de menu sélectionnés à l'écran. L'élément sélectionné est représenté par un arrière-plan bleu clair ou une bordure.

Lorsque les messages affichés sur l'écran LCD débordent de l'écran, utilisez les boutons flèches gauche et droite pour faire défiler le texte vers la gauche et vers la droite.

Les icônes décrites dans le tableau suivant permettent de naviguer d'un écran à l'autre du panneau LCD.

Tableau 45. Icônes de navigation de l'écran LCD

Icône normale	Icône en surbrillance	Nom et description de l'icône
		**Précédent** — Mettez cette icône en surbrillance et appuyez sur le bouton central pour revenir à l'écran précédent.

Tableau 45. Icônes de navigation de l'écran LCD (suite)

Icône normale	Icône en surbrillance	Nom et description de l'icône
		**Accepter/Oui** — Mettez cette icône en surbrillance et appuyez sur le bouton central pour accepter une modification, puis revenir à l'écran précédent.
		**Ignorer/Suivant** — Mettez cette icône en surbrillance et appuyez sur le bouton central pour ignorer toutes les modifications, puis passer à l'écran suivant.
		**Non** — Mettez cette icône en surbrillance et appuyez sur le bouton central pour répondre « Non » à une question, puis passer à l'écran suivant.
		**Identifier le composant** — Fait clignoter la LED bleue d'un composant. **REMARQUE : Un rectangle bleu clignotant entoure cette icône lorsque l'identification de composant est activée.**

Un indicateur d'état LED de l'écran LCD fournit une indication de l'intégrité générale du châssis et de ses composants.

- Un voyant bleu continu indique une intégrité satisfaisante.
- Un voyant orange clignotant indique qu'au moins un composant est défaillant.
- Un voyant bleu clignotant est un signal d'identification d'un châssis au sein d'un groupe de châssis.

Menu principal

Vous pouvez naviguer vers l'un des écrans suivants depuis le **menu principal** :

- **Association KVM** : contient les options d'association de l'interface KVM aux serveurs et de dissociation.
- **Association de DVD :** cette option s'affiche dans le **menu principal** uniquement si vous avez installé un lecteur de DVD.
- **Enceinte** : affiche les informations d'état du châssis.
- **Résumé IP** : affiche des informations sur CMC IPv4, CMC IPv6, iDRAC IPv4 et iDRAC 4 IPv6.
- **Paramètres** : contient des options, telles que **Langue de l'écran LCD**, **Orientation du châssis**, **Écran LCD par défaut** et **Paramètres réseau**.

Menu de mappage KVM

Dans cet écran, vous pouvez afficher les informations d'association du KVM au serveur, associer un autrre serveur au KVM ou dissocier la connexion existante. Pour utiliser le KVM pour un serveur, sélectionnez **Association KVM** dans le menu principal, accédez au serveur approprié, puis appuyez sur le bouton central **Vérifier**.

Association d'un lecteur de DVD

En utilisant cette page, vous pouvez afficher les informations d'association de lecteur de DVD à un serveur, associer un autre serveur au lecteur de DVD dans le châssis ou dissocier la connexion existante. Pour permettre à un serveur d'accéder au lecteur de DVD, sélectionnez **Association de lecteur de DVD** dans le menu principal, accédez au serveur et appuyez sur le bouton central **Vérifier**.

Le lecteur de DVD peut être associé au logement de serveur uniquement s'il est activé pour ce logement. Il ne peut pas être dissocié pour éviter l'utilisation par les logements de serveur. L'intégrité du lecteur de DVD est critique si le câble SATA n'est pas correctement connecté entre le lecteur de DVD et la carte principale. Si l'intégrité du lecteur de DVD est critique, le serveur ne peut pas accéder au lecteur de DVD.

REMARQUE : La fonction d'association de lecteur de DVD figure dans l'écran Menu principal de l'écran LCD uniquement si vous avez installé un lecteur de DVD.

Menu Boîtier

Cet écran vous permet de naviguer vers les écrans suivants :

- **État de la face avant**
- **État à l'arrière**
- **État latéral**
- **État du boîtier**

Utilisez les boutons de navigation pour mettre en surbrillance l'élément voulu (mettez en surbrillance l'icône **Précédent** pour revenir au **Menu principal**), puis appuyez sur le bouton central. L'écran sélectionné s'affiche.

Menu Résumé IP

L'écran **Résumé IP** affiche des informations IP sur le contrôleur CMC (IPv4 et IPv6) sur chacun des serveurs installés dans le châssis.

