Dell Chassis Management Controller version 2.0 pour PowerEdge FX2 et FX2s

Guide de l'utilisateur

Septembre 2017
Rév. A01

Remarques, précautions et avertissements

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

PRÉCAUTION : Une PRÉCAUTION indique un risque d'endommagement du matériel ou de perte de données et vous indique comment éviter le problème.

AVERTISSEMENT : Un AVERTISSEMENT indique un risque d'endommagement du matériel, de blessures corporelles ou même de mort.

Table des matières

1

Présentation

Le contrôleur Dell Chassis Management Controller (CMC) pour Dell EMC PowerEdge FX2/FX2s est une solution matérielle et logicielle de gestion de systèmes pour châssis **PowerEdge FX2/FX2s**. Le contrôleur CMC dispose de son propre microprocesseur et de sa propre mémoire ; il est alimenté par le châssis modulaire sur lequel il est raccordé.

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

- Afficher l'inventaire.
- Exécuter des tâches de configuration et de surveillance.
- Mettre sous tension ou hors tension à distance le châssis et les serveurs.
- Activer les alertes pour les événements des serveurs et des composants du module de serveur.
- Afficher les informations de mappage PCIe et réattribuer des emplacements PCIe.
- Fournir une interface de gestion un à plusieurs avec les modules iDRAC et les modules E/S du châssis.

Le contrôleur CMC fournit plusieurs fonctions de gestion de système pour serveurs. Ainsi la gestion de l'alimentation et la gestion thermique s'inscrivent parmi les principales fonctions du contrôleur CMC, lesquelles sont répertoriées ci-dessous :

- Gestion automatique des températures et de la consommation au niveau du châssis et en temps réel.
  - Le module 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 d'enceinte facultative (limitation de la puissance d'entrée du système) qui envoie des alertes et exécute des actions, telles que limiter la consommation électrique des serveurs et bloquer la mise sous tension des nouveaux serveurs, pour maintenir l'enceinte dans la limite de puissance maximale définie.
  - Le CMC surveille et contrôle automatiquement le fonctionnement des ventilateurs en se basant sur la mesure en temps réel des températures ambiantes et internes.
  - Le contrôleur CMC offre des fonctions complètes d'inventaire et de consignation des erreurs ou des états.
- Le contrôleur CMC permet de centraliser la configuration des paramètres suivants :
  - Réseau et sécurité de l'enceinte Dell PowerEdge FX2/FX2s.
  - 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. Si nécessaire, le contrôleur CMC désactive également les composants afin de protéger le matériel du système.
  - Sécurité des accès utilisateur
  - Logements PCIe

Vous pouvez configurer le CMC pour qu'il envoie des alertes par e-mail ou par interruption SNMP lorsque des erreurs ou des avertissements surviennent concernant par exemple la température, une configuration matérielle incorrecte, une panne de courant ou la vitesse des ventilateurs.

REMARQUE : Les termes « traîneau de stockage » et « module de stockage » sont utilisés indifféremment dans ce document.

Sujets :

- Autres documents utiles
- Accès au contenu de support à partir du site de support Dell EMC

Principales fonctions

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

Nouveautés de cette version

Cette version de contrôleur CMC pour Dell EMC PowerEdge FX2/FX2s prend en charge :

- L'affichage des informations relatives à la vitesse et la température du ventilateur à l'aide de la commande WSMan.
- L'intégration du daemon opensource LLDP afin de transmettre les paquets LLDP au contrôleur iDRAC via un réseau VLAN.
- Le transfert des dumplogs CMC au contrôleur iDRAC.
- L'utilisation de la carte mezzanine PCIe retimer.
- L'utilisation de l'option Fault Tolerant Redundancy (FTR, Redondance pour tolérance aux pannes) permettant l'ajout d'alimentation.

Fonctions de gestion

Le contrôleur CMC offre les fonctionnalités de gestion suivantes :

- Enregistrement DDNS (Système de noms de domaine dynamique) pour IPv4 et IPv6
- Gestion des connexions et configuration des utilisateurs locaux, Active Directory et LDAP.
- Gestion et surveillance à distance du système à l'aide de SNMP, d'une interface Web, d'un KVM intégré 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, des traîneaux de stockage et de l'infrastructure du châssis.
- Mise à jour micrologicielle des composants des serveurs, tels que le BIOS et les contrôleurs de réseau 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
- Adaptation d'un traîneau à plusieurs nœuds. Le PowerEdge FM120x4 est un traîneau à plusieurs nœuds.
- Surveillance de la consommation maximale du châssis.
- prise en charge de la fonction de l'identité d'E/S de l'iDRAC pour un inventaire d'adresses WWN/MAC.
- Fonctionnalité FlexAddress : remplace les ID de nom WWN/MAC (World Wide Name/Media Access Control, nom universel/contrôle de l'accès aux supports) définis en usine par les ID WWN/MAC attribués par le châssis pour un emplacement spécifique, mise à niveau facultative.
- Affichage graphique de l'état et de l'intégrité des composants de châssis
- Prise en charge des serveurs à connecteur unique ou multiple
- 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
- Gestion de plusieurs châssis. Celle-ci permet à jusqu'à 19 autres châssis d'être visibles depuis le châssis maître.

  REMARQUE : La gestion multi-châssis n'est pas prise en charge sur les réseaux IPv6.
- Fonctionnalité du proxy RACADM d'iDRAC local et distant permettant de gérer les traîneaux de stockage dans le châssis FX2s.

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
- Image signé par CMC : utilisé pour protéger l'image du micrologiciel à partir de la modification non détectée à l'aide de la signature numérique.

Présentation du châssis

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.

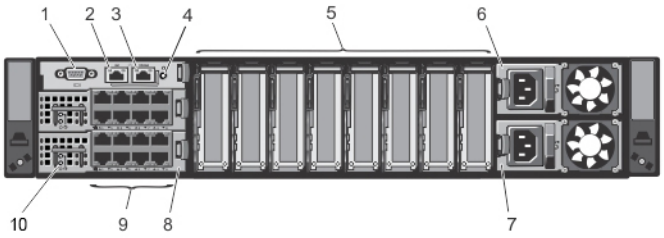


Figure 1. Panneau arrière du châssis

Tableau 1. Panneau arrière du châssis : composants

Élément	Voyant, bouton ou connecteur
1	Connecteur série
2	connecteur Ethernet GB1
3	Connecteur Ethernet STK/Gb2 (pile)
4	Bouton d'identification du système
5	Logements d'extension PCIe mi-hauteur
6	Bloc d'alimentation (PSU1)
7	Bloc d'alimentation (PSU2)
8	Module d'E/S (2)

Tableau 1. Panneau arrière du châssis : composants (suite)

Élément	Voyant, bouton ou connecteur
9	Ports de module E/S
10	Voyants du module d'E/S

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.

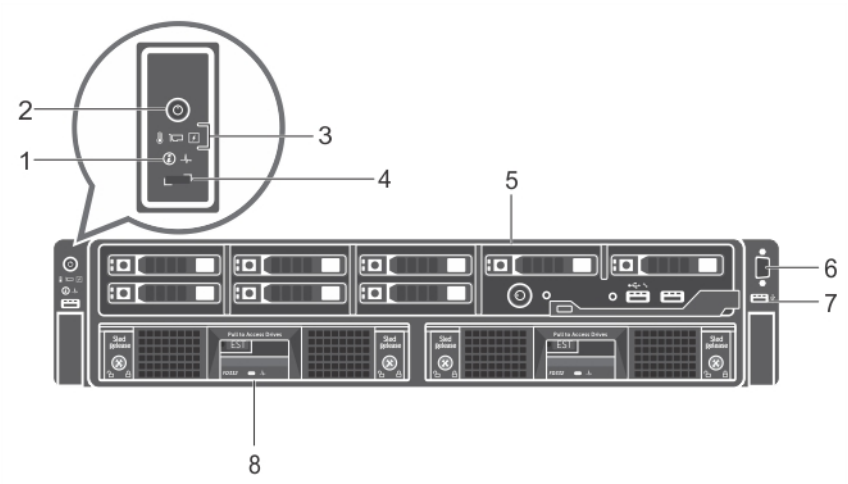


Figure 2. Panneau avant du châssis

Tableau 2. Panneau avant du châssis : composants

Élément	Voyant, bouton ou connecteur
1	Bouton d'identification du système
2	Voyant de mise sous tension, bouton d'alimentation de boîtier
3	Voyants de diagnostic
4	Bouton de sélection KVM
5	Traîneau de calcul
6	Connecteur vidéo
7	Connecteur USB
8	Traîneau de stockage

Connexions d'accès distant prises en charge

Le tableau suivant répertorie les connexions d'accès distant prises en charge.

Tableau 3. Connexions d'accès distant prises en charge

Connexion	Fonctionnalités
Ports d'interface réseau CMC	• Ports Gb : interface réseau dédiée pour l'interface Web CMC. Le CMC dispose de deux ports RJ-45 Ethernet : ○ Gb1 (le port de données sortantes)

Tableau 3. Connexions d'accès distant prises en charge (suite)

Connexion	Fonctionnalités
	○ Gb2 (le port d'empilage ou de consolidation des câbles). Le port STK/Gb2 peut également être utilisé pour le basculement de la carte réseau du CMC. **REMARQUE :** Pour implémenter le basculement de la carte réseau, vérifiez que le CMC est modifié pour passer du paramètre par défaut **Empilage** au paramètre **Redondant**. **PRÉCAUTION : La connexion du port STK/Gb2 au réseau de gestion peut provoquer des résultats imprévisibles si la configuration du contrôleur CMC n'est pas modifiée en remplaçant le paramètre par défaut Empilage par le paramètre Redondant afin d'implémenter le basculement de la carte réseau. Avec le mode par défaut Empilage, le câblage des ports Gb1 et STK/Gb2 au même réseau (domaine de diffusion) peut provoquer une perturbation importante de la diffusion (broadcast storm). Un broadcast storm peut également se produire si la configuration du contrôleur CMC est basculée en mode Redondance alors qu'en mode Empilage le câblage des châssis est réalisé en série. Vérifiez que le modèle de câblage correspond à la configuration du contrôleur CMC nécessaire à l'utilisation prévue.** ● Prise en charge de DHCP ● Interruptions SNMP et notifications d'événements par e-mail ● Interface réseau pour le firmware 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 spécifiquement 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).

Plateformes prises en charge

Le contrôleur CMC prend en charge les modèles de châssis **PowerEdge FX2** et **FX2s**. Les plateformes prises en charge sont les suivantes : PowerEdge FC430, PowerEdge FC630, PowerEdge FM120x4, PowerEdge FC830, PowerEdge FC640 et PowerEdge FD332. Pour plus d'informations sur la compatibilité avec le CMC, voir la documentation de votre périphérique.

Pour connaître les dernières plateformes prises en charge, consultez les *notes de mise à jour de Dell Chassis Management Controller (CMC) version 2.0 pour Dell PowerEdge FX2/FX2s* disponibles à l'adresse **dell.com/cmcmanuals**.

Navigateurs Web pris en charge

Pour obtenir les dernières informations sur les navigateurs web pris en charge, voir le document *Dell Chassis Management Controller (CMC) Version 2.0 for Dell PowerEdge FX2/FX2s Release Notes [Notes de mise à jour de Dell Chassis Management Controller (CMC) version 2.0 pour Dell PowerEdge FX2/FX2s]* sur le site **dell.com/support/manuals**.

- Microsoft Internet Explorer 9
- Microsoft Internet Explorer 10
- Microsoft Internet Explorer 11
- Microsoft EDGE
- Safari version 7
- Safari version 8
- Safari version 9
- Mozilla Firefox version 52
- Mozilla Firefox version 53

- Google Chrome version 57
- Google Chrome version 58

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

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

Versions micrologicielles prises en charge

Le tableau suivant répertorie les versions de micrologiciel du BIOS, d'iDRAC et du Lifecycle Controller qui prennent en charge les serveurs répertoriés :

Tableau 4. Les dernières versions de micrologiciel du BIOS, de l'iDRAC et du Lifecycle Controller

Serveurs	BIOS	iDRAC	Lifecycle Controller
PowerEdge FC830	2.2.5	2.40.40.40	2.40.40.40
PowerEdge FC630	2.2.5	2.40.40.40	2.40.40.40
PowerEdge FC430	2.2.5	2.40.40.40	2.40.40.40
PowerEdge FM120	1.5	2.40.40.40	2.40.40.40
PowerEdge FC640	1.0.0	3.10.10.10	3.10.10.10

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

Le tableau suivant répertorie les versions micrologicielles prises en charge pour les composants du serveur lorsque le micrologiciel du contrôleur CMC PowerEdge FX2/FX2s est mis à jour de la version 1.4 à la version 2.0, mais que les composants de serveur ne sont pas mis à jour à la version suivante.

Tableau 5. Versions de composants serveur pris en charge pour la mise à jour des composants serveur à la version N

Plate-forme	Composant serveur	Composant de la version précédente (Version N-1)	Version des composants mis à jour (Version N)
FD332	iDRAC	2.41.40.40	2.41.40.40
	Lifecycle Controller	2.41.40.40	2.41.40.40
FC430	iDRAC	2.41.40.40	2.50.50.50
	Lifecycle Controller	2.41.40.40	2.50.50.50
	Diagnostics	4239A33	4239A36
	BIOS	2.4.2	2.5.4
FC630	iDRAC	2.41.40.40	2.50.50.50
	Lifecycle Controller	2.41.40.40	2.50.50.50
	Diagnostics	4239A33	4239A36
	BIOS	2.4.2	2.5.4
FC830	iDRAC	2.41.40.40	2.50.50.50

Tableau 5. Versions de composants serveur pris en charge pour la mise à jour des composants serveur à la version N (suite)

Plate-forme	Composant serveur	Composant de la version précédente (Version N-1)	Version des composants mis à jour (Version N)
	Lifecycle Controller	2.41.40.40	2.50.50.50
	Diagnostics	4239A33	4239A36
	BIOS	2.4.2	2.5.4
FM120x4	iDRAC	2.41.40.40	2.50.50.50
	Lifecycle Controller	2.41.40.40	2.50.50.50
	Diagnostics	4247A1	4247A1
	BIOS	1.5.0	1.6.0
FC640	iDRAC	Sans objet	3.10.10.10
	Lifecycle Controller	Sans objet	3.10.10.10
	Diagnostics	Sans objet	4301.13 (YFXV5)
	BIOS	Sans objet	1.0.0

Adaptateurs réseau pris en charge

Le tableau suivant répertorie les adaptateurs réseau pris en charge par PowerEdge FX2/FX2s.

Tableau 6. Adaptateurs réseau pris en charge par PowerEdge FX2/FX2s

	Plateformes			
Modèle	**FC430**	**FC630**	**FC830**	**FC640**
5718 DP 1 G	Oui	Oui	Non	Oui
57810S 10 G SFP+	Non	Oui	Non	Oui
57810S 10 G BASE-T	Non	Oui	Non	Oui
5719 QP 1 G	Oui	Oui	Oui	Oui
5720 DP 1G	Oui	Non	Non	Oui
57416 DP 10G	Non	Non	Non	Oui
57414 DP 25G	Non	Non	Non	Oui
57412 DP 10G	Non	Non	Non	Oui
BCOM QP 1G	Oui	Oui	Oui	Oui
Adaptateur HBA LightPulse LPE12002 FC8	Oui	Oui	Oui	Oui
LightPulse LPe15002B-M8-D DP 8 G Gén 5	Oui	Oui	Oui	Oui
Adaptateur HBA FC16 LPe16002 double port	Oui	Oui	Oui	Oui
Adaptateur HBA LightPulse LPE12000 FC 8	Non	Oui	Oui	Oui
LightPulse LPe 15000B-M8-D SP 8 G Gén 5	Non	Oui	Oui	Oui
Adaptateur HBA LPE 16000 FC 16 un port	Non	Oui	Oui	Oui

Tableau 6. Adaptateurs réseau pris en charge par PowerEdge FX2/FX2s (suite)

	Plateformes			
Modèle	**FC430**	**FC630**	**FC830**	**FC640**
LPE 31K0 FC16 1P	Non	Oui	Oui	Oui
LPE 32002 FC32 2P	Non	Oui	Oui	Oui
LPE 31K2 FC16 2P	Oui	Oui	Oui	Oui
LPE 32000 FC32 1P	Non	Oui	Oui	Oui
Carte CNA OCe 14102-UX-D 10 GbE	Non	Non	Non	Non
Carte CNA OCe 14102-U1-D 10 GbE	Oui	Oui	Oui	Oui
Carte CNA OCe 14102-U1-D 10 GbE	Oui	Oui	Oui	Oui
X540 DP 10 G BASE-T	Oui	Oui	Oui	Oui
i350 DP 1 G	Oui	Oui	Oui	Oui
i350 QP 1 G	Oui	Oui	Oui	Oui
X520 DP 10 G SFP+	Non	Oui	Non	Oui
X710 DP 10 GBE SFP+ (Fortville)	Oui	Oui	Oui	Oui
CX3 DP 40 GbE QSFP+	Oui	Oui	Oui	Oui
CX3 DP 10 GbE DA/SFP+	Oui	Oui	Oui	Oui
CX3 MCX354–A-FCBT	Non	Non	Non	Non
Adaptateur HBA unique QLE2560 FC8	Non	Oui	Oui	Oui
578 10S 10 G BASE-T	Oui	Oui	Oui	Oui
Adaptateur HBA QLE2660 SP FC 16	Non	Oui	Oui	Oui
Adaptateur HBA QLE2662 DP FC16	Oui	Oui	Oui	Oui
QLG SFP DP 10G	Non	Non	Non	Oui
QLG BT DP 10G	Non	Non	Non	Oui
Adaptateur HBA QLE2560 FC 8	Non	Oui	Oui	Oui
QLG SFP DP 25G	Non	Non	Non	Oui
Adaptateur HBA QLE2562 FC8	Oui	Oui	Oui	Oui
Adaptateur HBA QLE2690 FC16 SP	Non	Oui	Oui	Oui
Adaptateur HBA QLE2742 FC32 SP+	Non	Oui	Oui	Oui
Adaptateur HBA QLE2740 FC32 SP	Non	Oui	Oui	Oui
Adaptateur HBA QLE2692 FC16 DP	Oui	Oui	Oui	Oui
PCIE SF852P DP 10G	Oui	Oui	Oui	Oui
INTEL OPA x16 LP	Non	Non	Oui	Oui

Gérer les licences

Les fonctionnalités CMC sont disponibles en fonction de la licence (CMC Express ou CMC Enterprise) achetée. Seules les fonctionnalités sous licence sont disponibles dans les interfaces qui permettent de configurer ou d'utiliser CMC. Par exemple, l'interface Web CMC, RACADM, WS-MAN, etc. Les fonctionnalités de mise à jour du firmware et de gestion des licences CMC sont toujours disponibles via l'interface Web CMC et RACADM.

Licences de traîneau de stockage

Vous pouvez également acheter des licences de traîneau de stockage pour gérer les contrôleurs RAID dans CMC. Les licences de traîneau de stockage peuvent être installées en usine ou achetées en ligne. Vous trouverez ci-dessous les types de licences de traîneau de stockage pris en charge :

- Un contrôleur RAID et un contrôleur HBA (RAID/HBA)
- Les deux contrôleurs RAID

Des licences de traineau de stockage peuvent être utilisées pour un ou deux contrôleurs RAID. Si une licence est attribuée à RAID sur un seul contrôleur, elle s'applique uniquement au premier contrôleur. La suppression d'une licence de traîneau de stockage peut entraîner une perte de données RAID.

Les licences de traîneau de stockage sont propres à un traîneau de stockage et sont associées au numéro de série du traîneau de stockage. Par exemple, si vous déplacez un traîneau de stockage d'un châssis à un autre, la licence est déplacée en même temps que le traîneau de stockage. Les copies principales des licences de traîneau de stockage sont stockées dans le magasin persistant. Pour plus d'informations, voir le *Guide de référence de la ligne de commande RACADM de Dell Chassis Management Controller pour PowerEdge FX2/FX2s* disponible à l'adresse **dell.com/support/manuals**.

Les messages du journal concernant toutes les activités de la licence de traîneau de stockage sont stockés dans le fichier journal du CMC.

REMARQUE : Des licences de traîneau de stockage sont requises pour modifier les contrôleurs RAID FD33xS et FD33xD du mode HBA au mode RAID.

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 permanente.

REMARQUE : Les licences d'évaluation et de site s'appliquent uniquement au contrôleur CMC.

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 en savoir plus, reportez-vous à la section Acquisition de licences et consultez le document *Guide de présentation et des fonctions* disponible à l'adresse **dell.com/support**. 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 : affiche les informations relatives à la licence actuelle du CMC et des traîneaux de stockage.
- Importer : après l'acquisition d'une licence, stockez la licence dans un emplacement de stockage local et importez-la vers 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.

  Vous pouvez également importer des licences pour les traîneaux de stockage installés dans un châssis et lorsque les traîneaux de stockage sont hors tension. Si vous disposez déjà d'une licence pour un traîneau de stockage, supprimez la licence existante avant

d'importer la nouvelle licence. La licence importée est stockée dans le gestionnaire de licences CMC et dans le magasin de traîneaux de stockage persistant. Les fonctions sous licence sont uniquement disponibles si le RAID est réinitialisé lors du redémarrage du serveur hôte. Vous pouvez importer des licences de traîneau de stockage uniquement sur le périphérique cible.

- Exporter : exportez la licence installée sur un périphérique de stockage externe pour disposer d'une sauvegarde ou pour la réinstaller après le remplacement d'un composant du serveur. Le nom et le format de fichier de la licence exportée sont `<EntitlementID>.xml`
- Supprimer : supprimez la licence attribuée à un composant ou un traîneau de stockage si ce dernier est manquant. Une fois supprimée, la licence n'est plus stockée dans CMC et les fonctions de base du produit sont activées.

  Vous pouvez supprimer des licences de traîneau de stockage uniquement lorsque le traîneau de stockage est hors tension. Les licences supprimées sont supprimées du magasin de traîneaux de stockage persistant et du gestionnaire de licences.

- 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.

  Pour les traîneaux de stockage, les nouvelles licences remplacent la licence existante dans le gestionnaire de licences CMC et le magasin de traîneaux de stockage persistant. Mettez le traîneaux de stockage hors tension avant de remplacer la licence. Les fonctionnalités sous licence sont disponibles uniquement après la réinitialisation du contrôleur RAID lors du prochain redémarrage de l'hôte.

- 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 une licence mise à jour. Pour plus d'informations, consultez le portail de gestion des licences logicielles Dell à l'adresse **WWW.DELL.COM/SUPPORT/LICENSING/US/EN/19**
- 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 en savoir plus, voir l'aide d'Internet Explorer.

  REMARQUE : Si vous tentez d'installer la licence PowerEdge FM120x4 sur PowerEdge FC630, l'installation de la licence échoue. Pour plus d'informations sur la gestion des licences, voir le *Guide de l'utilisateur d'iDRAC*.

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 7. Fonctions du CMC selon les types de licence

Fonction	Express	Enterprise
Réseau CMC	Oui	Oui
Port série CMC	Oui	Oui
RACADM (SSH, local et distant)	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
Sauvegarde des paramètres du CMC	Non	Oui
Restauration des paramètres du CMC	Oui	Oui
Syslog distant	Non	Oui

Tableau 7. Fonctions du CMC selon les types de licence (suite)

Fonction	Express	Enterprise
Services d'annuaire	Non	Oui
Prise en charge de l'authentification unique	Non	Oui
Authentification bifactorielle	Non	Oui
Authentification PK	Non	Oui
Partage de fichier à distance	Non	Oui
Seuil maximal de puissance au niveau de l'enceinte	Non	Oui
Gestion de plusieurs châssis :	Non	Oui
Activation de FlexAddress	Non	Oui
Mise à jour de micrologiciel de serveur un à plusieurs	Non	Oui
Configuration un-à-plusieurs d'iDRAC	Non	Oui

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 8. 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

Affichage des versions localisées de l'interface Web du CMC

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

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, consultez l'*Aide en ligne du contrôleur CMC pour Dell PowerEdge FX2/FX2s* à laquelle vous pouvez accéder depuis l'interface Web.
- Commandes RACADM : la commande RACADM ou l'objet que vous devez utiliser est indiqué ici. Pour en savoir plus sur les commandes RACADM, voir le *Guide de référence de la ligne de commande RACADM de Dell Chassis Management Controller pour PowerEdge FX2/FX2s* disponible à l'adresse **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 documents suivants disponibles sur le site **dell.com/support/manuals**.