Utilisez les touches Haut et Bas pour passer d'une entrée de la liste à une autre. Utilisez les touches Gauche et Droite pour faire défiler les messages sélectionnés qui débordent de l'écran.

Utilisez les boutons flèche haut et bas pour sélectionner l'icône **Précédent** et appuyez sur le bouton central pour retourner au menu **Enceinte**.

Paramètres

Le menu **Paramètres** affiche un menu d'options pouvant être définies :

- **Langue de l'écran LCD** : choisissez la langue à utiliser pour afficher le texte et les messages sur l'écran LCD.
- **Orientation du châssis** : sélectionnez **Mode Tour** ou **Mode Rack** en fonction de l'orientation d'installation du châssis.
- **Ecran LCD par défaut** : sélectionnez l'écran (**Menu principal**, **Statut de police**, **Statut arrière**, **Statut latéral** ou **Personnalisé**) qui s'affiche lorsque l'écran LCD est inactif.
- **Paramètres réseau** : sélectionnez cette option pour définir les paramètres réseau d'un contrôleur CMC. Pour plus d'informations sur cette fonction, voir Configuration du réseau CMC à l'aide de l'interface de l'écran LCD.

Utilisez les boutons fléchés Haut et Bas pour mettre un élément en surbrillance dans le menu ou mettez en surbrillance l'icône **Précédent** pour revenir au **menu principal**.

Pour activer votre sélection, appuyez sur le bouton central.

Langue de l'écran LCD

L'écran **Langue de l'écran LCD** permet de choisir la langue utilisée pour les messages de l'écran LCD. La langue actuellement active est mise en surbrillance sur fond bleu clair.

1. Utilisez les boutons flèche haut, bas, gauche et droite pour mettre la langue souhaitée en surbrillance.
2. Appuyez sur le bouton central. L'icône **Accepter** s'affiche et est mise en surbrillance.
3. Appuyez sur le bouton central pour confirmer la modification. Le menu **Configuration de l'écran LCD** s'affiche.

Écran par défaut

La zone **Écran par défaut** vous permet de modifier l'écran que le panneau LCD affiche en l'absence de toute activité. L'écran par défaut défini en usine est l'écran **Menu principal**. Vous pouvez choisir d'afficher l'un des écrans suivants :

- **Menu principal**
- **État de la face avant** (vue graphique de la face avant du châssis)
- **État de la face arrière** (vue graphique de la face arrière du châssis)
- **État du côté** (vue graphique du côté gauche du châssis)
- **Personnalisé** (logo Dell avec le nom du châssis)

L'écran par défaut actif est mis en surbrillance en bleu clair.

1. Utilisez les boutons fléchés Haut et Bas pour mettre en surbrillance l'écran à définir comme écran par défaut.
2. Appuyez sur le bouton central. L'icône **Accepter** est mise en surbrillance.
3. Appuyez de nouveau sur le bouton central pour confirmer la modification. L'**écran par défaut** s'affiche.

Diagnostics

L'écran LCD vous aide à diagnostiquer les problèmes d'un serveur ou d'un module dans le châssis. En cas de problème ou d'échec dans le châssis, ou au niveau d'un serveur ou d'un autre module du châssis, le voyant orange d'état de l'écran LCD clignote. Dans le **menu**

principal, une icône sur fond orange s'affiche en regard de l'option de menu (Boîtier) pour indiquer l'état de l'avant, de l'arrière, du côté ou du boîtier.

En suivant les icônes orange dans tout le système de menus de l'écran LCD, vous pouvez afficher l'écran d'état et les messages d'erreur de l'élément défaillant.

Vous pouvez supprimer les messages d'erreur de l'écran LCD en retirant le module ou le serveur à l'origine du problème ou bien en effaçant le journal du matériel du module ou du serveur. Pour les erreurs de serveur, utilisez l'interface Web iDRAC ou l'interface de ligne de commande (CLI) iDRAC pour effacer le journal d'événements système du serveur. Pour les erreurs de châssis, utilisez l'interface Web ou l'interface CLI CMC pour effacer le journal du matériel.

Message de l'écran LCD du panneau avant

Cette section contient deux sous-sections qui répertorient les informations sur les erreurs et les conditions qui apparaissent sur le panneau avant de l'écran LCD.

Les *Messages d'erreur* de l'écran LCD présentent un format similaire à celui du journal d'événements système (SEL) affiché dans l'interface de ligne de commande (CLI) ou l'interface Web.

Les tableaux de la section traitant des erreurs répertorient les messages d'erreur et d'avertissement affichés sur les différents écrans LCD, avec la cause possible de chaque message. Le texte entre chevrons (< >) peut varier.

Les *Informations de condition* affichées sur l'écran LCD incluent des informations descriptives concernant les modules du châssis. Les tableaux de cette section décrivent les informations affichées pour chaque composant.

Informations d'état des serveurs et modules sur l'écran LCD

Les tableaux figurant dans cette section décrivent les éléments de condition qui sont affichés sur le panneau avant de l'écran LCD pour chaque type de composant dans le châssis.

Tableau 46. État du CMC

Élément	Description
Nom/Emplacement	Exemple : CMC1, CMC2
Aucune erreur	S'il n'y a pas d'erreur, le message Aucune erreur s'affiche. Dans le cas contraire, les messages d'erreur sont répertoriés, les messages essentiels étant répertoriés en premier, suivis des messages auxquels sont reliés des avertissements.
Version du micrologiciel	S'affiche uniquement sur un CMC actif. Affiche Auxiliaire pour le CMC de secours.
IP4 <activée, désactivée>	Affiche la condition activée de l'IPv4 actuel uniquement sur un CMC actif.
Adresse IP4 : <adresse, en cours d'acquisition>	Ne s'affiche que si l'IPv4 est activée sur un CMC actif uniquement.
IP6 <activée, désactivée>	Affiche état actuel d'activation IPv6, uniquement pour le CMC actif.
Adresse locale IP6 : <adresse>	S'affiche uniquement si IPv6 est activé, uniquement sur le CMC actif.
MAC: <adresse>	Affiche l'adresse MAC du CMC.

Tableau 47. Condition du châssis ou de l'enceinte

Élément	Description
Nom défini par l'utilisateur	Exemple : « Système de rack Dell ». Ceci peut être configuré à l'aide de l'interface de ligne de commande ou de l'interface Web CMC.
Messages d'erreur	S'il n'y a pas d'erreur, le message Aucune erreur s'affiche. Dans le cas contraire, les messages d'erreur sont répertoriés, les messages essentiels étant répertoriés en premier, suivis des messages auxquels sont reliés des avertissements.
Numéro de modèle	Exemple « PowerEdgeM1000 »

Tableau 47. Condition du châssis ou de l'enceinte (suite)

Élément	Description
Consommation énergétique	Consommation électrique en watts
Alimentation de crête	Consommation électrique maximale en watts
Alimentation minimale	Consommation électrique minimale en watts
Température ambiante	Température ambiante en degrés Celsius
Numéro de service	Le numéro de service attribué par l'usine.
Mode de redondance de CMC	Non redondant ou redondant
Mode de redondance de l'unité d'alimentation	Non redondant, redondant en CA ou redondant en CC

Tableau 48. Condition du ventilateur

Élément	Description
Nom/Emplacement	Exemple : Ventilateur1, Ventilateur2, ainsi de suite.
Messages d'erreur	S'il n'y a pas d'erreur, le message Aucune erreur s'affiche. Dans le cas contraire, les messages d'erreur sont répertoriés, les messages essentiels étant répertoriés en premier, suivis des messages auxquels sont reliés des avertissements.
RPM	Vitesse actuelle du ventilateur en tr/min

Tableau 49. État PSU

Élément	Description
Nom/Emplacement	Exemple : PSU1, PSU2, ainsi de suite.
Messages d'erreur	S'il n'y a pas d'erreur, le message Aucune erreur s'affiche. Dans le cas contraire, les messages d'erreur sont répertoriés, les messages essentiels étant répertoriés en premier, suivis des messages auxquels sont reliés des avertissements.
État	Hors ligne, En ligne ou De secours : indique l'état de l'alimentation d'une unité d'alimentation.
Puissance maximale	Puissance maximale que l'unité d'alimentation peut fournir au système

Tableau 50. Condition du module d'E/S

Élément	Description
Nom/Emplacement	IOM A
Messages d'erreur	S'il n'y a pas d'erreur, le message Aucune erreur s'affiche. Dans le cas contraire, les messages d'erreur sont répertoriés, les messages essentiels étant répertoriés en premier, suivis des messages auxquels sont reliés des avertissements.
État	Off (Désactivé) ou On (Activé) : indique si le module d'E/S est opérationnel.
Modèle	Modèle du module d'E/S
Type de structure	Type de mise en réseau
Adresse IP	S'affiche uniquement si le module d'E/S est activé. Cette valeur est égale à zéro pour un module d'E/S d'intercommunication.
Numéro de service	Le numéro de service attribué par l'usine.