- L'*Aide en ligne du contrôleur CMC pour Dell PowerEdge FX2/FX2s* fournit des informations sur l'utilisation de l'interface web. Pour accéder à l'Aide en ligne, cliquez sur **Help (Aide)** dans l'interface web CMC.
- Le document *Chassis Management Controller Version 2.0 for Dell PowerEdge FX2/FX2s RACADM Command Line Reference Guide (Guide de référence de la ligne de commande RACADM du contrôleur Chassis Management Controller version 2.0 pour Dell PowerEdge FX2/FX2s)* explique comment utiliser les fonctions RACADM des systèmes FX2/FX2s.
- Les documents *Dell Chassis Management Controller (CMC) for Dell PowerEdge FX2/FX2s Version 2.0 Release Notes [Notes de mise à jour du contrôleur Dell Chassis Management Controller (CMC) pour Dell PowerEdge FX2/FX2s version 2.0]*, 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 *Integrated Dell Remote Access Controller 8 (iDRAC) User's Guide (Guide d'utilisation d'Integrated Dell Remote Access Controller 8 (iDRAC)* fournit des informations sur l'installation, la configuration et la maintenance du contrôleur iDRAC8 sur les systèmes gérés.
- Le manuel *« Dell OpenManage Server Administrator's User's Guide » (Guide d'utilisation de Dell OpenManage Server Administrator)* donne des informations sur l'installation et l'utilisation de Server Administrator.
- Le *Dell OpenManage SNMP Reference Guide for iDRAC and Chassis Management Controller (Guide de référence SNMP de Dell OpenManage pour iDRAC et Chassis Management Controller)* fournit des informations à propos des SNMP de MIB.
- Le manuel *« Dell Update Packages User's Guide » (Guide d'utilisation des progiciels Dell Update Package)* 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.
- 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.

Les documents système suivants fournissent des informations supplémentaires sur le système sur lequel le CMC PowerEdege FX2/FX2s est installé :

- Le document « Safety instructions » (Consignes de sécurité) fourni avec votre système contient des informations importantes sur la sécurité et les réglementations en vigueur. Pour plus d'informations sur la réglementation, voir la page d'accueil « Regulatory Compliance » (Conformité à la réglementation) 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 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 de serveur contient des informations sur les fonctions du module de 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 du système, 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, localisateur de ressources rapide) disponible sur votre système et sur la fiche de configuration du système livrée avec celui-ci. Téléchargez l'application QRL de votre plateforme mobile pour activer l'application sur votre périphérique mobile.

Accès au contenu de support à partir du site de support Dell EMC

Accédez au contenu de support lié à un ensemble d'outils de gestion de systèmes à l'aide de liens directs, en accédant au site de support Dell EMC, ou à l'aide d'un moteur de recherche.

- Liens directs :
  - Pour la gestion des systèmes Dell EMC Enterprise et la gestion à distance des systèmes Dell EMC Enterprise à distance :https://www.dell.com/esmmanuals
  - Pour les solutions de virtualisation Dell EMC :https://www.dell.com/SoftwareManuals
  - Pour Dell EMC OpenManage :https://www.dell.com/openmanagemanuals
  - Pour iDRAC :https://www.dell.com/idracmanuals
  - Pour la gestion des systèmes Dell EMC OpenManage Connections Enterprise :https://www.dell.com/OMConnectionsEnterpriseSystemsManagement
  - Pour les outils facilitant la maintenance Dell EMC :https://www.dell.com/serviceabilitytools
- 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.
  4. Cliquez sur le produit requis, puis sur la version requise.

À l'aide des 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.

Sujets :

Installation du matériel CMC

Le contrôleur CMC est pré-installé sur votre châssis, donc aucune installation n'est requise.

Liste de contrôle pour la configuration du châssis

Les étapes 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 étiqueté **GB1** et le réseau de gestion.

   Réseau de gestion : les contrôleurs CMC et iDRAC (sur chaque serveur) ainsi que les ports de gestion réseau du module d'E/S du commutateur sont connectés à un réseau interne commun dans le châssis PowerEdge FX2/FX2s. Cela permet d'isoler le réseau de gestion du réseau de données du serveur.

   Réseau d'application : l'accès aux serveurs gérés s'effectue via des connexions réseau avec le module d'E/S (IOM). Cela permet d'isoler le réseau d'application du réseau de gestion. Il est important de séparer ce trafic afin de garantir un accès ininterrompu à la gestion du châssis.

   REMARQUE : Il est recommandé d'isoler la gestion du châssis du réseau de données. En raison du potentiel de trafic sur le réseau de données, les interfaces de gestion du réseau interne peuvent être saturées par le trafic destiné aux serveurs. Il en résulte des retards de communication avec les contrôleurs CMC et iDRAC. Les retards peuvent donner lieu à un comportement imprévisible du châssis. Par exemple, le contrôleur CMC affiche le contrôleur iDRAC comme hors ligne alors qu'il est activé et en cours d'exécution. Cela entraîne à son tour un comportement indésirable. Si l'isolation physique du réseau de gestion s'avère peu pratique, l'autre option consiste à séparer le trafic des contrôleurs CMC et iDRAC sur un réseau VLAN distinct. Les interfaces réseau des contrôleurs CMC et iDRAC peuvent être configurées pour utiliser un réseau VLAN.

2. Le port STK/Gb2 peut également être utilisé pour le basculement de la carte réseau du CMC. Pour implémenter le basculement de la carte réseau, vérifiez que le CMC est modifié pour passer du paramètre par défaut **Stacking (Empilage)** au paramètre **Redundant (Redondant)**. Pour plus d'informations, voir la section Configuration du port de gestion 2.

   PRÉCAUTION : La connexion du port STK/Gb2 au réseau de gestion peut provoquer des résultats imprévisibles si la configuration du contrôleur CMC n'est pas modifiée en remplaçant le paramètre par défaut Stacking (Empilage) par le paramètre Redundant (Redondant) afin d'implémenter le basculement de la carte réseau. Avec le mode par défaut Stacking (Empilage), le câblage des ports Gb1 et STK/Gb2 au même réseau (domaine de diffusion) peut provoquer une perturbation importante de la diffusion (broadcast storm). Un broadcast storm peut également se produire si la configuration du contrôleur CMC est basculée en mode Redundant (Redondance) alors qu'en mode Stacking (Empilage) le câblage des châssis est réalisé en série. Vérifiez que le modèle de câblage correspond à la configuration du contrôleur CMC nécessaire à l'utilisation prévue.

3. Installez le module d'E/S dans le châssis et connectez le câble réseau à ce module.
4. Insérez les serveurs dans le châssis.

5. Connectez le châssis à la source d'alimentation.
6. Pour mettre le châssis sous tension, appuyez sur le bouton d'alimentation ou utilisez les interfaces suivantes après avoir effectué la tâche 6. Depuis l'interface web, accédez à **Chassis Overview (Présentation du châssis)** > **Power (Alimentation)** > **Control (Contrôle)** > **Power Control Options (Options de contrôle de l'alimentation)** > **Power On System (Mise sous tension du système)**. Cliquez sur **Appliquer**.

   Vous pouvez également mettre le châssis sous tension à l'aide de l'interface de ligne de commande en utilisant la commande `racadm chassisaction powerup`.

   REMARQUE : Ne mettez pas sous tension les serveurs.
7. La configuration réseau par défaut du contrôleur CMC est Static (Statique) et son adresse IP est 192.168.0.120. Si vous souhaitez basculer la configuration réseau sur DHCP, connectez un câble série au port série du contrôleur CMC. Pour plus d'informations sur la connexion série, reportez-vous à la rubrique Configuration du protocole/de l'interface série de la section Utilisation du logiciel d'accès distant depuis une station de gestion.

   Une fois la connexion série établie, connectez-vous et utilisez la commande `racadm setniccfg –d` pour basculer la configuration réseau sur DHCP. Le contrôleur CMC prend entre 30 et 60 secondes pour obtenir l'adresse IP auprès du serveur DHCP.

   Pour afficher l'adresse IP du CMC attribué par DHCP, utilisez l'une des méthodes suivantes :

   - Pour afficher l'adresse IP du CMC à l'aide d'une connexion série avec le CMC, procédez comme suit :
     a. Connectez l'une des extrémités du câble modem null en série au connecteur série situé à l'arrière du châssis.
     b. Connectez l'autre extrémité du câble au port série du système de gestion.
     c. Une fois la connexion établie, connectez-vous au CMC à l'aide des références du compte root par défaut.
     d. Exécutez la commande `racadm getniccfg`.

        Dans le champ affiché, recherchez l'**Adresse IP actuelle**.
   - Pour afficher l'adresse IP du CMC en connectant le serveur à l'aide de KVM, effectuez les opérations suivantes :
     a. Connectez-vous à un serveur dans le châssis à l'aide de KVM.

        REMARQUE : Pour en savoir plus sur la façon de connecter un serveur via KVM, voir la section Accès au server à l'aide de KVM.
     b. Allumez le serveur.
     c. Assurez-vous que le serveur est configuré pour un amorçage en mode UEFI (Unified Extensible Firmware Interface).
     d. Appuyez sur F2 pour accéder à la page Configuration du système.
     e. Dans la page **System Setup (Configuration du système)**, cliquez sur **iDRAC Settings (Paramètres iDRAC)** > **System Summary (Résumé du système)**.

        L'adresse IP du CMC s'affiche dans la section **Contrôleur de gestion du châssis**.

        Pour en savoir plus sur la page **iDRAC Settings (Paramètres iDRAC)** de l'interface GUI du contrôleur iDRAC, voir le document *Dell Integrated Dell Remote Access Controller (iDRAC) User's Guide (Guide d'utilisation du contrôleur iDRAC)*.
8. Connectez-vous à l'adresse IP du CMC avec un navigateur Web en saisissant les références du compte root par défaut.
9. Configurer les paramètres réseau du contrôleur iDRAC en fonction des besoins. Par défaut, le réseau LAN du contrôleur iDRAC est activé lorsqu'une adresse IP statique est configurée. Pour déterminer l'adresse IP statique par défaut avec une **licence Enterprise**, accédez à **Server Overview (Présentation du serveur)** > **Setup (Configuration)** > **iDRAC (Contrôleur iDRAC)**. Vous pouvez également déterminer l'adresse IP statique avec une **licence Express**. Accédez à **Server Overview (Présentation du serveur)** > **Server-Slot (logement de serveur)** > **Setup (Configuration)** > **iDRAC (Contrôleur iDRAC)**.
10. Indiquez le module d'entrée/sortie au travers d'une adresse IP de gestion externe (le cas échéant) dans l'interface web CMC. Vous pouvez obtenir l'adresse IP en cliquant sur **I/O Module Overview (Présentation du module d'E/S)**, puis sur **Setup (Configuration)**.
11. Connectez-vous à chaque iDRAC par l'intermédiaire de l'interface Web à l'aide des références du compte root par défaut pour effectuer toute opération de configuration requise.
12. Mettez sous tension les serveurs et installez le système d'exploitation.

REMARQUE : Les références du compte local par défaut sont « root » (nom d'utilisateur) et « calvin » (mot de passe utilisateur).

Connexion réseau CMC FX2 en chaîne

Si vous disposez de plusieurs châssis dans un rack, vous pouvez réduire le nombre de connexions au réseau de gestion en connectant en chaîne jusqu'à dix châssis. Vous pouvez réduire de dix à un le nombre de connexions de liaison montante réseau de gestion requis.

Lorsque vous reliez des châssis par connexion en chaîne, le port GB est le port de liaison montante et le port STK, celui d'empilage (consolidation des câbles). Connectez les ports GB au réseau de gestion ou au port STK du CMC dans un châssis plus proche du réseau. Connectez le port STK uniquement à un port GB plus éloigné de la chaîne ou du réseau.

L'illustration suivante représente la disposition des câbles de quatre châssis connectés en chaîne, chacun comportant des CMC actifs.

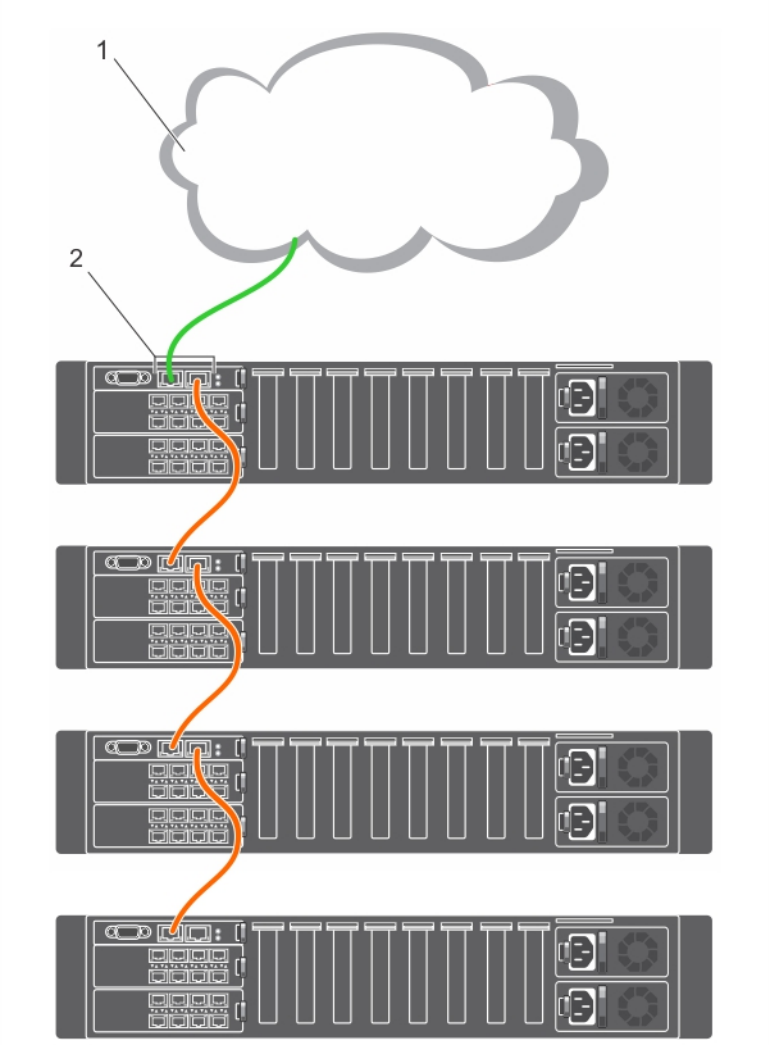
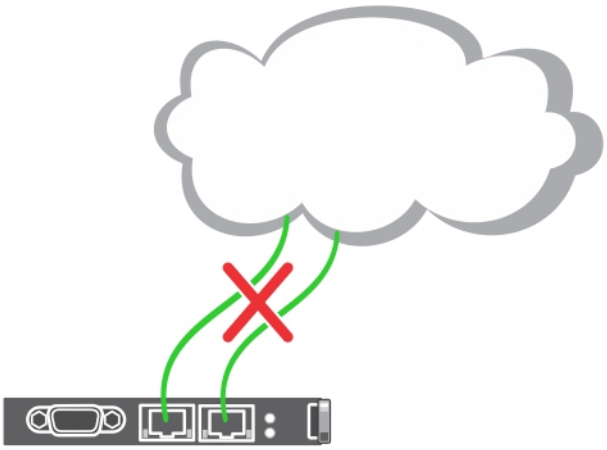


Tableau 9. Traîneaux de stockage connectés en chaîne

1	Réseau de gestion
2	CMC actif

La figure suivante illustre un exemple de câblage incorrect du CMC en mode d'empilage.



Vous trouverez ci-dessous les étapes à suivre pour connecter en chaîne quatre modules CMC FX2 :

1. Connectez le port GB du CMC FX2 du premier châssis au réseau de gestion.
2. Connectez le port GB du CMC FX2 du second châssis au port STK du CMC FX2 du premier châssis.
3. Si vous disposez d'un troisième châssis, connectez le port GB de son CMC FX2 au port STK du CMC FX2 du deuxième châssis.
4. Si vous disposez d'un quatrième châssis, connectez le port GB de son CMC FX2 au port STK du CMC FX2 du troisième châssis.

PRÉCAUTION : Le port STK d'un CMC ne doit jamais être connecté au réseau de gestion. Il ne peut être connecté qu'au port GB d'un autre châssis. La connexion d'un port STK au réseau de gestion peut perturber celui-ci et provoquer une perte de données. Le câblage du GB et du STK au même réseau (domaine de diffusion) peut provoquer une tempête de diffusion.

REMARQUE : La réinitialisation d'un CMC dont le port STK est connecté en chaîne à un autre CMC peut perturber le réseau pour les CMC situés en aval de la chaîne. Les CMC enfants peuvent consigner des messages signalant que la liaison réseau a été perdue.

Utilisation du logiciel d'accès à distance depuis une station de gestion

Vous pouvez accéder au contrôleur CMC depuis une station de gestion à l'aide d'un des nombreux logiciels d'accès à distance. Voici la liste des logiciels d'accès à distance Dell qui est disponible à partir de votre système d'exploitation.

Tableau 10. Interfaces CMC

Interface/ Protocole	Description
Série	Le CMC prend en charge une console texte série pouvant être lancée à l'aide de tout logiciel d'émulation de terminal. Voici quelques exemples de logiciels d'émulation de terminal que vous pouvez utiliser pour vous connecter au CMC. • Linux Minicom • HyperTerminal Hilgraeve pour Windows Connectez une extrémité du câble série null-modem (présent aux deux extrémités) sur le connecteur série situé à l'arrière du châssis. Connectez l'autre extrémité du câble dans le port série de la station de gestion. Pour plus d'informations sur la connexion des câbles, reportez-vous au panneau arrière du châssis dans la section Présentation du châssis. Configurez votre logiciel d'émulation de terminal avec les paramètres suivants : • Débit en bauds : 115 200 • Port : COM1 • Données : 8 bits • Parité: Aucune

Tableau 10. Interfaces CMC (suite)

Interface/ Protocole	Description
	• Arrêt : 1 bit • Contrôle de flux matériel : Oui • Contrôle de flux logiciel : Non
CLI RACADM a distance	L'interface RACADM à distance 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 et nécessite l'adresse IP, le nom d'utilisateur et le mot de passe du contrôleur CMC. Pour utiliser l'interface distante RACADM depuis votre station de gestion, installez-la à l'aide du DVD Documentation et outils de Dell Systems Management, qui est disponible avec votre système. Pour en savoir plus sur l'interface distante RACADM
Interface Web	Fournit un accès à distance à CMC à l'aide d'une interface utilisateur graphique. L'interface Web est intégrée au micrologiciel CMC et accessible via l'interface NIC d'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 de logiciels système Dell **sur dell.com/support/manuals**.
Telnet	Permet d'accéder à CMC par ligne de commande 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 est désactivé par défaut. Il transmet toutes les données, y compris les mots de passe, non cryptées.
SNMP	SNMP (Simple Network Management Protocol) est un ensemble de définitions de protocole permettant de gérer des périphériques sur les réseaux. Le contrôleur CMC fournit l'accès à SNMP, lequel vous permet d'utiliser les outils SNMP pour interroger le CMC et obtenir des informations relatives à la gestion des systèmes. Le fichier MIB du CMC peut être téléchargé à partir de l'interface Web CMC, accédez à **Présentation du châssis** > **Réseau** > **Services** > **SNMP**. Reportez-vous au *Guide de référence SNMP de Dell OpenManage* pour plus d'informations sur la MIB du CMC. L'exemple suivant montre comment utiliser la commande `net-snmp snmpget` en vue d'obtenir le numéro de service du châssis depuis le CMC. `snmpget -v 1 -c <CMC community name> <CMC IP address>.1.3.6.1.4.1.674.10892.2.1.1.6.0`
WSMan	Les services WSMan reposent sur le protocole de gestion WSMan (Web Services for Management) pour exécuter des tâches de gestion de systèmes un à plusieurs. Vous devez utiliser un client WSMan, tel que WinRM (Windows) ou OpenWSMan (Linux), pour pouvoir utiliser la fonctionnalité LC-Remote Services. 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 pouvant être modifiés sur un système géré. L'implémentation WSMan CMC 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. **REMARQUE :** Le port SSL utilisé à des fins de sécurité de transport est le même que le port HTTPS du CMC. Pour plus d'informations, voir : • 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**

Tableau 10. Interfaces CMC (suite)

Interface/ Protocole	Description
	• Spécifications DMTF WS-Management : **www.dmtf.org/standards/wbem/wsman** 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**>.

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 à l'aide de Dell Server Administrator, lancez Server Administrator sur votre station de gestion. Dans le panneau de gauche de la page d'accueil de Server Administrator, cliquez sur **Système** > **Châssis principal du système** > **Remote Access Controller**. Pour plus d'informations, voir le *Guide de l'utilisateur de Dell Server Administrator* à l'adresse **dell.com/support/manuals**.

Installation de RACADM à distance

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 *Guide d'utilisation Installation et sécurité Dell OpenManage* disponible sur **dell.com/support/manuals**. Vous pouvez également télécharger la dernière version des outils Dell DRAC depuis le site **dell.com/support**.

Installation de RACADM distante sur une station de gestion Windows

Si vous utilisez le DVD, exécutez ***<path>*\SYSMGMT\ManagementStation\windows\DRAC*<.msi file name>***

Si vous avez téléchargé le logiciel à partir du site **dell.com/support** :

1. Décompressez le fichier téléchargé et exécutez le fichier **.msi** fourni.
   En fonction de la version téléchargée, le fichier sera nommé DRAC.msi RACTools.msi, ou RACTools64Bit.msi.
2. Acceptez le contrat de licence. Cliquez sur **Suivant**.
3. Sélectionnez l'emplacement dans lequel il doit être installé. **Cliquez sur Suivant**.
4. Cliquez sur **Installer**).
   La fenêtre d'installation apparaît.
5. Cliquez sur **Terminer**.

Ouvrez une invite de commande d'administration, tapez `racadm` et appuyez sur **Entrée**. Si vous obtenez les instructions d'aide de RACADM, cela signifie que le logiciel est correctement installé.

Installation de RACADM distante 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 de l'aide concernant la commande RACADM, entrez `racadm help` après avoir saisi les commandes précédentes. Pour plus d'informations sur RACADM, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge FX2/FX2s*.

   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 RACADM à distance depuis 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 configurer et gérer le contrôleur CMC, les serveurs et les modules installés dans le châssis à l'aide d'un navigateur Web. Reportez-vous à la section relative aux navigateurs pris en charge dans le document *Dell Systems Software Support Matrix (Matrice de support logiciel des systèmes Dell)* sur le site **dell.com/support/manuals**.

Le contrôleur CMC et la station de gestion où vous utilisez le navigateur doivent se trouver sur le même réseau, appelé *réseau de gestion*. En fonction des vos exigences de sécurité, le réseau de gestion peut être un réseau isolé très protégé.

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 accès à Internet. Si la station de gestion possède un système d'exploitation Windows, certains paramètres Internet Explorer interfèrent avec les connexions, même si vous utilisez une interface de ligne de commande (CLI) pour accéder au réseau de gestion.

REMARQUE : Pour résoudre 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 contrôleur CMC.

Serveur proxy

Pour naviguer jusqu'à 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 qu'il doit contourner le serveur proxy pour l'accès au réseau de gestion.

Filtre anti-hameçonnage 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**.

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**.

Activer les 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**.

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 le nom du châssis ainsi que son emplacement dans un centre de données pour l'identifier sur le réseau (le nom par défaut est **cmc-« Numéro de service »**). Par exemple, une requête SNMP concernant le nom de châssis renvoie 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. Dans la page **Paramètres généraux du châssis**, entrez les propriétés d'emplacement et le nom du châssis. Pour plus d'informations sur la définition des propriétés du châssis voir l'*Aide en ligne de CMC*.

   REMARQUE : Le champ **Emplacement du châssis** est facultatif. Il est recommandé d'utiliser les champs **Centre de données**, **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 à l'aide de l'interface de ligne de commande, voir les commandes **setsysinfo** et **setchassisname**.

Par exemple : `racadm setsysinfo –c chassisname` ou `racadm setsysinfo –c chassislocation`

Pour plus d'informations, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge FX2/FX2s*.

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 à l'aide de 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 *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge FX2/FX2s* sur le site **dell.com/support/manuals**.

Par exemple : `racadm setractime -l 20140207111030`.

Pour lire la date et l'heure, utilisez la commande `racadm getractime`.

Configuration des voyants LED pour l'identification des composants du châssis

Vous pouvez activer les voyants des composants (châssis, serveurs, traîneaux de stockage et modules d'E/S) pour qu'ils clignotent afin que vous puissiez identifier le composant sur le châssis.

REMARQUE : Pour pouvoir modifier ces paramètres, vous devez disposer du privilège d'**Administrateur de débogage** sur un CMC.