Tableau 51. État d'adressage de KVM

Élément	Description
Serveur <numéro>	Affiche la liste des serveurs auxquels le KVM peut être adressé.

Tableau 51. État d'adressage de KVM (suite)

Élément	Description
Messages d'erreur	S'il n'y a pas d'erreur, le message Aucune erreur s'affiche. Dans le cas contraire, les messages d'erreur sont répertoriés, les messages essentiels étant répertoriés en premier, suivis des messages auxquels sont reliés des avertissements.
Adressé	Affiche la liste des serveurs adressés à un KVM, le cas échéant.
Logement <numéro>	Indique le logement de serveur auquel le KVM est mappé. Les valeurs possibles sont LOGEMENTS *<01 à 04>*.
Désadressé	S'affiche si le commutateur KVM n'est adressé à aucun des serveurs.

Tableau 52. État d'adressage de DVD

Élément	Description
Serveur <numéro>	Affiche la liste des serveurs auxquels le DVD peut être adressé.
Messages d'erreur	S'il n'y a pas d'erreur, le message Aucune erreur s'affiche. Dans le cas contraire, les messages d'erreur sont répertoriés, les messages essentiels étant répertoriés en premier, suivis des messages auxquels sont reliés des avertissements.
Adressé	Affiche la liste des serveurs adressés à un DVD, le cas échéant.
Logement <numéro>	Indique le logement de serveur auquel le DVD est mappé. Les valeurs possibles sont LOGEMENTS *<01 à 04>*.
Désadressé	S'affiche si le commutateur KVM n'est adressé à aucun des serveurs.

Tableau 53. Condition du ventilateur

Élément	Description
Nom/Emplacement	Exemple : Blower1, Blower2, et ainsi de suite.
Messages d'erreur	S'il n'y a pas d'erreur, le message Aucune erreur s'affiche. Dans le cas contraire, les messages d'erreur sont répertoriés, les messages essentiels étant répertoriés en premier, suivis des messages auxquels sont reliés des avertissements.
RPM	Vitesse actuelle du ventilateur en tr/min

Tableau 54. État SPERC

Élément	Description
SPERC : <numéro>	Affiche le nom du SPERC au format SPERC n, où « n » correspond au numéro du SPERC. Par exemple : SPERC 1, SPERC 2, etc.
Messages d'erreur	S'il n'y a pas d'erreur, le message Aucune erreur s'affiche. Dans le cas contraire, les messages d'erreur sont répertoriés, les messages essentiels étant répertoriés en premier, suivis des messages auxquels sont reliés des avertissements.
État de fonctionnement	On (Activé) ou Off (Désactivé) : indique si le SPERC fonctionne.
Nom : <nom>	Nom du PERC partagé. Exemple : SPERC
État d'intégrité	Ok
Version du micrologiciel	Version SPERC
Manufacturer	Nom du fabricant
État	Hors ligne, en ligne ou De secours : indique l'état de l'alimentation d'un SPERC.

Tableau 55. État de la carte PCIe

Élément	Description
Carte PCIe <*numéro*>	Affiche le nom de la carte PCIe au format Carte PCIe <*n*>, où « n » correspond au numéro de la carte PCIe. Exemple : Carte PCIe 1, Carte PCIe 2, etc.
Messages d'erreur	S'il n'y a pas d'erreur, le message Aucune erreur s'affiche. Dans le cas contraire, les messages d'erreur sont répertoriés, les messages essentiels étant répertoriés en premier, suivis des messages auxquels sont reliés des avertissements.
État de fonctionnement	On (Activé) ou Off (Désactivé) : indique si la carte PCIe fonctionne.
Nom : <nom>	Nom de la carte PCIe.
Adressé à un serveur	Adressé ou Désadressé.

Tableau 56. État du lecteur de disque dur

Élément	Description
Disque dur : <numéro>	Affiche le nom du disque dur au format Lecteur de disque dur <*n*>, où « n » correspond au numéro du disque dur. Exemple : Lecteur de disque dur 1, Lecteur de disque dur 2, etc.
Messages d'erreur	S'il n'y a pas d'erreur, le message Aucune erreur s'affiche. Dans le cas contraire, les messages d'erreur sont répertoriés, les messages essentiels étant répertoriés en premier, suivis des messages auxquels sont reliés des avertissements.
État de l'alimentation	En rotation accélérée, Transition, ou En rotation réduite : indique l'état de l'alimentation d'un lecteur de disque dur
Manufacturer	Nom du fabricant
Capacité	Capacité de stockage disponible du lecteur de disque dur en gigaoctets (Go)
Version du micrologiciel	Affiche la version du micrologiciel du lecteur de disque.
État	Hors ligne, En ligne ou De secours : indique l'état de l'alimentation du disque dur.

Tableau 57. État du serveur

Élément	Description
Nom/ Emplacement	Exemple : Serveur1, Serveur2, et ainsi de suite.
Aucune erreur	S'il n'y a pas d'erreur, le message Aucune erreur s'affiche. Dans le cas contraire, les messages d'erreur sont répertoriés, les messages essentiels étant répertoriés en premier, suivis des messages auxquels sont reliés des avertissements. Pour plus d'informations, consultez « Messages d'erreur LCD ».
Nom du logement	Nom de logement du châssis. Par exemple, LOGEMENT-01. **REMARQUE : Ce tableau est configurable via l'interface de ligne de commande ou l'interface Web du CMC.**
Numéro de modèle	S'affiche si iDRAC a fini de démarrer.
Numéro de service	S'affiche si iDRAC a fini de démarrer.
Version du BIOS	Version micrologicielle du BIOS du serveur.
Nom DNS d'iDRAC	Affiche le nom DNS du serveur iDRAC.
Dernier code POST	Affiche la dernière chaîne de messages du code POST du BIOS du serveur.

Tableau 57. État du serveur (suite)

Élément	Description
Version du micrologiciel iDRAC	S'affiche si iDRAC a fini de démarrer. **REMARQUE : iDRAC version 1.01 s'affiche sous la forme 1.1. Il n'y a pas d'iDRAC version 1.10.**
IP4 <activée, désactivée>	Affiche la condition activée de l'IPv4.
Adresse IP4 : <adresse, en cours d'acquisition>	S'affiche uniquement si l'IPv4 est activée.
IP6 <activée, désactivée>	S'affiche uniquement si l'iDRAC prend en charge IPv6. Affiche l'état activé de l'IPv6.
Adresse locale IP6 : <adresse>	S'affiche uniquement si l'iDRAC prend en charge IPv6 et si IPv6 est activée.
Adresse globale IP6 : <adresse>	S'affiche uniquement si l'iDRAC prend en charge IPv6 et si IPv6 est activée.
FlexAddress activée sur les structures	S'affiche uniquement si la fonctionnalité est installée. Répertorie les structures activées pour ce serveur (c'est-à-dire, A, B, C).
État de la détection automatique	Affiche l'état de la détection automatique du serveur.

Les informations de la table sont mises à jour de façon dynamique. Si le serveur ne prend pas en charge cette fonctionnalité, les informations suivantes ne s'affichent pas. Sinon, les options Server Administrator sont les suivantes :

- Option « Aucune » = Aucune chaîne ne doit être affichée sur l'écran LCD.
- Option « Par défaut » = Aucun effet.
- Option « Personnalisé » = Vous permet d'entrer un nom de chaîne pour le serveur.

Les informations s'affichent uniquement si le démarrage de l'iDRAC est terminé. Pour plus d'informations sur cette fonctionnalité, consultez le *Guide de référence de la ligne de commande RACADM pour CMC dans PowerEdge VRTX*.

19

Questions fréquemment posées

Cette section répertorie les questions courantes sur les éléments suivants :

- RACADM
- Gestion et restauration d'un système distant
- Active Directory
- FlexAddress et FlexAddressPlus
- Modules d'E/S

Sujets :

RACADM

Après réinitialisation du CMC (avec la sous-commande RACADM racreset), lorsque vous entrez une commande, le message suivant s'affiche :

```
racadm <subcommand> Transport: ERROR: (RC=-1)
```

Qu'est-ce que ce message signifie ?

Vous devez attendre la fin de la réinitialisation du CMC avant d'émettre une autre commande.

L'utilisation de sous-commandes RACADM génère parfois une ou plusieurs des erreurs suivantes :

- Messages d'erreur locaux : problèmes tels que erreurs de syntaxe, erreurs typographiques et noms incorrects. Exemple : `ERROR: <message>`

  Utilisez la sous-commande RACADM `help` pour afficher la syntaxe correcte et les informations d'utilisation. Par exemple, si l'effacement du journal du châssis génère une erreur, exécutez la sous-commande suivante.

  ```
  racadm chassislog help clear
  ```

- Messages d'erreurs du contrôleur CMC : problèmes pour lesquels le contrôleur CMC ne peut pas exécuter une action. Le message d'erreur suivant s'affiche.

  ```
  racadm command failed.
  ```

Pour afficher des informations sur un châssis, entrez la commande suivante :

```
racadm gettracelog
```

Lorsque vous utilisez le micrologiciel RACADM, l'invite devient « > » et le caractère d'invite « $ » n'est plus affiché.