Lorsqu'un traîneau de calcul exécute une action d'identification, le voyant situé à l'avant du traîneau de stockage connecté clignote également selon le schéma d'identification. Si un traîneau de stockage est en mode de fractionnement simple et est connecté à deux nœuds de calcul, il clignote selon le schéma d'identification si l'un ou l'autre des deux nœuds de calcul exécute une action d'identification.

Si vous démarrez une action d'identification d'un traîneau de calcul, d'un lecteur ou d'une enceinte à l'aide d'OMSS ou iDRAC, le traîneau de stockage associé exécute également l'action d'identification.

REMARQUE : Vous ne pouvez pas sélectionner uniquement des traîneaux de stockage pour une action d'identification.

Configuration du clignotement des LED à l'aide de 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.

Pour activer le clignotement d'un voyant de composant, sélectionnez le composant, puis cliquez sur **Faire clignoter**. Pour désactiver le clignotement d'un voyant de composant, désélectionnez le serveur, puis cliquez sur **Arrêter le clignotement**.

Configuration du clignotement des LED à l'aide de 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>* indique le module dont vous voulez configurer le voyant. Options de configuration :

- `server-n` où *n* = 1-4 (PowerEdge FM120x4) et `server-nx` où *n* = 1–4 et *x* = a à b (PowerEdge FC630).
- `switch-1`
- `cmc-active`

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

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

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 du panneau avant

Vous pouvez utiliser la page du panneau avant pour configurer :

- Bouton d'alimentation
- KVM

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.

Accès au serveur à l'aide de KVM

Pour adresser un serveur à KVM à partir de l'interface Web :

1. Connectez un écran au connecteur vidéo et un clavier au connecteur USB situé à l'avant du châssis.
2. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Panneau avant** > **Configuration**.
3. Sur la page **Configuration du panneau avant** , dans la section **Configuration KVM** , sélectionnez l'option **Activer l'adressage de KVM**.
4. Sur la page **Configuration du panneau avant** , dans la section **Configuration KVM**, pour l'option **KMV adressé**, sélectionnez le serveur voulu dans la liste déroulante.
5. Cliquez sur **Appliquer**.

Pour adresser un serveur à l'interface KVM à l'aide de racadm, utilisez la commande `racadm config -g cfgKVMInfo -o cfgKvmMapping [logement de serveur #]`.

Pour afficher l'adressage KVM actuel à l'aide de racadm, utilisez la commande `racadm getconfig -g cfgKVMInfo`.

Configuration de la gestion de châssis en mode Serveur

Cette fonctionnalité vous permet de gérer et de surveiller les composants partagés du châssis et les nœuds du châssis en tant que serveurs de rack. Lorsque cette fonctionnalité est activée, vous pouvez utiliser le proxy RACADM d'iDRAC, les systèmes d'exploitation de serveur lame et le Lifecycle Controller pour effectuer les opérations suivantes :

- Surveiller et gérer les ventilateurs du châssis, les blocs d'alimentation et les capteurs de température
- Mettre à jour et configurer le micrologiciel CMC

Configuration de la gestion du châssis en mode Serveur à l'aide de l'interface Web CMC

Pour activer la gestion du châssis en mode Serveur :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Configurer** > **Général**.
2. Dans la page **Paramètres généraux du châssis**, à partir de la liste déroulante **Gestion du châssis en mode Serveur**, sélectionnez l'un des modes suivants :
   - **Aucun** : ce mode ne vous permet pas de surveiller ou gérer le composant du châssis par le biais d'iDRAC, du système d'exploitation ou du Lifecycle Controller.
   - **Surveiller** : ce mode vous permet de surveiller les composants du châssis, mais ne vous permet pas d'effectuer de mise à jour de micrologiciel au moyen d'iDRAC, du système d'exploitation, du proxy RACADM d'iDRAC ou du Lifecycle Controller.
   - **Gérer et surveiller** : ce mode vous permet de surveiller les composants de châssis et de mettre à jour le micrologiciel CMC à l'aide de DUP au moyen d'iDRAC, du système d'exploitation, du proxy RACADM d'iDRAC ou du Lifecycle Controller.

Configuration de la gestion de châssis en mode Serveur à l'aide de RACADM

Pour activer la gestion du châssis en mode Serveur à l'aide de RACADM, utilisez les commandes suivantes :

- Pour désactiver la gestion du châssis en mode Serveur, utilisez :

```
racadm config -g cfgRacTuning - cfgRacTuneChassisMgmtAtServer 0
```

- Pour définir la gestion du châssis en mode Serveur sur Surveiller, utilisez :

```
racadm config -g cfgRacTuning - cfgRacTuneChassisMgmtAtServer 1
```

- Pour définir la gestion du châssis en mode Serveur sur Gérer et surveiller, utilisez :

```
racadm config -g cfgRacTuning - cfgRacTuneChassisMgmtAtServer 2
```

3

Connexion au contrôleur CMC

Vous pouvez ouvrir une session sur CMC en tant qu'utilisateur CMC local, tel qu'un utilisateur Microsoft Active Directory, ou un utilisateur LDAP. Vous pouvez également ouvrir une session à l'aide de la connexion directe ou par carte à puce.

Sujets :

Configuration de l'authentification par clé publique sur SSH

Vous pouvez configurer jusqu'à 6 clés publiques pouvant être utilisées avec le nom d'utilisateur du service sur l'interface SSH. Avant d'ajouter ou de supprimer des clés publiques, veillez à utiliser la commande `view` pour identifier les clés déjà définies afin qu'aucune clé ne soit accidentellement remplacée ou supprimée. Le nom d'utilisateur du service correspond à un compte utilisateur spécial qui peut être utilisé pour l'accès au contrôleur CMC via SSH. Si vous configurez et utilisez correctement l'authentification PKA sur SSH, vous n'avez pas besoin d'entrer de nom d'utilisateur ni de mot de passe pour la connexion au contrôleur CMC. Cela est particulièrement utile pour définir des scripts automatisés afin de réaliser différentes fonctions.

REMARQUE : L'interface utilisateur n'est pas prise en charge pour la gestion de cette fonction ; vous ne pouvez utiliser que RACADM.

Lorsque vous ajoutez de nouvelles clés publiques, vérifiez que les clés existantes ne se situent pas à l'index où vous allez ajouter la nouvelle clé. Le contrôleur CMC ne vérifie jamais si les clés précédentes sont supprimées lors de l'ajout d'une nouvelle clé. Dès que vous ajoutez une nouvelle clé, elle est automatiquement activée, à condition que l'interface SSH soit activée.

Lorsque vous utilisez la section de commentaire de la clé publique, notez que le contrôleur CMC utilise uniquement les 16 premiers caractères. Le commentaire de clé publique permet au contrôleur CMC de distinguer les utilisateurs SSH lors de l'utilisation de la commande RACADM `getssninfo`, car tous les utilisateurs de PKA emploient le nom d'utilisateur de 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`, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge FX2/FX2s*.

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. Vous disposez de deux méthodes pour générer la paire de clés privée/publique : utilisation de l'application de génération de clés PuTTY Key Generator pour les clients Windows ou utilisation de l'interface de ligne de commande (CLI) ssh-keygen pour les clients Linux.

Cette section fournit des instructions simples de génération d'une paire de clés publique/privée pour les deux applications. Pour en savoir plus ou connaître l'utilisation avancée de ces outils, voir l'aide 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 comme type de clé à générer (SSH-1 n'est pas pris en charge).
2. Entrez le nombre de bits de la clé. La taille de la clé RSA doit être comprise entre 768 et 4 096.

   REMARQUE :
   - Le contrôleur CMC peut ne pas afficher de message si vous ajoutez des clés de moins de 768 ou de plus de 4096, mais lorsque vous essayez de vous connecter avec ces clés, la connexion échoue.
   - Le CMC accepte les clés RSA avec une puissance allant jusqu'à 4096, mais la puissance recommandée est de 1024.

3. Cliquez sur **Générer** et 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 entrer une phrase de phase 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 exécutant 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

`-t` doit être 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 passer à RACADM afin de téléverser le fichier.

Accès à l'interface Web CMC

Avant de vous connecter au CMC avec l'interface Web, vérifiez que vous avez configuré un navigateur Web pris en charge 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 ouvrir une session CMC, vous devez disposer d'un compte CMC doté du privilège **Connexion au contrôleur CMC**. La valeur par défaut du compte root est le compte administratif par défaut livré avec le CMC.

REMARQUE : Pour plus de sécurité, Dell recommande de modifier le mot de passe par défaut du compte root lors de la procédure de configuration initiale.

REMARQUE : Lorsque la validation des certificats est activée, vous devez fournir le nom de domaine complet 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>

     REMARQUE : Le nom d'utilisateur CMC peut contenir uniquement des caractères alphanumériques et des caractères spéciaux. Le symbole arobase (@) et les caractères spéciaux suivants ne sont pas pris en charge :
     - / (barre oblique)
     - / (barre oblique)
     - ; (point-virgule)
     - ` (guillemet vers l'arrière)
     - " (guillemets)
   - 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 champ **Domaine**, dans le menu déroulant, 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 nomcmc est le nom d'hôte CMC du contrôleur CMC, *port number* est le nom du domaine et *numéro de port* 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 CMC avec une 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 configuré, 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.

Connexion au 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 phrase 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 cette phrase 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 la saisie de la phrase 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
WSMan	4

4

Mise à jour du micrologiciel

Vous pouvez mettre à jour le micrologiciel de :

- Contrôleur CMC
- Infrastructure du châssis
- Module d'E/S

Vous pouvez mettre à jour le micrologiciel des composants de serveur suivants :

- BIOS
- iDRAC7
- iDRAC8
- Lifecycle Controller
- Diagnostics 32 bits
- Pack de pilotes de système d'exploitation
- Contrôleurs d'interface réseau (NIC)
- Contrôleurs RAID

Sujets :

Signature de l'image du micrologiciel CMC

Le micrologiciel CMC intègre une signature. Le micrologiciel CMC effectue une étape de vérification de signature afin de vérifier l'authenticité du micrologiciel téléversé. La mise à jour du micrologiciel est réussie uniquement si l'image du micrologiciel est authentifiée par CMC comme une image valide auprès du fournisseur de service et n'a pas été modifiée. La mise à jour du micrologiciel est interrompue si le contrôle CMC ne peut pas vérifier la signature de l'image micrologicielle téléversée. Un événement d'avertissement est alors consigné et un message d'erreur approprié s'affiche. La mise à jour du micrologiciel comprend une mise à niveau et une rétrogradation.

Téléchargement du micrologiciel du contrôleur CMC

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

Il est recommandé de respecter l'ordre des mises à jour suivant lors de la mise à jour de micrologiciel pour le châssis :

- Micrologiciel des composants du serveur lame
- Micrologiciel du CMC
- Micrologiciel d'infrastructure du châssis

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 à l'aide de 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**

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 firmware actuellement installées à l'aide de RACADM

La commande `racadm getversion` permet d'afficher les versions de firmware actuellement installées. Pour plus d'informations sur les autres commandes RACADM, voir le *Guide de référence de la ligne de commande RACADM de Dell Chassis Management Controller pour PowerEdge FX2/FX2s*.

Mise à jour du micrologiciel du contrôleur CMC

Vous pouvez mettre à jour le micrologiciel CMC à l'aide de l'interface web ou de l'interface RACADM. Par défaut, la mise à jour du micrologiciel conserve les paramètres actuels du CMC.

REMARQUE : Pour pouvoir mettre à jour le micrologiciel du contrôleur CMC, vous devez disposer du privilège Administrateur de configuration du châssis.

REMARQUE : Vous ne pouvez pas mettre à jour le micrologiciel CMC si le fichier d'image de micrologiciel ne contient pas une signature de vérification ou s'il contient une signature de vérification qui n'est pas valide ou est endommagée.

REMARQUE : Vous ne pouvez pas rétrograder le micrologiciel CMC vers une version précédente si la signature de cette version n'est pas reconnue par le micrologiciel CMC actuel.

Si une session de l'interface utilisateur web est utilisée pour mettre à jour le micrologiciel d'un composant système, le paramètre Idle Timeout (Délai d'inactivité) (**0, 60 à 10 800**) doit avoir une valeur suffisamment élevée pour gérer la durée du transfert de fichiers. Dans certains cas, le transfert du fichier du micrologiciel peut prendre jusqu'à 30 minutes. Pour définir la valeur du délai d'inactivité, voir la section Configuration des services.

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

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

Pendant la phase finale du processus de mise à jour du micrologiciel dans le contrôleur CMC, la session de navigateur et la connexion au contrôleur CMC sont temporairement perdues lorsque ce dernier n'est pas connecté au réseau. Le contrôleur CMC détermine 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 de connexion. Le contrôleur CMC détermine ensuite que l'intégrité générale du châssis est saine et que la liaison du réseau du contrôleur CMC est montante. Une fois le contrôleur CMC réinitialisé, la nouvelle version micrologicielle s'affiche sur la page **Firmware Update (Mise à jour micrologicielle)**.

Lorsque vous transférez des fichiers vers et depuis le contrôleur CMC, les icônes de transfert de fichiers tournent. Si votre icône est inactive, vérifiez que votre navigateur est configuré pour autoriser les animations. Pour plus d'informations sur l'autorisation des animations dans le navigateur, reportez-vous à la rubrique Autoriser les animations dans Internet Explorer.

REMARQUE : Dans un châssis utilisant deux blocs d'alimentation de 2 400 W en CA, si vous tentez de mettre à jour/rétrograder le micrologiciel à une version non prise en charge par lesdits blocs d'alimentation, un message d'erreur s'affiche. Les blocs d'alimentation de 2 400 W en CA prennent en charge les images 1.40-A00 et ultérieures du contrôleur CMC.

Mise à jour du micrologiciel CMC via l'interface Web

Pour mettre à jour le micrologiciel 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 micrologiciel**, dans la section **Micrologiciel CMC**, sélectionnez les composants requis dans la colonne **Mettre à jour les cibles** du contrôleur CMC à mettre à jour, puis cliquez sur **Appliquer la mise à jour CMC**.
3. Dans le champ **Image du micrologiciel**, entrez le chemin d'accès au fichier image du micrologiciel sur la station de gestion ou le réseau partagé, ou bien cliquez sur **Parcourir** pour accéder à l'emplacement du fichier. Le fichier image du micrologiciel du CMC s'appelle par défaut `fx2_cmc.bin`.
4. Cliquez sur **Lancer la mise à jour du micrologiciel**, puis sur **Oui**. La section **Avancement de la mise à jour du micrologiciel** fournit des informations sur l'état de mise à jour du micrologiciel. Un indicateur d'état apparaît sur la page pendant le téléversement du fichier d'image. La durée du transfert de fichier varie en fonction du débit de la connexion. Lorsque le processus de mise à jour interne démarre, la page est automatiquement actualisée et le chronomètre de mise à jour du micrologiciel s'affiche. Pour en savoir plus sur les différents états de micrologiciel, voir l'Aide en ligne.
5. Au cours des dernières étapes de mise à jour du micrologiciel du CMC, la session du navigateur et la connexion au CMC sont temporairement perdues car le CMC n'est pas connecté au réseau. Vous devez vous connecter après quelques minutes, une fois que le CMC a redémarré. Après la réinitialisation du CMC, la nouvelle version du micrologiciel s'affiche sur la page **Mise à jour du micrologiciel**.

   REMARQUE : Après la mise à jour du micrologiciel, supprimez les fichiers du cache du navigateur Web. Pour savoir comment effacer le cache du navigateur Web, voir son aide en ligne.

Instructions supplémentaires :

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

  REMARQUE : Le processus de mise à jour peut prendre quelques minutes.

Mise à jour du micrologiciel CMC via RACADM

Pour mettre à jour le micrologiciel CMC à l'aide de RACADM, utilisez la sous-commande `fwupdate` .

Par exemple, `racadm fwupdate <options> <firmware image>`.

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 FX2/FX2s*.

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

Mise à jour du CMC à l'aide de DUP

Vous pouvez mettre à jour le firmware du CMC à l'aide de DUP (Dell Update Package) via les composants suivants :

- Proxy RACADM d'iDRAC
- Système d'exploitation du serveur lame
- Lifecycle Controller

Pour en savoir plus sur la mise à jour de CMC via l'iDRAC, voir le *Guide de l'utilisateur d'iDRAC*.

Avant de poursuivre la mise à jour du CMC à l'aide de DUP, vérifiez que :

- Le package de firmware CMC est disponible sous forme de DUP sur un système local ou un partage réseau.
- L'option **Gestion de châssis en mode Serveur** est définie sur **Gérer et surveiller**.

  Pour en savoir plus, voir la section Configuration de Gestion de châssis en mode Serveur

- Pour les mises à jour via le système d'exploitation ou Lifecycle Controller, l'option iDRAC **Activer la mise à jour des composants partagés via OS/USC** doit être activée. Pour plus d'informations sur l'activation de cette option, voir le *Guide de l'utilisateur d'iDRAC*.

REMARQUE : Lorsque vous effectuez la mise à jour du CMC à l'aide de DUP, les mises à jour du coprocesseur du module d'E/S (IOM) disponibles dans l'image CMC sont appliquées lors du prochain cycle d'alimentation du châssis.

Mise à jour du micrologiciel de l'infrastructure du châssis

L'opération de mise à jour de l'infrastructure du châssis met à jour la carte mère.

REMARQUE : Avant de mettre à jour le micrologiciel de l'infrastructure du châssis, mettez hors tension tous les serveurs du châssis, si nécessaire.

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, la connexion au CMC est perdue pendant la réinitialisation du châssis. Actualisez l'interface Web avant de vous reconnecter. Accédez à **Présentation du châssis** > **Contrôleur de châssis**.

Une fois la mise à jour terminée, la version du micrologiciel de la carte mère s'affiche.

.

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 à l'aide de RACADM, utilisez la sous-commande `fwupdate` .

Par exemple, `racadm fwupdate <options> <firmware image>`.

Pour plus d'informations sur l'utilisation des commandes RACADM, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge FX2/FX2s*.

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

Mise à jour du micrologiciel iDRAC du serveur

Vous pouvez mettre à jour le micrologiciel d'iDRAC7 ou iDRAC8. Pour utiliser cette fonction :

- Vous devez disposer d'une licence Enterprise.
- La version du micrologiciel iDRAC7 doit être la version 1.57.57 ou ultérieure.
- La version du micrologiciel iDRAC8 doit être la version 2.05.05 ou ultérieure.

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

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 châssis** > **Contrôleur de châssis** > **Mise à jour**.

   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 plus d'informations, voir Mise à niveau du micrologiciel des composants de serveur.
2. Pour mettre à jour le micrologiciel iDRAC7 ou iDRAC8, dans la section **Micrologiciel iDRAC<numéro de version> Enterprise**, cliquez sur le lien **Mise à jour** du serveur dont vous souhaitez 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.

Mise à jour du micrologiciel des composants de serveur

La fonctionnalité de mise à jour un-à-plusieurs du contrôleur CMC vous permet de mettre à jour un micrologiciel de composant serveur sur plusieurs serveurs. Vous pouvez mettre à jour les composants serveur à l'aide des progiciels DUP (Dell Update Packages) disponibles sur le système local ou sur un partage réseau. Cette opération s'active à l'aide de la fonctionnalité Lifecycle Controller sur le serveur.

Le service Lifecycle Controller est disponible sur chacun des serveurs et son utilisation garantie par le contrôleur iDRAC. Cette page permet de gérer le micrologiciel des composants et des terminaux sur les serveurs à l'aide du service Lifecycle Controller. Ce service utilise un algorithme d'optimisation pour mettre à jour le micrologiciel 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. Vous devez utiliser un micrologiciel iDRAC version 2.3 ou ultérieure pour mettre à jour un micrologiciel en utilisant le service Lifecycle Controller.

Les progiciels DUP (Dell Update Packages) permettent de mettre à jour un micrologiciel en utilisant le service Lifecycle Controller. Le progiciel DUP du composant Operating System Driver Pack (Pack de pilotes de système d'exploitation) dépasse cette limite et doit être mis à jour séparément en utilisant la fonction Extended Storage (Stockage étendu).

REMARQUE : Avant d'utiliser la fonctionnalité de mise à jour basée sur Lifecycle Controller, les versions micrologicielles des serveurs doivent être mises à jour. Vous devez également mettre à jour le micrologiciel CMC avant de mettre à jour les modules micrologiciels des composants serveur.

REMARQUE : Pour mettre à jour un micrologiciel de composant, l'option CSIOR doit être activée pour les serveurs. Pour activer CSIOR :

- Serveurs de 12e génération et ultérieurs : après le redémarrage du serveur, depuis la configuration F2, sélectionnez **iDRAC Settings (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 **Hardware Inventory (Inventaire du matériel)** en sélectionnant **Hardware Configuration (Configuration matérielle)** > **Hardware Inventory (Inventaire matériel)**. Sur la page **Hardware Inventory (Inventaire matériel)**, cliquez sur **Collect System Inventory on Restart (Collecter l'inventaire système au redémarrage)**.

La méthode **Update from File (Mettre à jour à partir d'un fichier)** permet de mettre à jour le micrologiciel des composants serveur à l'aide des fichiers DUP stockés sur le système local. Vous pouvez sélectionner les composants serveur individuels pour mettre à jour le micrologiciel à l'aide des fichiers DUP requis. Vous pouvez mettre à jour un grand nombre de composants simultanément en utilisant une carte SD pour stocker un fichier DUP dont la mémoire dépasse 48 Mo.

REMARQUE : Notez les points suivants :

- Lors de la sélection de composants serveur individuels à des fins de mise à jour, assurez-vous qu'il n'existe aucune dépendance entre les composants sélectionnés. En effet, la sélection de certains composants présentant des dépendances avec d'autres à des fins de mise à jour peut provoquer un arrêt brutal du serveur.
- Assurez-vous de mettre à jour les composants serveur dans l'ordre prescrit. Sinon, le processus de mise à jour micrologicielle des composants risque d'échouer.

  Mettez toujours à jour les modules de micrologiciel de composant de serveur dans l'ordre suivant :
  - iDRAC
  - Lifecycle Controller
  - BIOS

La mise à jour de toutes les lames en un seul clic ou la méthode **Update from File (Mettre à jour à partir d'un fichier)** permet de mettre à jour le micrologiciel des composants serveur à l'aide des fichiers DUP stockés sur un partage réseau. Vous pouvez utiliser la fonction de mise à jour basée sur Dell Repository Manager (DRM) pour accéder aux fichiers DUP stockés sur un partage réseau et mettre à jour les composants serveur en une seule opération. Vous pouvez configurer une logithèque distante personnalisée constituée de progiciels DUP de micrologiciels et d'images binaires à l'aide du gestionnaire Dell Repository Manager et la partager sur le partage réseau. Vous pouvez également utiliser le gestionnaire Dell Repository Manager (DRM) pour rechercher les dernières mises à jour micrologicielles disponibles. Le gestionnaire Dell Repository Manager (DRM) permet de s'assurer que les systèmes Dell disposent des dernières mises à jour pour le BIOS, les pilotes, les micrologiciels et les logiciels. Vous pouvez rechercher sur le site de support (**support.dell.com**) l'ensemble des dernières mises à jour disponibles pour les plates-formes prises en charge, par marque, modèle ou numéro de série. Vous pouvez télécharger les mises à jour ou créer une logithèque à partir des résultats de la recherche. Pour en savoir plus sur l'utilisation du gestionnaire DRM pour rechercher les dernières mises à jour micrologicielles, rendez-vous sur le Dell TechCenter, à l'adresse http://en.community.dell.com/TECHCENTER/EXTRAS/M/WHITE_PAPERS/20438118/DOWNLOAD. Pour plus d'informations sur l'enregistrement du fichier d'inventaire utilisé comme entrée par le gestionnaire DRM pour créer les logithèques, voir la section Enregistrement du rapport d'inventaire du châssis via l'interface web CMC.

REMARQUE : La méthode de mise à jour d'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 chaque micrologiciel de 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 le DVD de téléchargement de l'utilitaire Dell Server Update Utility (SUU) ou créer et personnaliser les versions de mise à jour requises dans le gestionnaire Dell Repository Manager (DRM). Vous n'avez pas besoin de disposer de la dernière version du gestionnaire Dell Repository Manager pour créer ce répertoire. Cependant, la version 1.8 du gestionnaire Dell Repository Manager fournit une option permettant de créer une logithèque (répertoire de mises à jour) en fonction de l'inventaire exporté à partir des serveurs dans le châssis. Pour plus d'informations sur la création d'une logithèque à l'aide du gestionnaire Dell Repository Manager voir les documents *Dell Repository Manager Data Center Version 1.8 User's Guide (Guide d'utilisation du datacenter du gestionnaire de logithèques Dell version 1.8)* et *Dell Repository Manager Business Client Version 1.8 User's Guide (Guide d'utilisation du client privé du gestionnaire de logithèques Dell version 1.8)* disponible à l'adresse **dell.com/support/manuals**.