Si vous entrez des guillemets (") dépareillés ou une apostrophe (') isolée dans la commande, l'interface de ligne de commande (CLI) bascule vers l'invite « > » et met toutes les commandes en file d'attente.

Pour revenir à l'invite « $ », entrez <Ctrl>–d.

Le message d'erreur `Not Found` s'affiche lorsque vous utilisez les commandes `logout $` et `$ quit`.

Gestion et restauration d'un système distant

L'interface distante RACADM et les services Web ne sont plus disponibles lorsqu'une propriété est modifiée. Pourquoi ?

Il peut s'écouler une minute avant que les services RACADM à distance et l'interface Web ne redeviennent disponibles après la réinitialisation du serveur Web CMC.

Le serveur Web CMC est réinitialisé dans les cas suivants :

- Modification de la configuration réseau ou des propriétés de sécurité réseau à l'aide de l'interface utilisateur Web CMC.
- Modification de la propriété cfgRacTuneHttpsPort (y compris à l'aide de la commande « config -f <fichier de configuration> »).
- Utilisation de la commande `racresetcfg` ou restauration de la sauvegarde d'une configuration de châssis.
- Vous réinitialisez CMC.
- Un nouveau certificat de serveur SSL est téléchargé.

Le serveur DNS n'enregistre pas le contrôleur CMC.

Certains serveurs DNS enregistrent uniquement les noms qui ne dépassent pas 31 caractères.

Lors de l'accès à l'interface Web CMC, un avertissement de sécurité signale que le certificat SSL a été émis par une autorité de certification (CA) qui n'est pas de confiance.

Le contrôleur CMC contient un certificat de serveur CMC par défaut qui permet d'assurer la sécurité du réseau pour les fonctions de l'interface Web et de l'interface RACADM distante. Ce certificat n'est pas émis par une autorité de certification de confiance. Pour résoudre ce problème de sécurité, téléversez un certificat de serveur CMC émis par une autorité de certification de confiance (telle que Thawte ou Verisign).

Pourquoi le message suivant s'affiche-t-il pour des raisons inconnues ?

Remote Access: SNMP Authentication Failure

Au cours de la détection, IT Assistant tente de vérifier les valeurs d'obtention (**get**) et de définition (**set**) du nom de communauté du périphérique. Dans IT Assistant, **get community name = public** et **set community name = private**. Par défaut, le nom de communauté de l'agent CMC est public. Lorsqu'IT Assistant envoie une requête de définition (set), l'agent CMC génère une erreur d'authentification SNMP car il accepte uniquement les requêtes provenant de **community = public**.

Modifiez le nom de communauté CMC avec RACADM. Pour afficher le nom de communauté CMC, utilisez la commande suivante :

```
racadm getconfig -g cfgOobSnmp
```

Pour définir le nom de communauté CMC, utilisez la commande suivante :

```
racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <community name>
```

Pour interdire la génération des interruptions d'authentification SNMP, entrez des noms de communauté acceptés par l'agent. Comme CMC accepte un seul nom de communauté, entrez les mêmes noms de communauté pour les commandes get et set dans la configuration de détection IT Assistant.

Lors de l'accès à l'interface Web CMC, un avertissement de sécurité s'affiche et indique que le nom d'hôte du certificat SSL ne correspond pas au nom d'hôte CMC.

Le contrôleur CMC contient un certificat de serveur CMC par défaut qui permet d'assurer la sécurité du réseau pour les fonctions de l'interface Web et de l'interface RACADM distante. Lorsque vous utilisez ce certificat, le navigateur Web affiche un avertissement de sécurité si le certificat par défaut ne correspond pas au nom d'hôte du contrôleur CMC (l'adresse IP, par exemple).

Pour résoudre ce problème de sécurité, téléversez un certificat de serveur CMC émis pour l'adresse IP de CMC. Lorsque vous générez la requête de signature de certificat (RSC) à utiliser pour l'émission du certificat, assurez-vous que le nom commun (CN) de la CSR correspond à l'adresse IP CMC (par exemple, 192.168.0.120) ou au nom DNS CMC enregistré.

Afin de vous assurer que la RSC correspond au nom de DNS CMC enregistré :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis.**
2. Cliquez sur **Réseau**.
   La page **Configuration réseau** s'affiche.
3. Sélectionnez l'option **Enregistrer le contrôleur CMC dans DNS**.
4. Entrez le nom d'un contrôleur CMC dans le champ **Nom CMC DNS**.
5. Cliquez sur **Appliquer les changements**.

Active Directory

Active Directory prend-il en charge la connexion CMC sur plusieurs arborescences ?

Oui. L'algorithme de requête Active Directory de CMC prend en charge plusieurs arborescences d'une même forêt.

La connexion à CMC avec Active Directory est-elle possible en mode mixte (avec les contrôleurs de domaine de la forêt exécutant des systèmes d'exploitation différents, comme Microsoft Windows 2000 ou Windows Server 2003) ?

Oui. En mode mixte, tous les objets utilisés par le processus de requête CMC (utilisateur, objet Périphérique RAC et objet Association) doivent être dans le même domaine.

Le snap-in Utilisateurs et ordinateurs Active Directory étendu par Dell vérifie le mode et limite les utilisateurs pour créer des objets dans les domaines en mode mixte.

L'utilisation de CMC avec Active Directory permet-elle de prendre en charge des environnements avec plusieurs domaines ?

Oui. Le niveau de la fonction de forêt de domaines doit être en mode natif ou en mode Windows 2003. De plus, les groupes Objet Association, Objets Utilisateur RAC et Objets Périphérique RAC (y compris l'objet Association) doivent être des groupes universels.

Ces objets étendus pour Dell (objets Association Dell, Périphériques RAC Dell et Privilèges Dell) peuvent-ils appartenir à différents domaines ?

L'objet Association et l'objet Privilège doivent être dans le même domaine. Le snap-in d'extension Dell Utilisateurs et ordinateurs Active Directory vous permet de créer ces deux objets uniquement dans le même domaine. Les autres objets peuvent appartenir à des domaines différents.

Y a-t-il des restrictions concernant la configuration SSL du contrôleur de domaine ?

Oui. Tous les certificats SSL des serveurs Active Directory de la forêt doivent être signés par le même certificat signé par l'autorité de certification (CA) racine, car CMC ne vous permet de téléverser qu'un seul certificat SSL signé par une autorité de certification de confiance.

L'interface Web ne se lance pas après la création et le téléversement d'un nouveau certificat RAC.

Si vous utilisez les services de certificats Microsoft pour générer le certificat RAC, l'option Certificat utilisateur a peut-être été utilisée au lieu de l'option Certificat Web lors de la création du certificat.

Pour résoudre le problème, générez une requête de signature de certificat (RSC), créez un certificat Web depuis les services de certificats Microsoft, puis téléversez-le en exécutant les commandes RACADM suivantes :

```
racadm sslcsrgen [-g] [-f {filename}]
```

```
racadm sslcertupload -t 1 -f {web_sslcert}
```

FlexAddress et FlexAddressPlus

Que se passe-t-il si une carte de fonction est retirée ?

Il ne se produit aucun changement visible si vous retirez une carte de fonction. Vous pouvez retirer les cartes de fonction pour les stocker ou les laisser en place.

Que se passe-t-il si une carte de fonction utilisée dans un châssis est retirée et insérée dans un autre châssis ?

L'interface Web affiche le message d'erreur suivant :

```
This feature card was activated with a different chassis. It must be removed before accessing
the FlexAddress feature.
```

```
Current Chassis Service Tag = XXXXXXXX
```

```
Feature Card Chassis Service Tag = YYYYYYYY
```

```
An entry is added to the CMC log that states:
```

```
cmc <date timestamp> : feature 'FlexAddress@YYYYYYYY' not activated; chassis ID='XXXXXXXX'
```

Que se passe-t-il si la carte de fonction est retirée et qu'une carte non FlexAddress est installée ?

Cette carte n'est ni activée, ni modifiée. La carte est ignorée par CMC. Dans ce cas, la commande **$racadm featurecard -s** renvoie le message suivant :

```
No feature card inserted
```

```
ERROR: can't open file
```

Que se passe-t-il si une carte de fonction est liée à un châssis dont le numéro de service est reprogrammé ?