Il est recommandé de mettre à jour le micrologiciel CMC avant de mettre à jour les modules micrologiciels des composants serveur. Une fois la mise à jour du micrologiciel CMC effectuée, dans l'interface web CMC, vous pouvez mettre à jour le micrologiciel des composants serveur dans la page **Chassis Overview (Présentation du châssis)** > **Server Overview (Présentation du serveur)** > **Update (Mise à jour)** > **Server Component Update (Mise à jour des composants serveur)**. Il est également recommandé de sélectionner l'ensemble des modules des composants serveur devant être mis à jour simultanément. Ceci permet au service Lifecycle Controller d'utiliser ses algorithmes optimisés pour mettre à jour le micrologiciel et ainsi réduire le nombre d'amorçages.

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

Si le serveur ne prend pas en charge le service Lifecycle Controller, la section **Component/Device Firmware Inventory (Inventaire des micrologiciels des composants/terminaux)** affiche **Not Supported (Non pris en charge)**. Pour les serveurs nouvelle

génération, installez le micrologiciel Lifecycle Controller et mettez à jour le micrologiciel iDRAC afin d'activer le service Lifecycle Controller sur le serveur. Pour les serveurs de génération antérieure, cette mise à niveau n'est pas possible.

Normalement, le micrologiciel Lifecycle Controller est installé à l'aide d'un progiciel d'installation dédié exécuté sur le système d'exploitation du serveur. Pour les serveurs pris en charge, un progiciel de réparation ou d'installation spécial avec extension de fichier `.usc` est disponible. Ce fichier vous permet d'installer le micrologiciel Lifecycle Controller via la fonctionnalité de mise à jour micrologicielle disponible sur l'interface native du navigateur web iDRAC.

Vous pouvez aussi installer le micrologiciel Lifecycle Controller à l'aide d'un progiciel d'installation dédié exécuté sur le système d'exploitation du serveur. Pour plus d'informations, voir le document *Dell Lifecycle Controller User's Guide (Guide d'utilisation du service Dell Lifecycle Controller)*.

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

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

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
- BIOS
- Diagnostics (en option)
- Pack de pilotes du système d'exploitation (en option)
- RAID
- Carte réseau
- CPLD
- 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 du 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**.
- Dans la page **Menu principal de la configuration du système**, accédez à **Paramètres iDRAC** > **Lifecycle Controller** et cliquez sur **Activé**. Accédez à la page **Menu principal de configuration du système** et cliquez sur **Terminer** pour enregistrer les paramètres.
- L'annulation des services système vous permet d'annuler toutes les tâches planifiées en attente et de les supprimer de la file d'attente. Pour plus d'informations sur le Lifecycle Controller, les composants de serveur pris en charge et la gestion du micrologiciel de périphériques, voir le *Guide de démarrage rapide des services à distance du Lifecycle Controller* ou rendez-vous sur **delltechcenter.com/page/Lifecycle+Controller**.
- La page **Mise à jour des composants du serveur** permet de mettre à jour différents composants de micrologiciel sur le serveur. Pour pouvoir utiliser les fonctions de cette page, vous devez disposer des privilèges suivants pour les éléments ci-dessous :
  - Contrôleur CMC : Administrateur de serveur.
  - iDRAC : Configuration d'iDRAC et Connexion à iDRAC.

Si vos privilèges sont insuffisants, vous pouvez uniquement afficher l'inventaire des micrologiciels des composants et périphériques du serveur. Vous ne pouvez sélectionner aucun élément ni périphérique pour aucun type d'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 du 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.

Le **Filtre de mise à jour de composants/périphériques** à la page **Mise à jour des composants du serveur** vous permet de filtrer les informations en fonction du composant et est uniquement disponible en mode de **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.

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

Affichage de l'inventaire des micrologiciels à l'aide de 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 :

- Si serveur est répertorié comme **Non prêt**, cela indique que, lors de la collecte de l'inventaire des micrologiciels, l'iDRAC du serveur était encore en cours d'initialisation. Attendez que le contrôleur iDRAC soit pleinement opérationnel, puis actualisez la page pour récupérer à nouveau l'inventaire des micrologiciels.
- Un lien hypertexte est fourni. Celui-ci vous dirige vers une autre page permettant de mettre directement à jour le micrologiciel iDRAC uniquement. Cette page ne prend en charge que la mise à jour du micrologiciel iDRAC et ne gère aucun autre composant ou périphérique du serveur. La mise à jour du micrologiciel iDRAC est indépendante du service Lifecycle Controller.
- Si l'inventaire des composants et périphériques ne reflète pas les éléments physiquement installés sur le serveur, vous devez appeler le Lifecycle Controller pendant le processus d'amorçage du serveur. Cela permet d'actualiser les informations internes des composants et des périphériques et de vérifier les périphériques et composants actuellement installés. Cette situation existe dans les cas suivants :
  - 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 dans l'utilitaire Paramètres iDRAC, utilisez l'option correspondante accessible via la console d'amorçage :
  a. 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	Affiche le logement occupé par le serveur dans le châssis. Les numéros de logement sont les ID séquentiels de 4 logements disponibles dans le châssis : ● 1, 1a, 1b, 1c, 1d ● 2, 2a, 2b, 2c, 2d ● 3, 3a, 3b, 3c, 3d ● 4, 4a 4b, 4c, 4d, Ce schéma de numérotation vous permet d'identifier l'emplacement du serveur dans le châssis. Si moins de quatre serveurs occupent des logements, seuls les logements occupés par des serveurs s'affichent.
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.
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 *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge FX2/FX2s* 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 à l'aide de l'interface Web 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.
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 : Le **Nom du fichier** est optionnel uniquement lorsque le nom de fichier du catalogue par défaut est *catalog.xml*. Si le nom de fichier du catalogue est modifié, le nouveau nom doit être saisi dans ce champ.
   - Dossier de profil
   - Nom de domaine
   - Nom d'utilisateur
   - Mot de passe

   Pour en savoir plus, consultez l'*Aide en ligne de CMC pour Dell PowerEdge FX2/FX2s*.
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.
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 du 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. Sur la page **Mise à jour des composants du serveur**, cliquez sur le type approprié dans la section **Choisir le type de mise à jour**.
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 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→Mise à jour**.
2. Sur la page **Mise à jour des composants du serveur**, cliquez sur le type approprié dans la section **Choisir le type de mise à jour**.
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 85 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 85 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 à partir d'un fichier à l'aide de 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 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 le fichier**. Pour en savoir plus, reportez-vous à la section Sélection du type de mise à jour des composants du serveur
3. Dans la section **Filtre de mise à jour des composants/périphériques**, filtrez le composant ou périphérique (en option). Pour en savoir plus, voir CMC_Stmp_Filtrage des composants pour les mises à jour du micrologiciel.
4. Dans la colonne **Mise à jour**, cochez les cases des composants ou périphériques dont vous souhaitez mettre à jour le micrologiciel vers la nouvelle version. Utilisez la touche de raccourci CTRL pour sélectionner le type de composant ou de périphérique à mettre à jour sur l'ensemble des serveurs applicables. En appuyant sur la touche CTRL et en la maintenant enfoncée, vous mettez tous les composants en surbrillance en jaune. Tout en maintenant la touche CTRL 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 en savoir plus 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'applique 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.

Mise à jour des composants de serveur avec un seul clic à l'aide du partage réseau

La mise à jour des serveurs ou des composants du serveur à partir d'un partage réseau à l'aide de l'intégration du châssis modulaire Dell Repository Manager et Dell PowerEdge FX2/FX2s simplifie la mise à jour du micrologiciel à l'aide d'un groupe de micrologiciels personnalisés pour que vous puissiez déployer plus rapidement et plus facilement. La mise à jour à partir d'un partage réseau vous offre la possibilité de mettre à jour tous les composants des serveurs 12G en même temps grâce à un catalogue unique à partir d'un CIFS ou à partir d'un NFS.

Cette méthode fournit un moyen simple et rapide de créer une logithèque personnalisée de vos systèmes Dell à l'aide du Dell Repository Manager et le fichier d'inventaire du châssis exportés à l'aide de l'interface Web CMC. DRM vous permet de créer une logithèque personnalisée qui inclut uniquement les progiciels 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 une ligne de référentiel qui contient des mises à jour pour 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 vous permet d'enregistrer le référentiel vers un partage CIFS ou NFS. L'interface Web CMC vous permet de configurer les informations d'identification et l'emplacement pour le partage. À l'aide de l'interface Web CMC, vous pouvez effectuer la mise à jour des composants du serveur pour un seul serveur ou plusieurs serveurs.

Configuration requise à l'utilisation du mode de mise à jour de partage réseau

La configuration minimale suivante est requise pour mettre à jour le micrologiciel des composants du serveur à l'aide du mode de partage réseau :

- La licence iDRAC Enterprise doit être installée sur les serveurs
- Lifecycle Controller doit être activé sur les serveurs.
- Dell Repository Manager 1.8 ou un version ultérieure doit être installée sur votre système.
- Vous devez détenir des 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 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 à partir d'un partage réseau**. Pour plus d'informations, reportez-vous à la section Sélection du type de mise à jour du firmware des composants du serveur.
3. Si le partage réseau n'est pas connecté, configurez-le pour le châssis. Pour configurer ou modifier les détails du partage réseau, cliquez sur **Modifier** dans le tableau Propriétés du partage réseau. Pour plus d'informations, reportez-vous à la section Configuration du partage réseau à l'aide de l'interface Web 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. Cette logithèque est stockée dans le partage CIFS ou NFS configuré par CMC. 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 du client commercial Dell Repository Manager version 1.8*, disponibles à l'adresse **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 du firmware des composants et des périphériques pour ce même logement. Sinon, pour afficher de nouveau tous les détails, cliquez sur **Développer**.
6. Dans la section **Inventaire des firmwares des composants/périphériques**, cochez la case **Sélectionner/Désélectionner tout** pour sélectionner tous les serveurs pris en charge. Vous pouvez également cocher la case correspondant au serveur dont 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 : La colonne État de la tâche affiche l'état de la tâche des opérations planifiées sur le serveur. La condition de la tâche est mise à jour de manière dynamique.

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.

Restauration du micrologiciel iDRAC avec CMC

Vous mettez généralement à jour le micrologiciel iDRAC avec les interfaces iDRAC, notamment l'interface Web iDRAC, l'interface de ligne de commande SM-CLP ou des progiciels de mise à jour propres au système d'exploitation, téléchargés depuis le site **support.dell.com**. Pour en savoir plus, voir le manuel *Dell Integrated Dell Remote Access Controller (iDRAC) User's Guide* (Guide d'utilisation de l'iDRAC).

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
- Tous les serveurs, ou chaque serveur séparément
- Modules d'E/S
- Ventilateurs
- Unité d'alimentation (PSU)
- Capteurs de température
- Périphériques PCIe
- Chariots de stockage

Sujets :

Affichage des résumés 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 et les sous-graphiques des composants, ainsi que les info-bulles, sont automatiquement modifiés pour refléter l'état actuel.

Pour afficher l'intégrité du châssis, cliquez sur **Présentation du châssis**. Le système affiche l'état d'intégrité globale du châssis, du CMC, des modules de serveur, des modules d'E/S (IOM), des ventilateurs, des blocs d'alimentation, des traîneaux de stockage et des périphériques PCIe. Des informations détaillées sur chaque composant s'affichent lorsque vous cliquez sur ce composant. En outre, les derniers événements consignés dans le journal du matériel CMC s'affichent. Pour en savoir plus, voir le *Guide d'utilisation Dell Integrated Dell Remote Access Controller (iDRAC)*.

Si le châssis est configuré comme maître de groupe, la page **Intégrité du groupe** s'affiche après la connexion. Elle contient les informations et les alertes relatives au châssis. Toutes les alertes actives, critiques et non critiques sont visibles.

Graphiques du châssis

Le châssis est représenté par les vues avant et arrière (respectivement, les images supérieure et inférieure). Les serveurs et les KVM figurent dans la vue avant, les composants restants se trouvant dans la vue arrrière. La sélection des composants est indiquée en bleu et contrôlée en cliquant sur l'image du composant approprié. Lorsqu'un composant est présent dans le châssis, une icône de type de composant apparaît dans le graphique à l'emplacement dans lequel le composant est installé. Les emplacements vides sont indiqués par un arrière-plan 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 info-bulle contenant des informations supplémentaires sur le composant.

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 de composant 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 13. Propriétés des composants

Composant	Propriétés d'intégrité et de performances	Propriétés	Liens rapides
CMC	• Adresse MAC • IPv4 • IPv6	• Firmware • Dernière mise à jour • Matériel	• État du CMC • Mise en réseau • Mise à jour du firmware
Tous les serveurs et les serveurs individuels	• État de l'alimentation • Consommation électrique • Intégrité • Alimentation allouée • Température	• Nom • Modèle • Numéro de série • Nom de l'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 à la place.

Tous le stockage et les traîneaux de stockage individuels	Intégrité	• Nom
		• Modèle
		• Numéro de série
		• Numéro d'inventaire
		• Nombre de contrôleurs
		  ○ Logements de disque physique
		  ○ Connecté au serveur
		  ○ Fonctionnalité du mode du contrôleur
		• État d'intrusion
			• État de la baie de stockage
			• Configuration de la baie de stockage

Tableau 13. Propriétés des composants (suite)

Composant	Propriétés d'intégrité et de performances	Propriétés	Liens rapides
Blocs d'alimentation	État de l'alimentation	Capacité	• Condition des blocs d'alimentation • Consommation électrique • Bilan de puissance du système
Périphériques PCIe	• Installé • Attribué	• Modèle • Adressage • Numéro/ID fournisseur • ID de périphérique • Type de logement • Type de module • 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
Logement IOM	• État de l'alimentation • Rôle	• Modèle • Numéro de série	Condition 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, cliquez sur le nœud d'arborescence **Présentation du serveur**. Tous les serveurs (du LOGEMENT 01 au LOGEMENT 04) apparaissent dans la liste des serveurs. Si un serveur ne se trouve pas dans un logement, l'image correspondante est estompée dans le graphique.
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 nom du modèle de stockage et du numéro de service

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

1. Dans le volet de gauche, sous le nœud d'arborescence **Présentation du serveur**, tous les traîneaux de stockage apparaissent dans la liste. Si un traîneau de stockage ne se trouve pas dans un logement, l'image correspondante est grisée dans le graphique.
2. Pointez le curseur sur le numéro de logement du traîneau de stockage.
   Un conseil, le cas échéant, s'affiche avec le nom du modèle et le numéro de service du traîneau de stockage.

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 en savoir plus sur cette page, voir l'*Aide en ligne de CMC pour Dell PowerEdge FX2/FX2s*.

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 en savoir plus, voir l'*Aide en ligne de CMC pour Dell PowerEdge FX2/FX2s*.

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. L'état d'intégrité du serveur est indiqué par le sous-graphique de serveur. Pour en savoir plus, voir l'*Aide en ligne de CMC pour Dell PowerEdge FX2/FX2s*.
- 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 des informations et de la condition d'intégrité des traîneaux de stockage

Pour afficher la condition d'intégrité des traîneaux de stockage :

Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Présentation du serveur**, puis sélectionnez le traîneau de stockage.
La page **État de la matrice de stockage** affiche les propriétés des traîneaux de stockage et la liste de nœuds de stockage connectés au traîneau de calcul. Pour plus d'informations, voir l'*Aide en ligne*.

Affichage des informations et de la condition d'intégrité des modules 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 supérieure 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 en savoir plus, voir l'*Aide en ligne de CMC pour Dell PowerEdge FX2/FX2s*.

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 l'augmentant ou en la diminuant en fonction des événements système. Vous pouvez faire fonctionner le ventilateur dans trois modes : Faible, Moyen et Élevé (commande fanoffset). Pour en savoir plus sur la configuration d'un ventilateur, voir l'*Aide en ligne de CMC pour Dell PowerEdge FX2/FX2s*.

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 FX2/FX2s* sur le site dell.com/support/manuals.

REMARQUE : Le contrôleur CMC surveille les capteurs de température et règle automatiquement la vitesse des ventilateurs de manière appropriée. En cas de substitution à l'aide de cette commande, le contrôleur CMC fait toujours fonctionner un ventilateur à la vitesse sélectionnée, même si une telle vitesse n'est pas nécessaire pour le bon fonctionnement du châssis. Cependant, vous pouvez remplacer les valeurs pour maintenir une vitesse de ventilateur minimale en utilisant la commande `fanoffset`.

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 la mise à jour du micrologiciel CMC ou iDRAC sur un serveur, certains ou tous les ventilateurs du châssis tournent à 100 %. Ce comportement 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 section supérieure droite du graphique du châssis contient la vue supérieure gauche du châssis et la condition d'intégrité des ventilateurs. Cette condition est indiquée par le sous-graphique de ventilateur. Placez le pointeur sur le sous-graphique. L'info-bulle fournit des informations supplémentaires sur le ventilateur. Cliquez sur le sous-graphique de ventilateur pour afficher les informations du ventilateur dans le volet de droite.
2. Accédez à **Présentation du châssis** > **Ventilateurs**.
   La page **Condition des ventilateurs** indique la condition et les mesures de vitesse (en tours par minute, ou tr/mn) des ventilateurs du châssis. Il peut exister 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

Décalage de ventilateur : cette fonctionnalité vous permet d'augmenter la distribution du flux d'air dans les logements de carte PCIe. Un exemple d'utilisation de la fonctionnalité Décalage de ventilateur serait l'utilisation de cartes PCIe haute puissance ou personnalisées exigeant plus de refroidissement que la norme. La fonctionnalité Décalage de ventilateur est dotée des valeurs Désactivé, Faible, Moyen et Élevé. Ces valeurs correspondent à un décalage de vitesse de ventilateur (augmentation) de 20 %, 50 % et 100 % de la vitesse maximale, respectivement. Il existe également une configuration de vitesse minimale pour chaque valeur, qui est de 35 % pour la valeur Faible, de 65 % pour la valeur Moyen et de 100 % pour la valeur Élevé. Toutefois, selon la configuration, les vitesses minimales des valeurs Faible, Moyen et Élevé peuvent être supérieures à ces valeurs.

Une valeur de décalage de ventilateur moyenne, par exemple, augmente la vitesse du ventilateur de 50 % par rapport à sa vitesse maximale. L'augmentation est supérieure à la vitesse déjà définie par le système pour le refroidissement en fonction de la configuration matérielle installée.

Dès que l'une des valeurs de décalage de ventilateur est activée, la consommation électrique augmente. Le système est plus bruyant avec un décalage faible, nettement plus bruyant avec un décalage moyen, et encore plus bruyant avec un décalage élevé. Lorsque l'option Décalage de ventilateur n'est pas activée, les vitesses de ventilateur seront réduites aux vitesses par défaut requises pour le refroidissement du système de la configuration matérielle installée.

Pour définir la fonctionnalité de décalage, accédez à **Présentation du châssis** > **Ventilateurs** > **Configuration**. Sur la page **Configuration avancée du ventilateur**, effectuez la sélection appropriée dans la liste déroulante **Valeur** associée à la fonctionnalité **Décalage du ventilateur**.

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>]
```

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 KVM**
   - **Voyants du panneau avant**

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 :

Cliquez 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 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.

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 du contrôleur CMC afin de pouvoir gérer ce dernier à distance. Cette configuration initiale définit les paramètres de mise en réseau TCP/IP qui permettent d'accéder au contrôleur CMC.

Vous pouvez configurer le CMC à l'aide de l'interface Web ou à l'aide de RACADM pour configurer l'accès initial au CMC.

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 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.
- Ajouter et configurer des traîneaux de stockage.

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 :

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

Lorsqu'elle est activée, la fonctionnalité DHCP pour l'adresse de carte réseau (NIC) du 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 désactivée par défaut.

Vous pouvez activer le service DHCP pour obtenir automatiquement une adresse IP auprès du serveur DHCP.

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

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

Pour activer la fonction d'adresse DHCP pour DNS pour IPv6 et spécifier les adresses statiques préférées et alternatives du serveur DNS, entrez :

```
racadm config -g cfgIPv6LanNetworking -o
cfgIPv6DNSServersFromDHCP6 1
```

Définition des adresses IP statiques 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 <IP-address> racadm config -g
cfgLanNetworking -o cfgDNSServer2 <IPv4-address>
```

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

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

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 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 à l'aide de 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 des paramètres réseau (LAN) du contrôleur CMC à l'aide de l'interface RACADM

Pour afficher les paramètres IPv4, utilisez l'objet `cfgCurrentLanNetworking` avec les sous-commandes ci-dessous :

- `getniccfg`
- `getconfig`

Pour afficher les paramètres IPv6, utilisez l'objet `cfgIpv6LanNetworking` avec la sous-commande `getconfig`.

Pour afficher les informations sur l'adressage IPv4 et IPv6 du châssis, utilisez la sous-commande `getsysinfo`.

Pour plus d'informations sur les sous-commandes et les objets, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge FX2/FX2s*.

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 :

Si vous désactivez l'interface réseau CMC, l'opération de désactivation effectue les actions suivantes :

- Désactive l'accès de l'interface réseau à la gestion du châssis hors bande, notamment la gestion d'iDRAC et du module d'E/S.
- Empêche la détection du statut des liens vers le bas.

  Pour ne désactiver que l'accès réseau de CMC, désactivez tant le CMC IPv4 que le CMC IPv6.

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 : L'adressage IPv6 de CMC est désactivé par défaut.