- Si la carte de fonction d'origine figure dans le contrôleur CMC actif sur ce châssis ou sur un autre châssis, l'interface Web affiche le message d'erreur suivant :
  - `This feature card was activated with a different chassis. It must be removed before accessing the FlexAddress feature.`

- Current Chassis Service Tag = XXXXXXXX
- Feature Card Chassis Service Tag = YYYYYYYY

  La carte de fonction d'origine ne peut plus être désactivée sur ce châssis ou sur un autre châssis, à moins que l'assistance Dell ne reprogramme le numéro de service du châssis d'origine dans un châssis et que le contrôleur CMC sur lequel est installée la carte de fonction d'origine devienne actif sur ce châssis.
- La fonction FlexAddress reste activée dans le châssis initialement lié. La valeur de liaison de cette fonction de châssis est mise à jour pour refléter le nouveau numéro de service.

Un message d'erreur s'affiche-t-il si deux cartes de fonction sont installées dans un système à CMC redondants ?

La carte de fonction du contrôleur CMC actif est active et installée dans le châssis. Le contrôleur CMC ignore la deuxième carte.

La carte SD dispose-t-elle d'un verrou de protection en écriture ?

Oui. Avant d'installer la carte SD dans le module CMC, vérifiez que son clapet de protection en écriture est en position déverrouillée. La fonction FlexAddress ne peut pas être activée si la carte SD est protégée en écriture. Dans ce cas, la commande **$racadm feature -s** renvoie le message suivant :

```
No features active on the chassis. ERROR: read only file system
```

Que se passe-t-il si aucune carte SD n'est présente dans le module CMC actif ?

La commande **$racadm featurecard -s** renvoie le message suivant :

```
No feature card inserted.
```

Que devient la fonction FlexAddress si le BIOS du serveur est mis à jour de la version 1.xx vers la version 2.xx ?

Vous devez mettre hors tension le module serveur pour pouvoir l'utiliser avec FlexAddress. Une fois la mise à jour du BIOS du serveur terminée, le module serveur ne reçoit aucune adresse attribuée par le châssis tant que vous n'avez pas réalisé un cycle d'alimentation.

Comment restaurer une carte SD si cette carte n'était pas dans le châssis lorsque la commande de désactivation a été exécutée dans FlexAddress ?

Le problème réside dans le fait qu'il est impossible d'utiliser la carte SD pour installer FlexAddress sur un autre châssis si cette carte n'était pas dans le contrôleur CMC lors de la désactivation de FlexAddress. Pour que la carte fonctionne à nouveau, insérez-la de nouveau dans un contrôleur CMC du châssis auquel elle est liée, réinstallez FlexAddress, puis désactivez à nouveau FlexAddress.

La carte SD est correctement installée et toutes les mises à jour de micrologiciel/logiciel ont été réalisées. La fonction FlexAddress est active, mais l'écran de déploiement de serveur n'affiche aucune option pour déployer cette fonction. Que se passe-t-il ?

Il s'agit d'un problème de mise en mémoire cache du navigateur. Déconnectez-vous du navigateur et relancez-le.

Que devient FlexAddress si je dois réinitialiser la configuration du châssis avec la commande RACADM racresetcfg?

La fonction FlexAddress est quand même activée et prête à l'emploi. Par défaut, toutes les structures et tous les logements sont sélectionnés.

REMARQUE : Il est vivement recommandé de mettre hors tension le châssis avant d'exécuter la commande RACADM racresetcfg.

Après avoir désactivé uniquement la fonction FlexAddressPlus (FlexAddress est toujours actif), la commande racadm setflexaddr échoue sur le contrôleur CMC (encore actif). Pourquoi ?

Si le contrôleur CMC est activé par la suite alors que la carte de fonction FlexAddressPlus est toujours dans son logement, la fonction FlexAddressPlus est réactivée et les modifications de configuration de logement/structure flexaddress peuvent se poursuivre.

Module d'E/S (IOM)

Après un changement de configuration, le CMC affiche parfois l'adresse IP 0.0.0.0.

Cliquez sur l'icône **Actualiser** pour déterminer si l'adresse IP est correctement définie sur le commutateur. Si vous faites une erreur en définissant l'adresse IP/le masque/la passerelle, le commutateur ne définit pas l'adresse IP et renvoie 0.0.0.0 dans tous les champs.

Erreurs les plus courantes :

- Les adresses IP de gestion hors bande et intrabande sont identiques ou configurées sur le même réseau.
- Le masque de sous-réseau n'est pas valide.
- La passerelle par défaut est définie vers une adresse qui ne se trouve pas sur un réseau, mais est connectée directement au commutateur.