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, le protocole DHCP est désactivé. Pour activer le protocole DHCP et utiliser le serveur DHCP sur le réseau afin d'attribuer une adresse IPv4, un masque de sous-réseau et une passerelle au contrôleur iDRAC ou CMC, saisissez :

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

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>
```

Configuration des paramètres du serveur 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.
- **Nom du contrôleur CMC** : par défaut, le nom du CMC sur le serveur DNS est cmc-*<service tag>*. Pour modifier le nom du CMC sur le serveur DNS, saisissez :

  ```
  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 maximal de caractères est de 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.
- **Nom de domaine DNS** : le nom de domaine DNS par défaut est un seul caractère vide. Pour définir un nom de domaine DNS, saisissez :

  ```
  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 du débit (IPv4 et IPv6)

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

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 à 1 (full duplex, valeur par défaut)

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

où :

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

Configuration du port de gestion 2

Le second port réseau du CMC peut être utilisé pour connecter en série des contrôleurs CMC dans le but de réduire le nombre de câbles, ou en tant que port redondant dans le cadre d'une opération de basculement de réseau. Le port de gestion **2** peut être connecté au commutateur de la partie supérieure du rack (TOR) ou à un autre commutateur. Il n'est pas nécessaire que les deux ports de carte d'interface réseau CMC soient connectés au même sous-réseau.

Le CMC doit être configuré pour prendre en charge la redondance de port du réseau de gestion avant d'être câblé pour cette opération. Le CMC doit utiliser une connexion réseau unique standard pour le déploiement. Une fois le déploiement effectué, une seconde connexion redondante peut alors être établie.

REMARQUE : Lorsque le port de gestion 2 est configuré pour la redondance mais est câblé pour l'empilage, les CMC en aval (les plus éloignés du commutateur de la partie supérieure du rack (TOR)) n'ont pas de liaison réseau.

REMARQUE : Lorsque le port de gestion 2 est activé pour l'empilage, mais câblé pour la redondance (deux connexions au commutateur TOR), les boucles de routage risquent de créer un orage réseau.

Pour spécifier l'opération de redondance, utilisez la commande `racadm config -g cfgNetTuning -o cfgNetTuningNicRedundant 1`.

Pour spécifier l'opération d'empilage, utilisez la commande `racadm config -g cfgNetTuning -o cfgNetTuningNicRedundant 0`.

Par défaut, le port de gestion 2 est activé pour l'empilage.

Configuration du port de gestion 2 à l'aide de l'interface Web CMC

Pour configurer le port de gestion à l'aide de l'interface Web du CMC :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Réseau**, puis cliquez sur l'onglet **Réseau** .
2. Sur la page **Configuration réseau**, dans la section **Paramètres généraux**, en regard de **Port de gestion 2**, sélectionnez **Redondant** ou **Empilage**.
3. Cliquez sur **Appliquer les changements**.
   - Lorsque le port de gestion 2 est configuré pour la redondance et qu'il est câblé pour l'empilage, les contrôleurs CMC en aval (les plus éloignés du commutateur TOR (Top-of-Rack) n'ont pas de liaison réseau.
   - Lorsque le port de gestion 2 est activé pour l'empilage, mais câblé pour la redondance (deux connexions au commutateur TOR), les boucles de routage risquent de créer un orage réseau.

Configuration du port de gestion 2 à l'aide de RACADM

Pour spécifier l'opération de redondance, utilisez la commande `racadm config -g cfgNetTuning -o cfgNetTuningNicRedundant 1`.

Pour spécifier l'opération d'empilage, utilisez la commande `racadm config -g cfgNetTuning -o cfgNetTuningNicRedundant 0`.

Par défaut, le port de gestion 2 est activé pour l'empilage.

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 distante : permet d'accéder au CMC à l'aide de 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.

REMARQUE : Lors de la modification des numéros de port de service du CMC avec SSH, Telnet, HTTP ou HTTPS, évitez d'utiliser des ports fréquemment utilisés par les services du système d'exploitation comme le port 111. Voir les ports réservés par IANA (Internet Assigned Numbers Authority) à l'adresse http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml.

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.

Les ports réseau réservés pour les communications CMC et iDRAC sont les suivants : 21, 68, 69, 123, 161, 546, 801, 4003, 4096, 5985 à 5990, 6900 et 60106.

Configuration des services à l'aide de RACADM

Pour activer et configurer les services, utilisez les objets RACADM suivants :

- `cfgRacTuning`
- `cfgRacTuneRemoteRacadmEnable`

Pour plus d'informations sur ces objets, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge FX2/FX2s* disponible 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 en savoir plus sur ces options, voir l'*Aide en ligne de CMC pour Dell PowerEdge FX2/FX2s*.
3. Cliquez sur **Appliquer** pour appliquer l'option sélectionnée.

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 des serveurs ou châssis membres.
- 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 19 membres. De plus, un maître ou un membre ne peut appartenir qu'à un seul groupe. Vous ne pouvez pas rejoindre un châssis, en tant que maître ou membre, qui est 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 en utilisant les 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.

REMARQUE : Une fois le groupe de châssis créé, l'objet **Présentation du châssis** dans la structure de l'arborescence est remplacé par le nom du châssis maître.

Ajout de membres à un groupe de châssis

Une fois le groupe de châssis défini, ajoutez-y des membres en procédant comme suit :

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**.

   REMARQUE : Pour que MCM fonctionne correctement, vous devez utiliser le port HTTPS par défaut (443) sur tous les membres du groupe et le châssis principal.

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 l'option **Synchroniser le nouveau membre avec les propriétés du maître** pour envoyer les propriétés du maître au membre. Pour plus d'informations, voir « Synchronisation d'un nouveau membre avec les propriétés du châssis maître ».
8. Cliquez sur **Appliquer**.
9. Pour ajouter jusqu'à 19 membres, 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 messages. 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**.

Lancement de 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 du châssis maître. Si le périphérique membre possède les mêmes informations d'identification de connexion que le châssis maître, vous pouvez utiliser ces informations d'identification pour accéder au périphérique membre.

REMARQUE : L'authentification unique et la connexion par carte à puce ne sont pas prises en charge dans la gestion de plusieurs châssis. Le lancement de membres via une authentification unique depuis le châssis maître nécessite un nom d'utilisateur/mot de passe commun entre le châssis maître et les membres. L'utilisation d'un nom d'utilisateur/mot de passe commun ne fonctionne qu'avec les utilisateurs locaux, Active Directory 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 vous essayez de vous connecter au châssis membre avec l'option **Lancer CMC** lorsque le maître et le châssis ont le mode FIPS activé ou désactivé, vous êtes redirigé vers la page **Intégrité du groupe du châssis**. Sinon, vous êtes redirigé vers la page **Connexion** du châssis membre.

   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 avec la page de destination ou l'écran de connexion.

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

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*.

Synchronisation d'un nouveau membre avec les propriétés du châssis maître

Vous pouvez appliquer les propriétés du maître à un châssis membre nouvellement ajouté à un groupe. Pour synchroniser un nouveau membre avec les propriétés du maître :

1. Connectez-vous au châssis maître avec les privilèges d'Administrateur.
2. Sélectionnez le châssis maître dans l'arborescence.
3. Cliquez sur **Configuration** > **Administration des groupes**.
4. Lorsque vous ajoutez un nouveau membre au groupe, ouvrez la page **Groupe de châssis** et sélectionnez **Synchroniser le nouveau membre avec les propriétés du maître**.
5. Cliquez sur **Appliquer**. Le membre prend les propriétés du leader.

Les propriétés du service de configuration suivantes de plusieurs systèmes dans le châssis sont affectées après la synchronisation:

Tableau 14. Propriétés du service de configuration

Propriété	Navigation
Configuration de SNMP	Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Réseau** > **Services** > **SNMP**.
Connexion à distance à un châssis	Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Réseau** > **Services** > **Syslog distant**.
Authentification d'utilisateur à l'aide de services LDAP et Active Directory	Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Authentification utilisateur** > **Services d'annuaire**.
Alertes de châssis	Dans le volet de gauche, cliquez sur **Présentation du châssis** et cliquez sur **Alertes**.

Inventaire des serveurs pour un groupe CMC

Un groupe est un châssis maître contenant de 0 à 19 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). ;
- Logements vides et logements d'extension.

Enregistrement du rapport d'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.

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*.

Importation des profils de configuration du châssis

Vous pouvez importer les profils de configuration du châssis stockés sur un partage réseau vers la station de gestion locale.

Pour importer un profil stocké sur un partage de fichiers distant vers le contrôleur CMC, effectuez les tâches suivantes :

1. Accédez à la page **Profils de configuration du châssis**. Dans la section **Profils de configuration du châssis** > **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**.

REMARQUE : Vous pouvez importer les profils de configuration du châssis à l'aide de RACADM. Pour plus d'informations, voir le *Guide de référence de la ligne de commande RACADM de Dell Chassis Management Controller pour PowerEdge M1000e*.

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 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>
```

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. Ouvrez une console texte Telnet/SSH sur CMC, ouvrez une session et 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 du contrôleur 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.

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 colonne 1. Un caractère « # » présent dans toute autre colonne est traité comme un caractère # classique.

  Certains paramètres de modem peuvent inclure des caractères # dans leurs chaînes. Aucun caractère d'échappement n'est requis. Vous pouvez être amené à générer un fichier `.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 colonne 1. Ce nom de groupe doit être spécifié avant tous les objets de ce groupe. Les objets n'incluant aucun nom de groupe associé génèrent une erreur. Les données de configuration sont organisées en groupes, comme défini dans le chapitre relatif aux propriétés de la base de données du document *Guide de référence de la ligne de commande RACADM pour iDRAC et CMC*. L'exemple suivant affiche un nom de groupe, un objet et 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 blanc à l'intérieur d'une chaîne de valeurs reste inchangé. Tout caractère placé à droite du signe = (par exemple, un second =, un symbole #, [,], etc.) est pris en compte tel quel. Ces caractères sont des caractères valides pour les scripts de chat de modem.

  ```
  [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, il est utilisé ou 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 1-16> <unique anchor name>
  ```

- La ligne d'un groupe indexé ne peut pas être supprimée à partir 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 vous signale l'erreur.

  Vous devez supprimer un objet indexé manuellement en utilisant la commande suivante :

  ```
  racadm config -g <groupname>  -o <objectname> -i <index 1-16> ""
  ```

  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 1-16>
  ```

- Pour les groupes indexés, l'objet Anchor doit être le premier objet après la paire de crochets [ ]. Vous trouverez ci-dessous des exemples de groupes indexés actuels :

```
[cfgUserAdmin]
cfgUserAdminUserName= <USER_NAME>
```

- Lorsqu'une commande RACADM distante est utilisée pour capturer les groupes de configuration dans un fichier, si une propriété de clé d'un groupe n'est pas définie, le groupe de configuration n'est pas enregistré dans le cadre du fichier de configuration. Si vous avez besoin de cloner ces groupes de configuration sur d'autres CMC, la propriété de clé doit être définie avant l'exécution de 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 via 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=192.x.x.x
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`.

7

Configuration des serveurs

Vous pouvez définir les paramètres suivants d'un serveur :

- Noms de logement
- Paramètres réseau d'iDRAC
- Paramètres de balise VLAN DRAC
- Périphérique de démarrage initial
- FlexAddress de serveur
- Partage de fichier à distance
- Paramètres BIOS en utilisant un clone de serveur

Sujets :

Configuration des noms de logement

Les noms de logement permettent d'identifier chaque serveur. Les règles suivantes s'appliquent au choix des noms de logement :

- Les noms peuvent contenir un maximum de 15 caractères ASCII non étendus (codes ASCII de 32 à 126). Également standard et les caractères spéciaux ne sont pas autorisés dans les noms.
- Les noms de logement doivent être uniques dans le châssis. Il ne peut pas exister deux logements de même nom.
- Les chaînes ne sont pas sensibles à la casse. `Server-1, server-1, and SERVER-1` sont des noms identiques.
- Les noms de logements ne doivent pas commencer par les chaînes de caractères suivantes :
  - `Switch-`
  - `Fan-`
  - `PS-`
  - `DRAC-`
  - `MC-`
  - `Chassis`
  - `Housing-Left`
  - `Housing-Right`
  - `Housing-Center`
- Les chaînes `Server-1` à `Server-4` peuvent être utilisées, mais uniquement pour le logement correspondant. Par exemple, `Server-3` est un nom valide pour le logement 3, mais pas pour le logement 4. Par contre, `Server-03` est valide pour n'importe quel logement.

  REMARQUE : Pour renommer un logement, vous devez disposer du privilège **Administrateur de configuration du châssis**.

Le paramètre de nom de logement défini dans l'interface Web réside uniquement dans le contrôleur CMC. Si vous retirez un serveur du châssis, il ne reste pas affecté au 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 de logement, sélectionnez l'option **Utiliser le nom d'hôte comme nom de logement**. Vous remplacez ainsi les noms de logement statiques par le nom d'hôte (nom système) du serveur, s'il existe. Pour cela, vous devez avoir installé l'agent OMSA sur le serveur. Pour plus d'informations sur l'agent OMSA, voir le *Guide d'utilisation de Dell OpenManage Server Administrator*.
4. Pour utiliser le nom DNS d'iDRAC comme nom de logement, sélectionnez l'option **Utiliser le nom DNS d'iDRAC comme nom de logement**. 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 un serveur pour le nom de logement par défaut (LOGEMENT-01 à LOGEMENT-4), en fonction de la position du logement d'un serveur), cliquez sur **Restaurer la valeur par défaut**.

Configuration des paramètres réseau d'iDRAC

Pour utiliser cette fonction, vous devez disposer d'une licence d'entreprise. Vous pouvez définir les paramètres de configuration réseau iDRAC d'un serveur. Vous pouvez utiliser les paramètres QuickDeploy pour définir les paramètres de configuration réseau iDRAC par défaut et le mot de passe root des serveurs installés ultérieurement. Ces paramètres par défaut sont les paramètres QuickDeploy iDRAC.

Pour en savoir plus sur iDRAC, voir le manuel *iDRAC User's Guide* (Guide d'utilisation d'iDRAC) à l'adresse dell.com/support/manuals.

Configuration des paramètres réseau QuickDeploy d'iDRAC

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 répertoriés dans le tableau suivant. Pour plus d'informations sur les champs, voir l'*Aide en ligne*.

Tableau 15. Paramètres QuickDeploy

Paramètre	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 de l'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. • **Quick Deploy et profil de serveur** : sélectionnez cette option pour appliquer les paramètres réseau de l'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**, ce mot de passe est affecté à l'utilisateur root iDRAC d'un serveur lorsque vous insérez le serveur dans le châssis. Ce mot de passe peut contenir de 1 à 20 caractères imprimables (espaces compris).

Tableau 15. Paramètres QuickDeploy (suite)

Paramètre	Description
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	Permet d'activer ou de désactiver le canal LAN iDRAC. Par défaut, cette option est désactivée.
Activer IPv4 pour iDRAC	Permet d'activer ou de désactiver IPv4 sur iDRAC. Par défaut, cette option est sélectionnée.
Activer IPMI sur le LAN pour iDRAC	Permet d'activer ou de désactiver la fonction IPMI sur canal LAN de chaque iDRAC présent dans le châssis. Par défaut, cette option est sélectionnée.
Activer le protocole DHCP IPv4 pour iDRAC	Permet d'activer ou de désactiver DHCP pour chaque iDRAC présent dans le châssis. Si vous activez cette option, les champs **Adresse IP QuickDeploy**, **Masque de sous-réseau QuickDeploy** et **Passerelle QuickDeploy** sont désactivés et vous ne pouvez pas les modifier, puisque DHCP sert à attribuer automatiquement ces paramètres pour chaque iDRAC. Pour pouvoir sélectionner cette option, vous devez sélectionner l'option **Activer IPv4 pour iDRAC**. L'option Adresse IP Quick Deploy est fournie avec les valeurs 4 et 2.
Adresse IP QuickDeploy réservée	Sélectionnez le nombre d'adresses IPv4 statiques réservées aux iDRAC dans le châssis. Les adresses IPv4 commençant à partir de l'**adresses IPv4 de l'iDRAC de départ (Logement 1)** sont considérées comme réservées et sont supposées ne pas être utilisées nulle part ailleurs sur le même réseau. La fonction Quick Deploy ne fonctionne pas pour les serveurs insérés dans les logements pour lesquels il n'existe aucune adresse IPv4 statique réservée.
Première adresse IPv4 d'iDRAC (logement 1)	Spécifie l'adresse IP statique de l'iDRAC du serveur installé dans le logement 1 de l'enceinte. 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 début est `192.168.0.250` et que le masque de sous-réseau est `255.255.0.0`, l'adresse IP QuickDeploy du logement 4c est `192.168.0.265`. Si le masque de sous-réseau est `255.255.255.0`, un message d'erreur signale que `QuickDeploy IP address range is not fully within QuickDeploy Subnet` 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	Active les paramètres du serveur DNS du CMC (IPv4 et IPv6) qui sont propagés à l'iDRAC lorsqu'un serveur lame est inséré dans le châssis.

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 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.

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 s'appliquent immédiatement. Par contre, il faut parfois quelques minutes pour que les modifications apportées aux paramètres de configuration réseau d'un ou plusieurs serveurs iDRAC soient propagées du contrôleur CMC au contrôleur l'iDRAC. Si vous cliquez trop tôt sur **Actualiser**, le système risque d'afficher uniquement des données partiellement correctes pour un ou plusieurs serveurs iDRAC.

Attributions d'adresses IP QuickDeploy aux serveurs

Les tableaux suivants indiquent la façon dont les adresses IP QuickDeploy sont attribuées aux serveurs en fonction des chariots présents dans le châssis FX2/FX2s :

- Deux chariots pleine largeur dans le châssis :

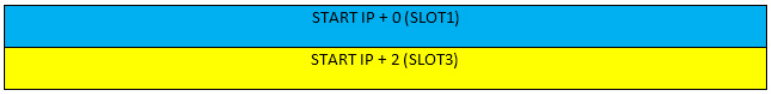


Figure 3. Deux traîneaux pleine largeur dans le châssis

- Quatre chariots demi-largeur dans le châssis :

Figure 4. Quatre traîneaux demi-largeur dans le châssis

- Huit chariots quart de largeur dans le châssis :

  REMARQUE : Les **Adresses IP QuickDeploy réservées** doivent être définies sur un minimum de 8.

Figure 5. Huit traîneaux quart de largeur dans le châssis

- Quatre chariots FM120x4 dans le châssis :

  REMARQUE : Les **Adresses IP QuickDeploy réservées** doivent être définies sur 16.

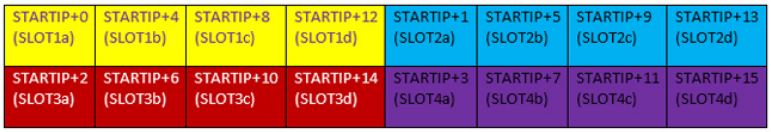


Figure 6. Quatre traîneaux FM120x4 dans le châssis

- La rangée du haut contient uniquement des chariots quart de largeur et la rangée du bas contient uniquement des chariots demi-largeur :

  REMARQUE : Les **Adresses IP QuickDeploy réservées** doivent être définies sur un minimum de 8.

Figure 7. Traîneaux quart de largeur dans la rangée du haut et traîneaux demi-largeur dans la rangée du bas

- La rangée du haut contient uniquement des chariots pleine largeur et la rangée du bas contient uniquement des chariots demi-largeur :

Figure 8. Traîneaux pleine largeur dans la rangée du haut et traîneaux demi-largeur dans la rangée du bas

- La rangée du haut contient des chariots pleine largeur et la rangée du bas contient uniquement des chariots quart de largeur :

  REMARQUE : Les **Adresses IP QuickDeploy réservées** doivent être définies sur un minimum de 8.

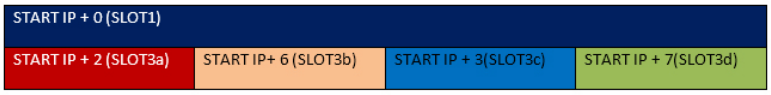


Figure 9. Traîneaux pleine largeur dans la rangée du haut et traîneaux quart de largeur dans la rangée du bas

Modification des paramètres réseau iDRAC de chaque iDRAC de serveur

Cette fonction permet de définir les paramètres de configuration réseau iDRAC de chaque serveur installé. Les valeurs initiales affichées de chacun des champs sont les valeurs en cours lues dans 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 réseau iDRAC** répertorie les paramètres de configuration réseau IPv4 et IPv6 iDRAC 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 LAN** pour spécifier les paramètres IPv4 ou IPv6. Pour en savoir plus sur les champs, voir l'*Aide en ligne de CMC pour Dell PowerEdge FX2/FX2s*.

3. Pour déployer les paramètres dans iDRAC, cliquez sur **Appliquer les paramètres réseau iDRAC**. Si vous avez modifié les **paramètres QuickDeploy**, ils sont également enregistrés.

   La table **Paramètres réseau iDRAC** reflète les futurs paramètres de configuration réseau ; les valeurs affichées pour les serveurs installés ne sont pas forcément identiques aux paramètres de configuration réseau des iDRAC actuellement installés. Cliquez sur **Actualiser** pour mettre à jour la page **Déployer iDRAC** avec les paramètres de configuration réseau de chaque iDRAC installé après réalisation des modifications.

   REMARQUE : Les modifications apportées aux champs QuickDeploy s'appliquent immédiatement. Par contre, il faut parfois quelques minutes pour que les modifications apportées aux paramètres de configuration réseau d'un ou plusieurs serveurs iDRAC soient propagées de CMC vers l'iDRAC. Si vous cliquez trop rapidement sur **Actualiser**, le système risque d'afficher uniquement des données partiellement correctes pour un ou plusieurs serveurs iDRAC.

Modification des paramètres réseau iDRAC à l'aide de RACADM

Les commandes RACADM `config` ou `getconfig` prennent en charge l'option `-m <module>` pour les groupes de configuration suivants :

- `cfgLanNetworking`
- `cfgIPv6LanNetworking`
- `cfgRacTuning`
- `cfgRemoteHosts`
- `cfgSerial`
- `cfgSessionManagement`

Pour en savoir plus sur les valeurs par défaut des propriétés et sur les plages, voir le *Guide de référence de la ligne de commande RACADM de Dell Integrated Dell Remote Access Controller (iDRAC)* et le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge FX2/FX2s* à l'adresse **dell.com/support/manuals**.

Configuration des paramètres de marquage VLAN iDRAC

Les réseaux VLAN permettent à plusieurs réseaux LAN virtuels de coexister sur le même câble réseau physique et de séparer le trafic réseau à des fins de sécurité ou de gestion de la charge. Lorsque vous activez la fonctionnalité VLAN, une balise VLAN est attribuée à chaque paquet réseau. Les balises VLAN sont des propriétés de châssis. Elles demeurent associées au châssis même lorsque vous retirez un composant.

REMARQUE : Les paramètres VLAN de l'iDRAC du CMC sont effectifs uniquement lorsque la sélection de carte réseau iDRAC est définie sur le contrôleur iDRAC en mode LOM (dédié) de châssis.

REMARQUE : L'ID du réseau VLAN configuré à l'aide du contrôleur CMC est appliqué au contrôleur iDRAC uniquement lorsque celui-ci est en mode dédié. Si le contrôleur iDRAC est en mode LOM partagé, les modifications apportées à l'ID du réseau VLAN dans le contrôleur iDRAC ne s'affichent pas dans l'interface GUI du contrôleur CMC.

Configuration des paramètres de marquage VLAN iDRAC dans l'interface Web

Pour configurer VLAN pour un 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 en savoir plus sur les champs, voir l'*Aide en ligne de CMC pour Dell PowerEdge FX2/FX2s*.
3. Cliquez sur **Appliquer** pour enregistrer les paramètres.

Configuration des paramètres de marquage VLAN iDRAC avec RACADM

- Spécifiez l'ID de VLAN 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 16.

  Par exemple :

  ```
  racadm setniccfg -m server-1 -v
  ```

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 sur 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 jusqu'à ce que vous le changiez à nouveau dans l'interface Web CMC 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. Cependant, pour définir un périphérique en tant que premier périphérique de démarrage par défaut, sélectionnez **Défaut**.

Pour ne pas remplacer la version de micrologiciel du serveur si la version du micrologiciel exécutée sur le serveur est la même que celle disponible dans le premier périphérique de démarrage, sélectionnez **Aucun**.

Vous pouvez définir les périphériques suivants comme premier périphérique de démarrage.

Tableau 16. 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 l'aide d'un lecteur de disque dur.
CD/DVD local	Démarrage à partir d'un lecteur de CD/DVD sur le serveur.
Configuration du BIOS	Démarrage lors de la configuration du BIOS.
Disquette virtuelle	Démarrage à partir d'une disquette virtuelle.
CD/DVD virtuel	Démarrage à partir d'un lecteur de CD ou de DVD virtuel.
Carte SD locale	Démarrage à partir de la carte SD (Secure Digital) locale.
Partage de fichier à distance	Démarrage à partir du partage de fichiers distant.
BIOS Boot Manager (Gestionnaire d'amorçage du BIOS)	Démarrage à l'aide du gestionnaire d'amorçage du BIOS.
Lifecycle Controller	Démarrage à l'aide du Lifecycle Controller.
Disquette locale	Démarrage à partir d'une disquette insérée dans le lecteur local de disquette.

Définition du premier périphérique d'amorçage pour plusieurs serveurs à l'aide de 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 d'un seul serveur à l'aide de 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 RACADM

Pour définir le premier périphérique de démarrage, utilisez l'objet `cfgServerFirstBootDevice`.

Pour activer l'option de démarrage ponctuel pour un périphérique, utilisez l'objet `cfgServerBootOnce`.

Pour en savoir plus sur ces objets, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge FX2s* disponible à l'adresse dell.com/support/manuals.

Configuration de données sortantes réseau de traîneau

Vous pouvez configurer les données sortantes de réseau de traîneau uniquement sur les traîneaux PowerEdge FM120x4 qui contiennent un commutateur réseau interne.

Pour configurer les données sortantes de réseau de traîneau, accédez à **Présentation du châssis** > **Présentation du serveur** > **Configuration** > **Données sortantes de réseau de traîneau**

Sélectionnez l'une des valeurs suivantes pour la propriété de configuration de données sortantes de réseau de chariot :

- **Standard (regroupé)** : la configuration des données sortantes où les quatre ports de données sortantes IOM sont configurés en un seul groupe de faisceaux et tous les LOM sont adressés à ce groupe. Cette option est sélectionnée par défaut.
- **Isolation de l'adaptateur réseau (sécurité optimisée)** : configuration de données sortantes semblable à la configuration standard, mais le routage entre les nœuds locaux n'est pas autorisé.
- **Réseaux isolés** : configuration de données sortantes où le LOM1 de chaque nœud est adressé au Module IOM A1 et le LOM2 est adressé au module IOM A2.
- **Isolation optimisée de la carte réseau** : configuration de données sortantes pour une sécurité renforcée dans les configurations multiclients. Cette configuration isole les différentes cartes réseau avec un port IOM dédié adressé au LOM de chaque nœud. Seul le LOM1 de chaque nœud est opérationnel.

REMARQUE : Lors de la rétrogradation depuis le CMC version 1.3 ou version supérieure, si la **Configuration de données sortantes réseau de traîneau** est définie sur **Isolation optimisée de la carte réseau** , la **Configuration de données sortantes réseau de**

traîneau est vide dans le CMC 1.2 ou versions inférieures. Dans l'interface de ligne de commande, la valeur non valide '4' s'affiche en tant que sortie de la commande suivante :

```
$ getconfig -g cfgRacTuning -o cfgRacTuneSledNetworkUplink
```

Déploiement d'un partage de fichier à distance

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 Enterprise.

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 **Deploy Remote File Share (Déployer le partage de fichiers distant)**, entrez les données appropriées dans les champs. Pour en savoir plus sur les descriptions de champ, voir l'*Aide en ligne du contrôleur CMC pour Dell PowerEdge FX2/FX2s*.
3. Pour vous connecter à un partage de fichiers distant, cliquez sur **Connect (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 d'amorçage pour les serveurs.
   - Le serveur est redémarré.
   - Le serveur est mis sous tension s'il est hors tension.

Configuration de FlexAddress pour un 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 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 comprend uniquement les paramètres BIOS d'un serveur.
- BIOS et amorçage : ce groupe comprend les paramètres de BIOS et d'amorçage d'un serveur.
- Tous les paramètres : cette version comprend tous les paramètres du serveur et des composants de ce serveur. Ces profils sont générés depuis :
  - Les serveurs de 12e génération avec iDRAC7 1.57.57 ou version ultérieure et Lifecycle Controller 2 version 1.1 ou ultérieure
  - Les serveurs de 13e génération avec iDRAC8 2.05.05 et Lifecycle Controller 2.00.00.00 ou version ultérieure.

La fonction de clonage de serveur prend en charge les serveurs iDRAC7 et iDRAC8. Les serveurs RAC de génération antérieure sont répertoriés, mais ils sont grisés sur la page principale et ils ne peuvent pas utiliser cette fonction.

Pour utiliser la fonction de réplication des configurations de serveur :

- iDRAC doit avoir la version minimale nécessaire. Les serveurs iDRAC7 nécessitent la version 1.57.57. Les serveurs iDRAC8 nécessitent la version 2.05.05.
- 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 des 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 **Quick Deploy**.
- Afficher les activités dans le journal pour des tâches récentes d'un profil de serveur.

Accès à la page Profil

Vous pouvez ajouter, gérer et appliquer des profils à un ou plusieurs serveurs à l'aide de la page **Profil**.

Pour accéder à la page **Profil** à l'aide de l'interface Web du CMC, dans le volet de gauche, cliquez sur**Présentation du châssis** > **Présentation du serveur** > **Configurer** > **Profils.**La page **Profils** s'affiche.

Gestion des profils stockés

Vous pouvez modifier, afficher ou supprimer les profils BIOS. Pour gérer les profils stockés d'un contrôleur CMC :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Présentation du serveur** > **Configurer** > **Profils**.
2. Dans la page **Profils**, sous **Appliquer un profil**, cliquez sur **Gérer les profils**. La page **Gérer les profils BIOS** s'affiche.

- Pour modifier un profil, cliquez sur **Modifier**.
- Pour afficher les paramètres BIOS, cliquez sur **Afficher**.
- Pour supprimer un profil, cliquez sur **Supprimer**. Pour en savoir plus sur les descriptions des champs, voir l'*Aide en ligne de CMC pour Dell PowerEdge FX2/FX2s*.

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 un nom et une description facultative pour 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 à l'aide du stockage étendu et du partage distant du CMC. Pour en savoir plus, voir la section Configuration d'un Partage réseau à l'aide de l'interface Web du CMC

La suppression (ou la désactivation) de supports de stockage étendu non volatile empêche l'accès aux profils stockés et désactive la fonction de clonage de serveur.

Pour ajouter un profil :

1. Accédez à la page **Profils de serveur**. Dans la section **Profils de serveur**, cliquez sur **Appliquer et enregistrer les profils**.
2. Sélectionnez le serveur dont les paramètres vous souhaitez utiliser pour générer le profil, puis cliquez sur **Enregistrer le profil**. La section **Enregistrer le profil** s'affiche.
3. Sélectionnez **Stockage étendu** ou **Partage réseau** comme emplacement d'enregistrement du profil.

   REMARQUE : L'option Partage réseau est activée et les détails s'affichent dans la section Profils stockés uniquement si le partage réseau est chargé et accessible. Si le Partage réseau n'est pas connecté, configurez le Partage réseau pour le châssis. Pour configurer le Partage réseau, cliquez sur Modifier dans la section Profils stockés. Pour en savoir plus, voir la section Configuration d'un Partage réseau à l'aide de l'interface Web du CMC

4. Dans les champs **Nom du profil** et **Description**, entrez le nom du profil et une description de celui-ci (facultatif), puis cliquez sur **Enregistrer le profil**.

   REMARQUE :

   Lors de l'enregistrement d'un profil de serveur. la liste des caractères qui ne sont pas pris en charge par le Nom de profil incluent le caractère dièse (#), la virgule (,) et le point d'interrogation (?).

   Le jeu de caractères ASCII standard est pris en charge. 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 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 d'un profil

Le clonage des serveurs est possible uniquement si les profils de serveur sont disponibles en tant que profils stockés dans le support non volatile sur le CMC. Pour lancer une opération de clonage de serveur, appliquez un profil stocké à un ou plusieurs serveurs.

Pour chaque serveur, l'état, le numéro de logement et le nom du type d'opération sont affichés dans le tableau **Appliquer un profil**.

REMARQUE : Si un serveur ne prend pas en charge le Lifecycle Controller 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. Dans 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 et triés par type, y compris ceux qui se trouvent sur l'espace de stockage 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**.

   Le message d'avertissement suivant s'affiche : l'application d'un nouveau profil va écraser les paramètres actuels et également redémarrer les serveurs sélectionnés. Vous êtes invité à confirmer si vous souhaitez continuer l'opération.

   REMARQUE : Pour effectuer des opérations de clonage de serveur, l'option CSIOR doit être activée sur les serveurs. Si elle est désactivée, un message d'avertissement s'affiche indiquant que l'option CSIOR n'est pas activée sur les serveurs. Pour terminer l'opération de clonage de lame, veillez à activer l'option CSIOR sur les serveurs.

4. Cliquez sur **OK** pour appliquer le profil au serveur sélectionné.

   Le profil sélectionné est appliqué aux serveurs et les serveurs peuvent être redémarré(s) immédiatement. Pour en savoir plus, voir l'*Aide en ligne de CMC pour Dell PowerEdge FX2/FX2s*.

Importation de profil

Vous pouvez importer vers le CMC un profil de serveur qui est stocké sur une station de gestion distante.

Pour importer un profil stocké depuis CMC :

1. Dans la page **Profil 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**.

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

Exportation de profil

Vous pouvez exporter un profil de serveur stocké vers un chemin spécifié 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 d'avertissement s'affiche si le profil est exporté et la description est perdue. Appuyez 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 chargé et accessible. Si le Partage réseau n'est pas connecté, configurez le Partage réseau pour le châssis. Pour configurer le Partage réseau, cliquez sur **Modifier** dans la section **Profils stockés**. Pour en savoir plus, voir la section Configuration du partage réseau à l'aide de l'interface Web CMC
   - Carte locale ou SD si le fichier source se situe sur le partage réseau.

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

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 BIOS — <Nom de profil>** 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.

Affichage des paramètres de profil

Pour afficher l'option 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 de serveur** correspondant au serveur souhaité. La page **Paramètres d'affichage** 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 l'option CSIOR, après avoir redémarré le serveur, activez l'écran de configuration avec **F2**, sélectionnez **Paramètres d'iDRAC** > **Lifecycle Controller**, puis activez **CSIOR** et enregistrez les changements.

Pour activer CSIOR :

1. Serveurs 12e génération : après avoir redémarré le serveur, activez l'écran de configuration avec F2, sélectionnez **Paramètres d'iDRAC** > **Lifecycle Controller**, puis activez **CSIOR** et enregistrez les modifications.
2. 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 **Collecte de l'inventaire système au redémarrage**.

Affichage des paramètres de profil stockés

Pour afficher les paramètres des profils de serveur stockés, accédez à la page **Profils de serveur**. Dans la section **Profils de serveur**, cliquez sur **Afficher** dans la colonne **Afficher le profil** du serveur souhaité. La page **Paramètres d'affichage** s'affiche. Pour en savoir plus sur les paramètres affichés, voir l'*Aide en ligne de CMC pour Dell PowerEdge FX2/FX2s*.

Affichage du journal de profil

Pour afficher le journal de profil, à la page **Profils du serveur**, voir la section **Journal de profil récent**. Cette section répertorie les 10 dernières entrées du journal de profil directement depuis les opérations de clonage du serveur. Chaque entrée du journal affiche la gravité, l'heure et la date de soumission de l'opération de réplication de la configuration du serveur, ainsi que la description du message 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 la l'*Aide en ligne*.

Condition 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** > **Configuration** > **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 le même ID de tâche (JID) 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 depuis le 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.

Déploiement rapide de profils

La fonction Quick Deploy vous permet d'attribuer un profil stocké à un logement de serveur. Tout serveur prenant en charge la réplication de la configuration de serveur inséré dans un logement est configuré à l'aide du profil attribué au logement. Vous pouvez exécuter l'action Quick Deploy uniquement si l'option **Action lorsque le serveur est inséré** dans la page Déployer iDRAC est définie sur **Profil du serveur** ou **Quick Deploy et Profil du serveur**. La sélection de cette option permet d'appliquer le profil de serveur qui est attribué 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.

REMARQUE : Pour configurer les **Profils de déploiement rapide**, vous devez détenir les droits d'Administrateur du châssis.

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 la section **Profils pour QuickDeploy**.
   Les attributions de profil actuelles s'affichent pour des logements dans les cases de sélection contenues dans la colonne **Attibuer 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 **Quick Deploy puis 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.

2. Dans le menu déroulant, sélectionnez le profil à attribuer au logement requis. Sélectionnez les profils à appliquer à plusieurs logements.
3. Cliquez sur **Attribuer un profil**.
   Les profils s'appliquent aux logements sélectionnés.

REMARQUE : Lorsque le traîneau FM120x4 est inséré, le profil stocké attribué au logement du serveur est appliqué à tous les quatre serveurs.

REMARQUE :

- Un logement auquel aucun profil n'est attribué est désigné par le terme « Aucun profil sélectionné » qui apparaît dans la case sélectionnée.
- Pour supprimer un profil attribué depuis un ou plusieurs logements, sélectionnez les logements, puis cliquez sur **Supprimer un profil attribué**. Un message s'affiche pour vous avertir que la suppression d'un profil d'un ou plusieurs logement(s) supprime les paramètres de configuration XML dans le profil de tous les serveurs insérés dans des logements lors de l'activation de la fonction **Profils Quick Deploy**. Cliquez sur **OK** pour supprimer les profils attribués.
- 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 dans un serveur à l'aide de la fonction **Profil de déploiement rapide**, la progression et les résultats de l'application demeurent dans le journal de 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, voir la section *Configuration du partage réseau via 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 en savoir plus, consultez l'*Aide en ligne de CMC pour Dell PowerEdge FX2/FX2s*.

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 contrôleur CMC fournit une gestion limitée des composants individuels du châssis, comme les serveurs. Pour une gestion complète de ces composants individuels, le contrôleur 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 iDRAC sans avoir à rouvrir une session. Les stratégies d'authentification unique sont les suivantes :

- Un utilisateur CMC disposant de privilèges d'administration de serveur est automatiquement connecté à l'iDRAC à l'aide de l'authentification unique (SSO). Une fois sur le site de l'iDRAC, cet utilisateur reçoit automatiquement des privilèges d'administrateur. Cela est vrai même si cet utilisateur n'a pas de compte sur l'iDRAC, ou si le compte ne possède pas les privilèges d'administrateur.
- Un utilisateur CMC qui **ne dispose pas** de privilèges d'administration de serveur, mais qui possède le même compte sur l'iDRAC est automatiquement connecté à l'iDRAC à l'aide de l'authentification unique (SSO). Une fois sur le site de l'iDRAC, cet utilisateur dispose des privilèges qui ont été créés pour le compte iDRAC.
- Un utilisateur CMC qui ne dispose pas de privilèges d'administration de serveur, ou du même compte sur l'iDRAC, n'est pas automatiquement connecté à l'iDRAC à l'aide de l'authentification unique (SSO). Cet utilisateur est dirigé vers la page d'ouverture de session iDRAC lorsqu'il clique sur **Lancer l'interface utilisateur d'iDRAC**.

  REMARQUE : Dans ce contexte, l'expression « même compte » signifie que l'utilisateur possède le même nom de connexion et le même mot de passe pour le contrôleur CMC et pour l'iDRAC. Un utilisateur qui a le même nom de connexion mais pas le même mot de passe est considéré comme ayant 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.

Si vous cliquez sur **Lancer l'interface utilisateur d'iDRAC**, une page d'erreur peut s'afficher, si :

- le serveur est retiré du châssis ;
- l'adresse IP de l'iDRAC a été modifiée ;
- la connexion réseau de l'iDRAC rencontre un problème.

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 l'interface graphique iDRAC**.
   L'interface Web d'iDRAC s'affiche. Pour en savoir plus sur les descriptions des champs, voir l'*Aide en ligne de CMC pour Dell PowerEdge FX2/FX2s*.

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 depuis la page de 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 souhaitez lancer la console distante.
3. Dans la page **État du serveur**, cliquez sur **Lancer la console distante**.

REMARQUE : Le bouton ou lien **Lancer la console distante** est activé uniquement si le serveur est équipé d'une licence Enterprise.

8

Configuration des traîneaux de stockage

Les traîneaux de stockage mi-largeur qui sont utilisés dans le châssis FX2s contiennent les éléments suivants :

- Un ou deux contrôleurs RAID
- Maximum de 16 lecteurs de disque

Vous pouvez configurer des traîneaux de stockage individuels contenant deux contrôleurs RAID pour fonctionner dans les modes suivants :

- Partagé unique
- Partagé double
- Joint

REMARQUE : N'insérez pas un traîneau de stockage dans le logement 1 du châssis car ce n'est pas un emplacement valide pour les traîneaux de stockage.

REMARQUE : Cette section s'applique uniquement aux modules de stockage à deux contrôleurs.

REMARQUE : Vous pouvez également configurer et surveiller les traîneaux de stockage à l'aide de l'IDRAC CEM (Comprehensive Embedded Management). Pour plus d'informations, voir le *Guide d'utilisation d'Integrated Dell Remote Access Controller (iDRAC)*.

Sujets :

Configuration de traîneaux de stockage partagé en mode unique

En mode Split unique, les deux contrôleurs RAID sont adressés à un seul traîneau de calcul. Les deux contrôleurs sont activés et chaque contrôleur est connecté à au moins huit unités.

Configuration de traîneaux de stockage mode partagé double

En mode partagé double, les deux contrôleurs RAID d'un traîneau de stockage sont connectés à deux traîneaux de calcul.

Si un traîneau de stockage se trouve sous un traîneau PowerEdge FC830 pleine largeur, il peut être configuré en mode partagé double. Cependant, les contrôleurs sont connectés à un seul traîneau de calcul et seul ce traîneau de calcul est signalé.

Si un traîneau de stockage est configuré en mode partagé double et se trouve à un endroit où il ne peut pas être connecté à deux traîneaux de calcul, le deuxième contrôleur n'est connecté à aucun traîneau de calcul.

Vous devez disposer du privilège **Administrateur de configuration du châssis** et mettre hors tension le traîneau de calcul avant la modification du réglage.

Configuration en mode groupé les traîneaux de stockage

En mode joint, les contrôleurs RAID sont adressés à un seul traîneau de calcul. Cependant, seul un contrôleur est activé et que tous les lecteurs sont connectés.

Configuration du Partage réseau via l'interface Web CMC

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Présentation du serveur** et cliquez sur un traîneau de stockage. Les informations détaillées concernant le traîneau de stockage s'affichent.
2. Dans le menu situé à droite, cliquez sur **Configuration**.
   La page **Configuration du stockage** s'affiche.

   Vous pouvez également accéder à la page **Configuration du stockage** en sélectionnant un traîneau de stockage sur la page **Intégrité du châssis**. Sous **Liens rapides**, cliquez sur **Configuration de matrice de stockage**.
3. Sous **Composants**, sélectionnez l'une des options suivantes :
   - **Fractionner les deux hôtes**
   - **Fractionner un seul hôte**
   - **Joint**

   REMARQUE : Mettez hors tension le traîneau de calcul avant de configurer le traîneau de stockage. Cliquez sur **Contrôle de l'alimentation du serveur** en haut de la page pour mettre hors tension le traîneau de calcul. Pour plus d'informations, voir l'Aide en ligne.
4. Cliquez sur **Appliquer**.

Configuration de traîneaux de stockage à l'aide de RACADM

Vous pouvez connecter les traîneaux de stockage de traîneaux de calcul à l'aide de la commande `config` ou `getconfig` RACADM en conjonction avec l'option `cfgStorageModule`. Pour plus d'informations, reportez-vous à la section **getstoragemoduleinfo** dans le document *Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* accessible sur le **site dell.com/support/manuals**.

Gestion des traîneaux de stockage à l'aide de proxy RACADM d'iDRAC

La fonctionnalité proxy RACADM d'iDRAC vous permet de gérer les traîneaux de stockage dans le châssis FX2s par le biais de RACADM d'iDRAC lorsque le CMC n'est pas dans le réseau.

Pour accéder à iDRAC localement, utilisez la commande suivante :

```
racadm <command> --proxy
```

Exemple : `racadm getractime --proxy`

Vous pouvez également accéder à l'iDRAC avec RACADM à distance. Pour plus d'informations, consultez la section *Proxy RACADM* du document *Guide de référence de l'interface de la ligne de commande RACADM d'Integrated Dell Remote Access Controller 8 (iDRAC8) version 2.10.10.10*.

REMARQUE : Seuls les proxys RACADM locaux et distants sont pris en charge dans cette version.

Affichage de la condition de la matrice de stockage

Dans le volet de gauche, cliquez sur **Présentation du châssis** > **Présentation du serveur** > **<traîneau de stockage>**. La page **Condition de la matrice de stockage** s'affiche dans le volet de droite. Vous pouvez également accéder à la page **Condition de la matrice de stockage** à partir de la page **Intégrité du châssis**.

1. Sur la page **Intégrité du châssis**, cliquez sur un traîneau de stockage sur l'image du panneau avant.
   Les détails du traîneau de stockage s'affichent dans la partie inférieure du volet de droite.
2. Dans la section **Liens rapides**, cliquez sur **Condition de la matrice de stockage**.

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

9

Configuration de CMC pour envoyer des alertes

Vous pouvez définir des alertes et des actions pour certains événements qui se produisent dans le châssis. Un événement se produit lorsque l'état d'un composant système est supérieur à l'état prédéfini. Si un événement correspond à un filtre d'événement et que ce filtre est configuré pour générer une alerte (par e-mail ou par interruption SNMP), cette alerte est envoyée à une ou plusieurs destinations, telles qu'une adresse e-mail, une adresse IP ou un serveur externe.

Pour configurer 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 avec 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**.

Activation ou désactivation des alertes à l'aide de RACADM

Pour activer ou désactiver la génération d'alertes, utilisez l'objet RACADM `cfgAlertingEnable`. Pour plus d'informations, voir le *Guide de référence de la ligne de commande RACADM de Dell Chassis Management Controller pour PowerEdge FX2/FX2s*.

Filtrage des alertes

Vous pouvez filtrer les alertes en fonction d'une catégorie ou d'un niveau de gravité.

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 trap SNMP

Vous pouvez configurer des adresses IPv6 ou IPv4 pour qu'elles reçoivent les interruptions SNMP.

REMARQUE : Pour plus d'informations sur la configuration du protocole SNMP et du format des interruptions, voir le *Guide de référence de la ligne de commande RACADM de Dell Chassis Management Controller pour PowerEdge FX2/FX2s*.

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 l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **Alertes** > **Paramètres d'interruption**. La page **Destinations des alertes des événements sur châssis** s'affiche.
2. Entrez la commande suivante :
   - 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 FQDN (Fully Qualified Domain Name, Nom de domaine entièrement qualifié). Par exemple : `123.123.123.123`, `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 **Châssis** > **Réseau** > **Services**. La chaîne de communauté des interruptions SNMP est celle que CMC utilise pour les interruptions sortantes destinées aux stations de gestion. La chaîne de communauté de la page **Châssis** > **Réseau** > **Services**est celle que les stations de gestion emploient pour interroger le démon SNMP sur le CMC.

     REMARQUE : Le CMC utilise une chaîne de communauté SNMP en mode public par défaut. Pour garantir un niveau de sécurité plus élevé, il est recommandé de modifier la chaîne de communauté par défaut et de définir une valeur qui n'est pas vide.
   - 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 filtrage pour chaque fonction (SNMP et e-mails d'alerte). Vous pouvez passer l'étape 2 si vous avez déjà défini un masque de filtrage.
2. Activez la génération d'alertes :

```
racadm config -g cfgAlerting -o cfgAlertingEnable 1
```

3. Activez les alertes par interruption :

```
racadm config -g cfgTraps -o cfgTrapsEnable 1 -i <index>
```

Où <index> est une valeur comprise entre 1 et 4. CMC utilise le numéro d'index pour distinguer un maximum de quatre adresses e-mail de destination configurables. Vous pouvez spécifier les destinations sous forme d'adresses numériques au format approprié (IPv6 ou IPv4) ou sous forme de noms FQDN (Fully-Qualified Domain Name - Nom de domaine entièrement qualifié).

4. Spécifiez une adresse IP de destination pour la réception des alertes par interruption :

```
racadm config -g cfgTraps -o cfgTrapsAlertDestIPAddr <IP address> -i <index>
```

où <IP address> est une destination valide et <index> est la valeur d'index spécifiée à l'étape 3.

5. Spécifiez le nom de communauté :

```
racadm config -g cfgTraps -o cfgTrapsCommunityName <community name> -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.

REMARQUE : Le CMC utilise une chaîne de communauté SNMP en mode public par défaut. Pour garantir un niveau de sécurité plus élevé, il est recommandé de modifier la chaîne de communauté par défaut et de définir une valeur qui n'est pas vide.

Vous pouvez configurer jusqu'à quatre destinations pour les alertes par interruption. Pour ajouter des destinations, répétez les étapes 2 à 6.

REMARQUE : Les commandes des étapes 2 à 6 écrasent les paramètres existants configurés pour l'index spécifié (1 à 4). Pour déterminer si un index possède des valeurs déjà configurées, tapez : `racadm getconfig -g cfgTraps -i <index>`. Si l'index est déjà configuré, des valeurs apparaissent pour les objets `cfgTrapsAlertDestIPAddr` et `cfgTrapsCommunityName`.

6. 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'alertes à tester.

Si vous n'êtes pas sûr du numéro d'index, utilisez la commande suivante :

```
racadm getconfig -g cfgTraps -i <index>
```

Configuration des paramètres d'alerte par e-mail

Lorsque CMC détecte un événement sur le 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.

Vous devez configurer le serveur e-mail SMTP pour qu'il accepte les e-mails relayés depuis l'adresse IP CMC. Cette fonction est normalement désactivée sur la plupart des serveurs d'e-mail pour des raisons de sécurité. Pour obtenir des instructions afin de réaliser l'opération 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 de CMC soit configuré pour que le serveur de messagerie puisse recevoir les alertes par e-mail du CMC.

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.

Configuration des paramètres d'alerte par e-mail à l'aide de l'interface Web CMC

Pour définir les paramètres d'alerte par e-mail en utilisant l'interface Web :

1. Dans l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **Alertes** > **Paramètres d'alertes par e-mail**.
2. Spécifiez les paramètres de serveur d'e-mail SMTP et les adresses e-mail devant recevoir les alertes. Pour plus d'informations sur les champs, voir l'*Aide en ligne CMC*.
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.

Configuration des paramètres d'alerte par e-mail à l'aide de RACADM

Pour envoyer un e-mail de test à une destination d'alerte par e-mail à l'aide de RACADM :

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
   ```

3. 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. CMC utilise le numéro d'index pour distinguer un maximum de quatre adresses e-mail de destination configurables.
4. 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.
5. 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 recevant l'alerte par e-mail, et `<index>` la valeur d'index spécifiée aux étapes 4 et 5. Le nom de l'e-mail peut contenir jusqu'à 32 caractères alphanumériques, tirets, traits de soulignement et points. Les espaces ne sont pas valides.
6. Configurez l'hôte SMTP :

   ```
   racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr host.domain
   ```

   où `host.domain` est le nom de domaine complet.

   Vous pouvez configurer jusqu'à quatre adresses e-mail de destination pour réceptionner des alertes par e-mail. Pour ajouter d'autres adresses e-mail, répétez les étapes 2 à 5.

   REMARQUE : Les commandes indiquées dans les étapes 2 à 5 remplacent tous les paramètres existants configurés pour l'index que vous avez spécifié (1 à 4). Pour déterminer si un index possède déjà des valeurs configurées, saisissez : `racadm getconfig -g cfgEmailAlert — I <index>`. Si l'index est configuré, des valeurs s'affichent pour les objets `cfgEmailAlertAddress` et `cfgEmailAlertEmailName`.

   Pour en savoir plus, voir le *Guide de référence de la ligne de commande RACADM d'iDRAC et de CMC* disponible à l'adresse **dell.com/support/manuals**.

10

Configuration des comptes et des privilèges des utilisateurs

Vous pouvez configurer des comptes d'utilisateur avec des privilèges spécifiques (droit basé sur un rôle) pour gérer votre système avec CMC et maintenir la sécurité du système. Par défaut, CMC est configuré avec un compte root par défaut. En tant qu'administrateur, vous pouvez configurer des comptes utilisateur pour autoriser d'autres utilisateurs à accéder au 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 de droits 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 CMC Active Directory et les utilisateurs iDRAC Active Directory résident dans deux branches distinctes de l'arborescence Active Directory. Pour créer un utilisateur de serveur local, l'Administrateur de configuration des utilisateurs doit se connecter directement au serveur. L'Administrateur de configuration des utilisateurs ne peut pas utiliser le contrôleur CMC pour créer un utilisateur de serveur et inversement. Cette règle protège la sécurité et l'intégrité des serveurs.

Tableau 17. 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 pour autant disposer d'un droit d'ouverture de session utilisateur CMC. Cette fonction est utile lorsqu'un utilisateur n'est plus autorisé à se connecter de manière temporaire. Lorsque le droit d'ouverture de session utilisateur CMC est rétabli, l'utilisateur conserve l'ensemble des 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. ● Sont associées au châssis, telles que le nom de logement et la priorité du logement. Bien qu'elles s'appliquent aux serveurs, il s'agit de propriétés exclusives du châssis qui concernent les logements

Tableau 17. Types d'utilisateurs (suite)

Droits	Description
	plutôt que les serveurs eux-mêmes. C'est pourquoi il est possible d'ajouter et de modifier les noms et priorités d'un logement, que celui-ci comporte un serveur ou non. 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 de logement précédents restent associés au châssis précédent. **REMARQUE :** Les utilisateurs CMC dotés de droits d'**Administrateur de configuration du châssis** peuvent configurer les paramètres d'alimentation. Cependant, il est nécessaire de disposer de droits d'**Administrateur de contrôle du châssis** pour effectuer les opérations d'alimentation du châssis, notamment 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 de droits d'**Administrateur d'alimentation du châssis** peuvent effectuer l'ensemble des opérations d'alimentation. Ils peuvent contrôler les opérations d'alimentation du châssis, notamment 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 doté de droits d'**Administrateur de serveur** émet une action à exécuter sur un serveur, le micrologiciel CMC envoie la commande au serveur cible sans vérifier les privilèges de l'utilisateur sur le serveur. Autrement dit, les droits d'**Administrateur de serveur** permettent de passer outre à 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 de droits d'**Administrateur de serveur** émet une action à exécuter sur un serveur, le contrôleur CMC envoie une commande au serveur cible 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 que le mot de passe correspond, le serveur renvoie les privilèges accordés à l'utilisateur sur le serveur. Selon les privilèges renvoyés par le serveur, le micrologiciel CMC détermine si l'utilisateur a le droit d'effectuer l'action.
	Nous avons répertorié ci-dessous les privilèges et les actions de serveur auxquels un Administrateur de serveur est autorisé. 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 ● 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

Tableau 17. Types d'utilisateurs (suite)

Droits	Description
	• 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.

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 18. 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 : • 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 19. 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 racine

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).

Configuration d'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.

Configurer des 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 CMC ou que vous avez utilisé la commande racadm `racresetcfg`, le seul compte d'utilisateur actuel est le compte par défaut root. La sous-commande `racresetcfg` rétablit 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.

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 20. : 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
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 de 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. À l'aide de 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.

Présentation d'Active Directory avec schéma étendu

Pour utiliser la solution de schéma étendu, vous devez disposer de l'extension de schéma Active Directory.

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.

Configuration d'utilisateurs LDAP générique

Le contrôleur CMC fournit une solution générique de prise en charge de l'authentification basée sur le protocole LDAP (Lightweight Directory Access Protocol). Cette fonctionnalité ne nécessite aucune extension de schéma sur vos services d'annuaire.

Un administrateur CMC peut désormais intégrer les connexions utilisateur au serveur LDAP avec le contrôleur CMC. Cette intégration requiert une configuration sur le serveur LDAP et le CMC. Sur le serveur LDAP, un objet de groupe standard est utilisé en tant que groupe de rôles. Un utilisateur disposant d'un accès CMC devient membre du groupe de rôles. Les privilèges sont toujours stockés sur le CMC pour obtenir une autorisation similaire au fonctionnement de la configuration du schéma standard avec une prise en charge d'Active Directory.

Pour permettre à l'utilisateur LDAP d'accéder à une carte CMC spécifique, le nom du groupe de rôles et son nom de domaine doivent être configurés sur la carte CMC en question. Vous pouvez configurer un maximum de cinq groupes de rôles dans chaque CMC. Un utilisateur peut être ajouté à plusieurs groupes au sein du service d'annuaire. Si un utilisateur est membre de plusieurs groupes, il obtient alors les privilèges de tous ces groupes.

Configuration de l'annuaire LDAP générique pour accéder au CMC

L'implémentation LDAP générique du contrôleur CMC utilise deux phases pour autoriser l'accès d'un utilisateur : authentification et autorisation.

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**.
   Sélectionnez LDAP générique. Les paramètres à configurer pour le schéma standard sont affichés dans la même page.
   REMARQUE : Les serveurs d'annuaire Windows n'autorisent pas la connexion anonyme. Par conséquent, saisissez les nom et mot de passe du nom unique de liaison.
3. Indiquez les informations 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 :

  ```
  _[Service Name]._tcp.[Search Domain]
  ```

  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 pour 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 les protocoles 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 éventuellement être configuré pour interroger un serveur DNS à la recherche d'enregistrements SRV. Si la propriété `cfgLDAPSRVLookupEnable` est activée, la propriété `cfgLDAPServer` est ignorée. La requête suivante permet de rechercher des enregistrements SRV dans le serveur DNS :

```
_ldap._tcp.domainname.com
```

`ldap` figurant dans la requête ci-dessus représente la propriété `cfgLDAPSRVLookupServiceName`.

`cfgLDAPSRVLookupDomainName` est configuré comme **domainname.com**.

Pour en savoir plus sur les commandes RACADM, voir le *Guide de référence de la ligne de commande RACADM de Dell Chassis Management Controller pour PowerEdge FX2/FX2s* disponible à l'adresse **dell.com/support/manuals**.
```

11

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 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 CMC).

Génération d'un fichier Keytab Kerberos

Pour prendre en charge l'authentification unique (SSO) et l'authentification de connexion par carte à puce, le contrôleur CMC prend en charge le réseau Windows Kerberos. L'outil **ktpass** permet de créer des liaisons SPN (Service Principal Name) avec un compte utilisateur et d'exporter les informations d'approbation dans un fichier keytab Kerberos de type MIT. Pour en savoir plus 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 :

```
C:\>ktpass -princ HTTP/cmcname.domain_name.com@REALM_NAME.COM - mapuser dracname -mapOp
set -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 types 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 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.

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 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`

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 en savoir plus sur les options, voir l'*Aide en ligne de CMC pour Dell PowerEdge FX2/FX2s*.

1. Au cours de la configuration d'Active Directory pour définir un compte d'utilisateur, réalisez les étapes supplémentaires suivantes :
   - 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 d'utilisateur Active Directory valide.

   Une commande réussie indique que le contrôleur CMC est en mesure d'acquérir les informations d'identification Kerberos et d'accéder au compte Active Directory de l'utilisateur. Si la commande échoue, corrigez l'erreur et réexécutez la commande. Pour plus d'informations, voir le *Guide de référence de la ligne de commande RACADM de Dell Chassis Management Controller pour PowerEdge FX2/FX2s* disponible à l'adresse 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 l'opération a réussi ou non.

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`

12

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 afin de pouvoir réaliser des opérations de gestion de système via la console. Pour obtenir des informations sur l'utilisation des commandes RACADM dans le contrôleur CMC avec la console de ligne de commande, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge FX2/FX2s*.

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 21. 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, voir le *Guide de référence de la ligne de commande RACADM de Dell Chassis Management Controller pour PowerEdge FX2/FX2s*.
`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 terminent la session en cours et redirigent l'utilisateur vers 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 2003, vous pouvez rencontrer un problème de caractères au cours d'une session Telnet CMC. Cela peut provoquer le blocage de la connexion, parce que la touche Entrée ne répond pas et que le message de saisie du mot de passe n'apparaît pas.

Pour résoudre la problème, téléchargez le hotfix 824810 depuis le site **support.microsoft.com**. Pour plus d'informations, vous pouvez également consulter l'article 824810 dans la base de connaissances de Microsoft.

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 de `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`. Pour en savoir plus sur les commandes RACADM, voir le *Guide de référence de la ligne de commande RACADM de Dell Chassis Management Controller pour PowerEdge FX2/FX2s* disponible à l'adresse 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 de scripts SSH en évitant d'intégrer ou de demander l'ID utilisateur/le mot de passe.

SSH est activé par défaut. Si SSH est désactivé, vous pouvez l'activer avec n'importe quelle autre interface prise en charge.

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 22. 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 • 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 6 clés publiques pouvant être utilisées avec le nom d'utilisateur du service sur l'interface SSH. Avant d'ajouter ou de supprimer des clés publiques, veillez à utiliser la commande `view` pour identifier les clés déjà définies afin qu'aucune clé ne soit accidentellement remplacée ou supprimée. Le nom d'utilisateur du service correspond à un compte utilisateur spécial qui peut être utilisé pour l'accès au contrôleur CMC via SSH. Si vous configurez et utilisez correctement l'authentification PKA sur SSH, vous n'avez pas besoin d'entrer de nom d'utilisateur ni de mot de passe pour la connexion au contrôleur CMC. Cela est particulièrement utile pour définir des scripts automatisés afin de réaliser différentes fonctions.

REMARQUE : L'interface utilisateur n'est pas prise en charge pour la gestion de cette fonction ; vous ne pouvez utiliser que RACADM.

Lorsque vous ajoutez de nouvelles clés publiques, vérifiez que les clés existantes ne se situent pas à l'index où vous allez ajouter la nouvelle clé. Le contrôleur CMC ne vérifie jamais si les clés précédentes sont supprimées lors de l'ajout d'une nouvelle clé. Dès que vous ajoutez une nouvelle clé, elle est automatiquement activée, à condition que l'interface SSH soit activée.

Lorsque vous utilisez la section de commentaire de la clé publique, notez que le contrôleur CMC utilise uniquement les 16 premiers caractères. Le commentaire de clé publique permet au contrôleur CMC de distinguer les utilisateurs SSH lors de l'utilisation de la commande RACADM `getssninfo`, car tous les utilisateurs de PKA emploient le nom d'utilisateur de 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`, voir le *Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge FX2/FX2s*.

Configuration du logiciel d'émulation de terminal

Le CMC prend en charge une console texte série qui peut être lancée à l'aide de tout logiciel d'émulation de terminal. Voici des exemples de logiciels d'émulation de terminal pouvant être utilisés pour se connecter au CMC.

1. Linux Minicom
2. HyperTerminal Hilgraveve pour Windows

Connectez une extrémité du câble série null-modem (présent aux deux extrémités) sur le connecteur série situé à l'arrière du châssis. Connectez l'autre extrémité du câble dans le port série de la station de gestion. Pour plus d'informations sur la connexion des câbles, reportez-vous au panneau arrière du châssis dans la section Présentation du châssis.

Configurez votre logiciel d'émulation de terminal avec les paramètres suivants :

- **Débit en bauds** : 115 200
- **Port** : COM1
- **Données** : 8 bits
- **Parité**: Aucune
- **Arrêt** : 1 bit
- **Contrôle de flux matériel** : Oui
- **Contrôle de flux logiciel** : Non

Connexion aux serveurs ou au module d'E/S 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) 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 FX2/FX2s*.
- 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, ainsi que la console série du système d'exploitation. Pour le module d'E/S, la console série du commutateur est disponible. Il existe un seul module d'E/S sur le châssis.

PRÉCAUTION : Lors de l'exécution à partir de la console série du contrôleur CMC, l'option `connect -b` reste connectée jusqu'à la réinitialisation du contrôleur 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 la commande `cfgSerialConsoleQuitKey` n'est pas utilisée. En outre, lors d'une connexion à un serveur à l'aide de la console série du contrôleur CMC, les transitions du signal DTR (par exemple, si le câble série est retiré pour connecter un débogueur) ne se produisent pas si vous quittez 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 la suivante : <Ctrl><\>.

Pour vous connecter à un module d'E/S, tapez :

```
connect switch-n
```

où `n` représente une étiquette de module d'E/S A1.

Lorsque vous référencez l'IOM dans la commande connect, l'IOM est associé à un commutateur, comme indiqué dans le tableau suivant.

Tableau 23. Association de module d'E/S à des commutateurs

Étiquette de module d'E/S	Commutateur
A1	commutateur-a1 ou commutateur-1
A2	commutateur-a2 ou commutateur-2

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 gérée par un serveur, exécutez la commande `connect server-n` , où *n* = 1-4 (PowerEdge FM120x4) et *n* = 1-8 (PowerEdge FC630). 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 la fenêtre de l'émulateur de terminal sur la valeur 80×25. Sinon, les caractères de la page ne s'affichent pas correctement.

REMARQUE : Toutes les touches ne fonctionnent pas sur les pages de configuration du BIOS. Par conséquent, indiquez des raccourcis clavier appropriés pour <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 iDRAC7 (voir le *Guide de l'utilisateur du Dell Integrated Dell Remote Access Controller (iDRAC)* à l'adresse **dell.com/support/manuals)**.

Par défaut, la communication série est désactivée dans le BIOS. Pour rediriger les données de console texte de l'hôte vers les communications série sur LAN, vous devez activer la redirection de console via COM1. Pour modifier la configuration du 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 **Communications série**, puis appuyez sur <Entrée>. Dans la boîte de dialogue, la liste des communications série affiche les options suivantes :
   - **Eteint**
   - **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 la 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 :

```
kernel 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 # # Note that you do not have to rerun grub after making
changes # to this file # NOTICE: You do not have a /boot partition. This means that #
all kernel and initrd paths are relative to /, e.g. # root (hd0,0) # kernel /boot/vmlinuz-
version ro root= /dev/sdal # initrd /boot/initrd-version.img # #boot=/dev/sda default=0
timeout=10 #splashimage=(hd0,2)/grub/splash.xpm.gzserial --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 la 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 This file describes how the INIT process
# should set up the system in a certain
# run-level.
#
# Author: Miquel van Smoorenburg
# Modified for RHS Linux by Marc Ewing and
# Donnie Barnes
#
# Default runlevel. The runlevels used by RHS are:
# 0 - halt (Do NOT set initdefault to this)
# 1 - Single user mode
# 2 - Multiuser, without NFS (The same as 3, if you
# do not have networking)
# 3 - Full multiuser mode
# 4 - unused
# 5 - X11
# 6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:
# System initialization.
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
# Things to run in every runlevel.
ud::once:/sbin/update
# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
# When our UPS tells us power has failed, assume we
have a few
# minutes of power left. Schedule a shutdown for 2
minutes from now.
# This does, of course, assume you have power
installed and your
```

```
# UPS is connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure;
System Shutting Down"
# If power was restored before the shutdown kicked in,
cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power
Restored; Shutdown Cancelled"
# Run gettys in standard runlevels
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

# Run xdm in runlevel 5
# xdm is now a separate service
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
```

Gestion de CMC à l'aide de proxy RACADM d'iDRAC

Le contrôleur CMC peut être géré à l'aide du proxy RACADM iDRAC lorsque le contrôleur CMC n'est pas sur le réseau. Le tableau suivant reprend l'adressage des privilèges CMC avec les privilèges iDRAC pour l'opération du proxy.

Tableau 24. CMC-mappage des privilèges iDRAC

Privilèges CMC	Privilège iDRAC requis pour l'opération de proxy
Ouverture de session utilisateur CMC	Connexion iDRAC
Administrateur de configuration du châssis	Configurer iDRAC
Administrateur de configuration des utilisateurs	Configurer les utilisateurs dans l'iDRAC
Administrateur des effacements de journaux	Journaux

Tableau 24. CMC-mappage des privilèges iDRAC (suite)

Privilèges CMC	Privilège iDRAC requis pour l'opération de proxy
Administrateur et contrôle du châssis	Contrôle du système
Server Administrator	Contrôle du système
Utilisateur d'alertes de test	Opérations système
Administrateur de commandes de débogage	Débogage
Fabric x Administrator (où x correspond à A, B ou C)	Contrôle du système

Pour plus d'informations, voir le document *Dell Chassis Management Controller Version 2.0 for PowerEdge FX2/FX2s RACADM Command Line Reference Guid* (*Guide de référence de la ligne de commande RACADM du contrôleur Dell Chassis Management Controller version 1.4 pour Dell PowerEdge FX2/FX2*).

13

Utilisation de cartes FlexAddress et FlexAdress Plus

Cette section fournit des informations sur FlexAddress et sur comment utiliser la carte FlexAddress Plus pour configurer FlexAddress.

REMARQUE : La fonction FlexAddress est disponible sous licence. Cette fonction est incluse dans la licence Enterprise.

Sujets :

À propos de FlexAddress

La fonction FlexAddress permet au CMC d'attribuer des ID WWN/MAC à un logement spécifique et de remplacer les ID définis en usine. Ainsi, si le module de serveur est remplacé, les ID WWN/MAC du logement restent identiques. Avec cette fonction, vous n'avez plus à reconfigurer les outils Ethernet de gestion de réseau, les ressources SAN, les serveurs DHCP et les routeurs de diverses structures pour un nouveau module de serveur.

Au cours du processus de fabrication, chaque module de serveur reçoit un nom WWN (World Wide Name, Nom universel) et/ou des ID MAC (Media Access Control, Contrôle de l'accès aux supports) uniques. Sans FlexAddress, si vous avez besoin de remplacer un module de serveur par un autre, l'ID WWN/MAC change et vous devez reconfigurer les outils Ethernet de gestion réseau et les ressources SAN afin d'identifier le nouveau module 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 retourne à l'adresse attribuée par le serveur.

En outre, ce *remplacement* se produit uniquement lorsque vous insérez un module de serveur dans un châssis où la fonction FlexAddress est activée. Aucune modification permanente n'est apportée au module de serveur. Si un module de serveur est déplacé vers un châssis qui ne prend pas en charge la fonction FlexAddress, les ID WWN/MAC utilisés sont ceux attribués en usine.

Le châssis du CMC FX2/FX2s est livré avec la carte SD FlexAddress Plus, qui prend en charge les fonctions FlexAddress, FlexAddress Plus et Stockage étendu.

REMARQUE : Les données contenues dans la carte SD FlexAddress Plus sont cryptées et vous ne devez pas les copier ni les altérer de quelque manière que ce soit, car cela pourrait inhiber la fonction système et entraîner un dysfonctionnement du système.

REMARQUE : L'utilisation d'une carte SD FlexAddress Plus est limitée à un seul châssis. Vous ne pouvez pas utiliser la même carte SD FlexAddress Plus sur un autre châssis.

À propos de FlexAddress Plus

Chaque carte de fonction FlexAddress Plus contient un pool unique d'adresses MAC/WWN qui permettent au châssis d'attribuer des adresses World Wide Name/Media Access Control (WWN/MAC) aux périphériques Fibre Channel et Ethernet. Les adresses WWN/MAC attribuées par le châssis sont globalement uniques et spécifiques à un logement de serveur.

Avant d'installer FlexAddress, vous pouvez déterminer la plage des adresses MAC contenues dans une carte avec fonction FlexAddress en insérant la carte SD dans un lecteur de carte 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 est la première adresse hexadécimale de début qui sera utilisée pour cette plage spécifique d'adresses MAC. La balise `mac_count` correspond au nombre total d'adresses MAC que la carte SD attribue. La plage totale d'adresses MAC attribuées peut être déterminée comme suit :

```
<mac_start> + <mac_count> - 1 = <mac_end>
```

Par exemple :

```
(starting_mac)00:18:8B:FF:DC:FA + (mac_count)0xCF – 1 = (ending_mac)00:18:8B:FF:DD:C8
```

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 CMC.

Vérification de l'activation de FlexAddress

Pour afficher l'état d'activation de la fonction FlexAddress, exécutez la commande RACADM suivante :

```
racadm featurecard -s
```

```
        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 un message : racadm feature -s No features active on the chassis

```
racadm feature -s
No features active on the chassis
```

Pour afficher les informations de la carte SD :

```
$ racadm featurecard -s
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
```

Tableau 25. 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.
`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.

Tableau 25. Messages d'état renvoyés par la commande featurecard -s (suite)

Message de condition	Actions
`The feature card inserted is valid and contains the following feature(s) FlexAddress: not bound.`	La carte de fonctions peut être déplacée vers un autre châssis ou réactivée sur le châssis actuel. Pour la réactiver sur le châssis actuel, saisissez `racadm racreset` jusqu'à ce que le module CMC sur lequel la carte de fonctions est installée devienne actif.

Les cartes de fonctions Dell (Dell Feature Card) peuvent contenir plusieurs fonctions. Dès que l'une des fonctions incluses sur une carte de fonctions Dell a été activée sur un châssis, toutes les autres fonctions incluses sur cette carte de fonctions 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 en savoir plus sur les commandes `feature` et `featurecard`, voir le *Guide de référence de la ligne de commande RACADM de Dell Chassis Management Controller pour PowerEdge FX2/FX2s*.

Désactivation de FlexAddress

La fonctionnalité FlexAddress peut être désactivée et la carte SD restaurée à un état de pré-installation à l'aide d'une commande RACADM. Aucune fonction de désactivation n'est disponible dans l'interface Web. La désactivation restaure la carte SD à son état d'origine. Elle peut alors être installée et activée dans un autre châssis. Dans ce contexte, le terme FlexAddress concerne à la fois FlexAddress et FlexAddressPlus.

REMARQUE : La carte SD doit être installée physiquement sur le contrôleur CMC et le châssis doit être mis hors tension avant l'exécution de la commande de désactivation.

Si vous exécutez la commande de désactivation sans installer de carte SD ou avec une carte d'un autre châssis, la fonction est désactivée et aucune modification n'est apportée à la carte.

Pour désactiver la fonction FlexAddress et restaurer la carte SD :

```
racadm feature -d -c flexaddress
```

La commande renvoie le message d'état suivant si sa désactivation réussit :

```
feature FlexAddress is deactivated on the chassis successfully.
```

Si le châssis n'est pas hors tension avant l'exécution de la commande, cette commande génère l'erreur suivante :

```
ERROR: Unable to deactivate the feature because the chassis is powered ON
```

REMARQUE : Pour activer à nouveau la fonction FlexAddress, redémarrez le CMC.

Pour en savoir plus sur la commande, voir la section de la commande **feature** dans le *Guide de référence de la ligne de commande RACADM de Dell Chassis Management Controller pour PowerEdge FX2/FX2s*.

Configuration de FlexAddress

FlexAddress est une mise à niveau facultative qui permet aux modules de serveur de remplacer l'ID WWN/MAC d'usine par un ID WWN/MAC fourni par le châssis.

REMARQUE : Vous pouvez réinitialiser l'adresse Flex d'un 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 Dell Chassis Management Controller pour PowerEdge FX2/FX2s* disponible à l'adresse **dell.com/cmcmanuals**.

Le serveur doit être mis hors tension avant de commencer la configuration. Vous pouvez activer ou désactiver FlexAddress en fonction de chacune des structures. Vous pouvez également activer ou désactiver la fonctionnalité pour chaque logement. Une fois la fonctionnalité activée pour chaque structure individuelle, vous pouvez sélectionner les logements à activer. Par exemple, si la structure A est activée, tous les logements activés ont la fonctionnalité FlexAddress activée uniquement sur la structure A. Toutes les autres structures utilisent l'adresse WWN/MAC attribuée en usine sur le serveur.

REMARQUE : Lors du premier déploiement de la fonctionnalité FlexAddress sur un module de serveur spécifique, celle-ci nécessite une séquence de mise hors et sous tension pour être effective. L'adresse FlexAddress est programmée sur les périphériques Ethernet par le BIOS du module de serveur. Pour que le BIOS du module de serveur puisse programmer l'adresse, celui-ci doit être opérationnel, ce qui nécessite que le module de serveur soit mis sous tension. Une fois les séquences de mise hors et sous tension terminées, les ID de MAC attribués par le châssis sont disponibles pour la fonction WOL (Wake-on-LAN).

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.

Affichage des ID WWN (World Wide Name) ou MAC (Media Access Control)

La page **WWN/MAC Summary (Résumé WWN/MAC)** permet d'afficher la configuration World Wide Name (WWN) et l'adresse Media Access Control (MAC) d'un logement présent dans le châssis.

Messages des commandes

Le tableau suivant répertorie les commandes RACADM et leurs sorties pour des problèmes FlexAddress courants.

Tableau 26. Commandes et sortie FlexAddress

Problème	Commande	Sortie
La carte SD du module du contrôleur CMC est liée à un autre numéro de service.	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)` `FlexAddress: bound to another chassis, svctag = <Service tag Number> SD card SN = <Valid flex address serial number>`
La carte SD du module du contrôleur CMC est liée au même numéro de service.	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)` `FlexAddress: bound`
La carte SD du module du contrôleur CMC n'est liée à aucun numéro de service.	`$racadm featurecard -s`	`The feature card inserted is valid and contains the following feature(s)` `FlexAddress:not bound`
La fonctionnalité FlexAddress n'est pas active sur le châssis pour une raison inconnue (Aucune carte SD insérée/ carte SD corrompue/ fonctionnalité désactivée/carte SD liée à un autre châssis)	`$racadm setflexaddr [-f <fabricName> <slotState>]` `$racadm setflexaddr [-i <slot#> <slotstate>]`	`ERROR: Flexaddress feature is not active on the chassis`

Tableau 26. Commandes et sortie FlexAddress (suite)

Problème	Commande	Sortie
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`
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 240 à l'aide des cartes FlexAddress et FlexAddress Plus ni le céder en crédit-bail, ni copier les documents papier qui l'accompagnent, 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 à 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.

Affichage des informations d'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 est considéré comme faisant partie de la Structure de gestion et est indiqué avec le reste des structures.
  - Une coche indique que la structure est activée pour FlexAddress ou FlexAddressPlus.
- Protocole utilisé sur le port de la carte réseau. Par exemple, LAN, iSCSI, FCoE, etc.
- Configuration Fibre Channel World Wide Name (WWN) et adresses MAC (Media Access Control d'un logement dans le châssis.
- Type d'attribution d'adresse Mac et type actuel d'adresse active, attribuée par le serveur, FlexAddress ou MAC d'identité d'E/S. Une coche verte indique le type de l'adresse active, attribuée par le serveur, par le châssis ou 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 RACADM. Selon l'interface, vous pouvez filtrer l'adresse MAC et savoir quelle adresse WWN/MAC est utilisée pour cette fonction ou partition. Si l'option NPAR est activée pour l'adaptateur, vous pouvez afficher les partitions activées ou désactivées.

L'interface Web vous permet d'afficher les informations relatives aux adresses WWN/MAC pour des logements spécifiques à l'aide de la page **FlexAddress** (cliquez sur **Présentation du serveur** > **Logement <x>** > **Configuration** > **FlexAddress**). Vous pouvez afficher les informations sur les adresses WWN/MAC pour tous les logements et le serveur à l'aide de la page **Résumé de WWN/MAC** (cliquez sur **Présentation du serveur** > **Propriétés** > **WWN/MAC**). Dans les deux pages, vous pouvez afficher les informations sur les 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 le champ 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 de base et tous les types de MAC (attribués par le serveur, Flex Address et identité IO). Vous pouvez les filtrer à l'aide de certains des champs affichés ou de tous les champs.

Dans les modes de base et avancé, les informations sur les adresses WWN/MAC s'affichent sous un format réduit. Cliquez sur  en regard d'un logement ou cliquez sur le bouton **Développer/Réduire tout** pour afficher les informations sur un logement spécifique ou tous les logements.

Vous pouvez également exporter les informations des adresses WWN/MAC pour tous les serveurs du châssis dans un dossier local.

Pour en savoir plus sur les champs, voir l'*Aide en ligne de CMC pour Dell PowerEdge FX2/FX2s*.

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 spécifique. 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 en regard d'un logement ou cliquez sur le bouton **Développer/Réduire tout** pour développer ou réduire les attributs répertoriés pour un logement spécifique ou tous les logements dans le tableau 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 MAC ou celles associées au protocole sélectionné.
8. Dans le champ **Adresses WWN/MAC**, pour filtrer un logement associé à une adresse MAC spécifique, saisissez l'adresse MAC exacte. Vous pouvez également saisir partiellement les entrées d'adresse MAC pour afficher les logements associés. Par exemple, saisissez `4A` pour afficher les logements avec des adresses MAC contenant `4A`.
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 désactivée, la ligne contenant la partition est grisée.

Pour en savoir plus sur les champs, voir l'*Aide en ligne de CMC pour Dell PowerEdge FX2/FX2s*.

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 le logement du serveur, la structure, le protocole, les adresses WWN/MAC, le type d'attribution de l'adresse MAC, attribuée par le serveur, FlexAddress ou MAC d'identité d'E/S, ainsi que l'état de la partition. Une coche verte indique le type de l'adresse active, attribuée par le serveur, par le châssis ou à distance. MAC. Si l'option FlexAddress ou Identité d'E/S n'est pas activée sur un serveur, **FlexAddress (attribué par le châssis)** ou **Identité d'E/S (attribuée à distance)** affiche l'état **Non activé**.
3. Dans le tableau **Adresses WWN/MAC**, cliquez sur **Exporter** pour enregistrer les adresses WWN/MAC au niveau local.
4. Cliquez sur en regard d'un logement ou cliquez sur le bouton **Développer/Réduire tout** pour développer ou réduire les attributs répertoriés pour un logement spécifique ou tous les logements dans le tableau 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. Vous pouvez également saisir partiellement les entrées d'adresse MAC pour afficher les logements associés. Par exemple, saisissez `4A` pour afficher les logements avec des adresses MAC contenant `4A`.
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 en savoir plus sur les champs, voir l'*Aide en ligne de CMC pour Dell PowerEdge FX2/FX2s*.

Affichage des informations d'adresse WWN ou MAC à l'aide de 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 les adresses MAC Ethernet et iSCSI de tous les LOM ou cartes mezzanine, utilisez la commande RACADM suivante :

```
racadm getmacaddress -a
```

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 en savoir plus sur les sous-commandes `getflexaddr` et `getmacaddress`, voir le *Guide de référence de la ligne de commande RACADM de Dell Chassis Management Controller pour PowerEdge FX2/FX2s*.

14

Gestion des structures

Le châssis prend en charge deux types de structure : Structure A1 et Structure A2, lesquelles sont utilisées par les deux modules d'E/S (IOM) et sont toujours connectées aux adaptateurs Ethernet intégrés des serveurs.

REMARQUE : Dans le châssis PowerEdge FX2s, les structures B et C sont la connexion PCIe pour les cartes d'extension PCIe.

Les modules d'E/S suivants sont pris en charge :

- 1 GbE d'intercommunication
- 10 GbE d'intercommunication
- Agrégateur d'E/S

Les deux structures prennent en charge Ethernet uniquement. Chaque adaptateur d'E/S de serveur (LOM) peut disposer de 2 ou 4 ports, selon la capacité. Les logements de carte mezzanine PCIe sont occupés par des cartes d'extension PCIe connectées aux cartes PCIe (et non aux modules d'E/S).

REMARQUE : Dans l'interface CLI CMC, l'IOM s'appelle par convention, un commutateur.

Sujets :

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.

Configuration des paramètres réseau d'un 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.

Configuration 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**, puis **Configuration**. En variante, si vous souhaitez configurer les paramètres de réseau des modèles d'E/S disponibles, c'est-à-dire **A1** et **A2**, cliquez sur **Gigabit Ethernet A1** or **Gigabit Ethernet A2**, puis sur **Configuration**.
   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 configurer les paramètres réseau d'un module IOM à l'aide de RACADM, définissez la date et l'heure. Consultez la section relative à la commande deploy dans le document *Guide de référence de la ligne de commande RACADM de Dell Chassis Management Controller pour PowerEdge FX2/FX2s*.

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 <username> -p <password>
```

```
racadm deploy -m switch -u -p <password> -v SNMPv2 <snmpCommunityString> ro
```

```
racadm deploy -a [server|switch] -u <username> -p <password>
```

Affichage de la condition des liaisons montantes et descendantes des modules d'entrée/sortie via l'interface web

REMARQUE : Cette fonction est disponible uniquement sur les serveurs PowerEdge FX2/FX2s.

Vous pouvez afficher les informations relatives à la condition des liaisons montantes et descendantes de l'agrégateur d'E/S Dell PowerEdge M à l'aide de l'interface Web CMC. Pour ce faire :

1. Accédez à **Présentation du châssis** > **Présentation du module d'E/S**.
   Tous les modules d'E/S (1–2) apparaissent dans la liste développée.
2. Cliquez sur le module d'E/S (logement) que vous souhaitez afficher.

   La page I/O Module Status (État du module d'E/S) spécifique au logement du module IOM s'affiche. Les tableaux I/O Module Uplink Status (État des liaisons montantes du module d'E/S) et I/O Module Downlink Status (État des liaisons descendantes du module

d'E/S) s'affichent. Ces tableaux affichent des informations sur les ports de liaison descendante (1 à 8) et montante (9 à 12). Pour en savoir plus, consultez l'*Aide en ligne de CMC pour Dell PowerEdge FX2/FX2s*.

Affichage des informations sur les sessions FCoE de modules d'E/S à l'aide de l'interface Web

Vous pouvez afficher les informations concernant la session FCoE de Dell PowerEdge M I/O Aggregator à l'aide de l'interface Web CMC. Pour ce faire :

1. Accédez à **Présentation du châssis** > **Présentation du module d'E/S**.
   Tous les modules IOM (2) apparaissent dans la liste développée.
2. Cliquez sur le module d'E/S (logement) que vous souhaitez afficher. Cliquez sur **Propriétés** > **FCoE**.
   La page **Module d'E/S FCoE** spécifique au logement du module d'E/S s'affiche.
3. Dans la liste déroulante, **Sélectionner un port**, sélectionnez le numéro de port requis pour le module d'E/S sélectionné, puis cliquez sur **Afficher les sessions**. L'option sélectionnée récupère les informations de la session FCoE pour le commutateur et les présente à l'utilisateur sous la forme d'un tableau.
   La section **Informations sur la session FCoE** affiche les informations sur la session FCoE du commutateur.
   REMARQUE : L'agrégateur d'E/S affiche également les sessions FCoE actives lorsque le commutateur utilise le protocole.

Restauration des paramètres IOM par défaut définis en usine

Vous pouvez réinitialiser le module d'E/S (IOM) sur les paramètres d'usine par défaut dans la page **Déployer les modules d'E/S**.

REMARQUE : Cette fonctionnalité est prise en charge uniquement sur l'IOM PowerEdge M I/O Aggregator. Les autres IOM, y compris MXL 10/40 GbE, ne sont pas pris en charge.

Pour réinitialiser les paramètres par défaut définis en usine des IOM sélectionnés avec l'interface Web CMC :

1. Dans l'arborescence système, accédez à **Présentation du module d'E/S**, puis cliquez sur **Configuration** ou développez l'entrée **Présentation du module d'E/S**, sélectionnez le module d'E/S (IOM) voulu, puis cliquez sur **Configuration**.
   La page **Déployer les modules d'E/S** affiche les modules IOM allumés.
2. Pour les IOM requis, cliquez sur **Réinitialiser**.
   Un message d'avertissement s'affiche.
3. Cliquez sur **OK** pour continuer.

Mise à jour du logiciel IOM à l'aide de l'interface Web CMC

Vous pouvez mettre à jour le logiciel OIM en sélectionnant l'image du logiciel requis à partir d'un emplacement spécifié. Vous pouvez également revenir à une version logicielle antérieure.

REMARQUE : Cette fonction est prise en charge uniquement sur l'**Agrégateur d'E/S Dell PowerEdge**.

Pour mettre à jour le logiciel de périphérique d'infrastructure IOM dans l'interface Web CMC :

1. Accédez à **Présentation du châssis** > **Présentation du module d'E/S** > **Mise à jour**.
   La page Mise à jour du micrologiciel du module d'E/S (IOM) s'affiche. Vous pouvez également accéder à
   - **Présentation du châssis** > **Mise à jour**.
   - **Présentation du châssis** > **Contrôleur de châssis** > **Mise à jour**.

   La page Mise à jour du micrologiciel s'affiche. Elle fournit un lien pour accéder à la page Logiciel et micrologiciel IOM.
2. Dans la page Mise à jour du micrologiciel du module d'E/S (IOM), dans la section Micrologiciel, cochez la case dans la colonne Mise à jour correspondant à l'IOM dont vous souhaitez mettre à jour le logiciel et cliquez sur **Appliquer la mise à jour du micrologiciel**. Vous pouvez également revenir aux versions antérieures du micrologiciel en cochant la case correspondante dans la colonne Restauration.
3. Sélectionnez l'image de logiciel correspondant à la mise à jour du logiciel en utilisant l'option Parcourir. Le nom de l'image du logiciel s'affiche dans le champ Emplacement du logiciel IOM.

La section État de la mise à jour fournit des informations sur l'état de restauration ou de mise à jour du logiciel. Un indicateur d'état apparaît 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 micrologiciel s'affiche.

REMARQUE : Ne cliquez pas sur l'icône Actualiser et ne naviguez vers aucune autre page pendant le transfert de fichiers.

REMARQUE : L'horloge de transfert de fichiers ne s'affiche pas lors de la mise à jour du micrologiciel IOMINF.

REMARQUE : La version du logiciel FTOS ou IOM est affichée au format X-Y(A à B). Par exemple, 8-3(1-4). Si la Version de restauration de l'image FTOS est une vieille image qui utilise le format de la chaîne 8-3-1-4 de l'ancienne version, alors la version actuelle apparaîtra de la manière suivante : 8-3(1 à 4).

Interface GUI IOA ou MXL

Vous pouvez lancer l'interface GUI IOA/MXL à partir du CMC pour gérer la configuration IOA/MXL. Pour lancer l'interface GUI IOA/MXL à partir du contrôleur CMC, vous devez définir le module IOM sur IOA ou MXL et vous devez disposer du privilège d'administration de structure A.

L'interface GUI MXL de Dell PowerEdge FX2 prend en charge la modification du mode du commutateur de MXL à IOA et l'interface GUI IOA de PowerEdge FX2 prend en charge la modification du mode du commutateur de IOA à MXL.

Vous pouvez lancer l'interface GUI MXL/IOA à partir des pages **Présentation du châssis** , **Présentation du module d'E/S** et **État du module d'E/S**.

REMARQUE : Lors de la première connexion à l'application MXL, vous êtes invité à personnaliser le mot de passe.

Lancement de l'interface GUI IOA/MXL depuis la page Présentation du châssis

Accédez à **Présentation du châssis** > **Liens rapides** > **Lancer l'interface GUI du module d'E/S**. La page de connexion IOA/MXL s'affiche.

Lancement de l'interface GUI IOA/MXL depuis la page Présentation du module d'E/S

Dans l'arborescence de répertoires, accédez à **Présentation du module d'E/S**. Dans la page **État du module d'E/S**, cliquez sur **Lancer l'interface GUI du module d'E/S**. La page de connexion IOA/MXL s'affiche.

Lancement de l'interface GUI IOA/MXL depuis la page « État du module d'E/S »

Dans l'arborescence de répertoires, sous **Présentation du module d'E/S**, cliquez sur un commutateur IOA/MXL. Dans la page **État du module d'E/S**, cliquez sur **Lancer l'interface GUI du module d'E/S**. La page de connexion IOA/MXL s'affiche.

Module agrégateur d'entrée/sortie

Vous pouvez afficher les détails du module IOM dans l'interface RACADM, aux pages Chassis Health (Intégrité du châssis), IOM Overview (Présentation du module IOM) et IOM Status (État du module IOM). Ces informations peuvent aussi être consultées dans l'interface RACADM du contrôleur CM.

Les modes du module IOM sont les suivants :

- Autonome
- VLT
- Stacking

- PMux
- Commutateur entier

Vous pouvez afficher le mode IOM sous forme d'une info-bulle en sélectionnant Module IOM dans les pages **Intégrité du châssisÉtat du module d'E/S** et **Présentation du module d'E/S**.

Lors du changement de mode d'un agrégateur IOA disposant d'une adresse IP statique (du mode empilage au mode autonome), assurez-vous que le réseau de l'agrégateur IOA est modifié par DHCP. Dans le cas contraire, l'adresse IP statique est doublée sur tous les agrégateurs IOA.

Lorsque les modules IOM sont en mode empilage, l'ID de pile est identique au module IOM maître gravé dans l'adresse MAC lors de la mise sous tension initiale. L'ID de pile ne change pas lorsque le mode du module IOM est modifié. Par exemple, lors de la mise sous tension initiale, si le commutateur 1 est défini comme maître, l'adresse MAC de la pile est identique à celle du commutateur 1 gravé dans l'adresse MAC. Plus tard, lorsque le commutateur 3 est défini comme maître, l'ID de pile reste identique à l'adresse MAC du commutateur 1.

La commande racadm `getmacaddress` affiche l'adresse MAC I/F gravée dans l'adresse MAC + 2.

15

Utilisation du Gestionnaire VLAN

Vous pouvez attribuer ou afficher les paramètres VLAN sur les modules d'E/S à l'aide de l'option **Gestionnaire VLAN** .

REMARQUE : Cette fonctionnalité est prise en charge uniquement sur les systèmes Agrégateur d'E/S Dell PowerEdge.

Une fois que le mode de l'agrégateur d'E/S est passé d'empilement à autonome, retirez la configuration initiale et relancez l'agrégateur d'E/S. Vous ne devez pas enregistrer la configuration du système lors du nouveau lancement de l'agrégateur d'E/S.

Sujets :

Affecter des VLAN au module d'E/S

Les réseaux virtuels (VLAN) des modules d'E/S (IOM) vous permettent de séparer les utilisateurs en segments de réseau distincts pour des raisons de sécurité ou autres. Avec les VLAN, vous pouvez isoler les réseaux de chaque utilisateur sur un commutateur 32 ports. Vous pouvez associer les ports sélectionnés d'un commutateur au VLAN de votre choix et traiter ces ports comme un commutateur distinct.

L'interface Web CMC vous permet de configurer les ports de gestion intrabande (VLAN) des IOM.

Pour affecter un VLAN à un module d'E/S, accédez à **Présentation du châssis** > **Présentation du module d'E/S** > **Configuration** > **Gestionnaire VLAN**.

Dans la section **Affectation de VLAN** , sélectionnez le module d'E/S et le type de configuration. Vous devez également indiquer l'étendue de port et l'emplacement.

Changez ou modifiez les VLAN en effectuant une sélection dans la liste déroulante.

Configuration des paramètres VLAN des IOM à l'aide de l'interface Web CMC

Pour configurer les paramètres VLAN des IOM avec l'interface Web CMC :

1. Accédez à **Présentation du module d'E/S** , puis cliquez sur **Configurer le gestionnaire VLAN**.
   La page Gestionnaire VLAN affiche les modules d'E/S allumés et les ports disponibles.
2. Dans la section **Sélectionner un module d'E/S**, sélectionnez un type de configuration dans la liste déroulante, puis sélectionnez les IOM requis.
3. Dans la section **Spécifier une plage de ports**, sélectionnez la plage de ports de structure à attribuer aux IOM sélectionnés.
4. Utilisez les options **Sélectionner tout ou Désélectionner tout** pour appliquer les changements à tous les modules d'E/S (IOM) ou à aucun.

   ou

   Cochez la case de chaque logement spécifique pour sélectionner les IOM requis.
5. Dans la section **Modifier les VLAN**, entrez les ID VLAN des IOM. Entrez des ID VLAN appartenant à la plage 1-4 094. Les ID VLAN peuvent être entrés en tant que plage ou séparés par une virgule.
6. Sélectionnez l'une des options suivantes dans le menu déroulant, selon vos besoins :
   - Ajouter des VLAN marqués

- Supprimer des VLAN
- Mettre à jour les VLAN non marqués
- Réinitialiser tous les VLAN
- Afficher les VLAN

7. Cliquez sur **Enregistrer** pour mémoriser les nouveaux paramètres définis dans la page **Gestionnaire VLAN**.

   REMARQUE : La section Récapitulatif des VLAN de tous les ports affiche des informations sur les modules d'E/S (IOM) présents dans le châssis et les VLAN qui leur sont attribués. Cliquez sur **Enregistrer** pour enregistrer le récapitulatif des paramètres VLAN actuels dans un fichier csv.

   REMARQUE : La section VLAN gérés par CMC affiche le récapitulatif de tous les VLAN attribués aux IOM.

8. Cliquez sur **Appliquer**.
   Les paramètres réseau sont configurés pour les IOM.

Affichage des paramètres VLAN des IOM avec l'interface Web CMC

Pour afficher les paramètres VLAN des IOM avec l'interface Web CMC :

1. Accédez à **Présentation du module d'E/S**, puis cliquez sur **Configuration** > **Gestionnaire VLAN**.
   La page **Gestionnaire VLAN** s'affiche. La section Récapitulatif des VLAN de tous les ports affiche des informations sur les paramètres VLAN actuels des modules IOM.
2. Cliquez sur **Enregistrer** pour stocker les paramètres VLAN dans un fichier.

Affichage des paramètres VLAN actuels des IOM avec l'interface Web CMC

Pour afficher les paramètres VLAN actuels des modules d'E/S (IOM) avec l'interface Web CMC :

1. Accédez à **Présentation du module d'E/S**, puis cliquez sur **Configuration** > **Gestionnaire VLAN**.
   La page **Gestionnaire VLAN** s'affiche.
2. Dans la section **Modifier les VLAN**, sélectionnez **Afficher les VLAN** dans la liste déroulante, puis cliquez sur **Appliquer**.
   Un message s'affiche pour signaler la réussite de l'opération. Les paramètres VLAN actuels attribués aux modules IOM s'affichent dans le champ **Récapitulatif d'attribution des VLAN**.

Suppression de VLAN pour les IOM avec l'interface Web CMC

Pour supprimer des VLAN des modules d'E/S (IOM) avec l'interface Web CMC :

1. Accédez à **Présentation du module d'E/S**, puis cliquez sur **Configuration** > **Gestionnaire VLAN.**
   La page Gestionnaire VLAN s'affiche.
2. Dans la section **Sélectionner un module d'E/S**, sélectionnez les IOM voulus.
3. Dans la section **Modifier les VLAN**, sélectionnez **Supprimer des VLAN** dans la liste déroulante, puis cliquez sur **Appliquer**.
   Les VLAN attribués aux IOM sont supprimés.

   Un message s'affiche pour signaler la réussite de l'opération. Les paramètres VLAN actuels attribués aux modules IOM s'affichent dans le champ **Récapitulatif d'attribution des VLAN**.

Mise à jour des VLAN sans balise des IOM à l'aide de l'interface Web CMC

Pour mettre à jour les VLAN sans balise des modules IOM à l'aide de l'interface Web CMC :

REMARQUE : Les VLAN non marqués ne peuvent pas être définis pour un ID de VLAN qui est déjà balisé.

1. Accédez à **Présentation du module d'E/S** , puis cliquez sur **Configuration** > **Gestionnaire VLAN**.
   La page Gestionnaire VLAN s'affiche.
2. Dans la section **Sélectionner un module d'E/S**, sélectionnez les IOM voulus.
3. Dans la section **Spécifier une plage de ports**, sélectionnez la plage de ports de structure à attribuer aux IOM sélectionnés.
4. Utilisez les options **Sélectionner tout ou Désélectionner tout** pour appliquer les changements à tous les modules d'E/S (IOM) ou à aucun.

   ou

   Cochez la case de chaque logement spécifique pour sélectionner les IOM requis.
5. Dans la section **Modifier les VLAN**, sélectionnez **Mettre à jour les VLAN non marqués** dans la liste déroulante, puis cliquez sur **Appliquer**.
   Un message d'avertissement s'affiche, indiquant que les configurations du VLAN non marqué existant vont être écrasées par celles du VLAN non marqué nouvellement attribué.
6. Cliquez sur **OK** pour confirmer.
   Les VLAN non marqués sont mis à jour avec les configurations du VLAN non marqué nouvellement attribué.

   Un message s'affiche pour signaler la réussite de l'opération. Les paramètres VLAN actuels attribués aux modules IOM s'affichent dans le champ Récapitulatif d'attribution des VLAN.

Réinitialisation de VLAN des IOM à l'aide de l'interface Web CMC

Pour réinitialiser les VLAN des modules d'E/S (IOM) sur les configurations par défaut avec l'interface Web CMC :

1. Accédez à **Présentation du module d'E/S**, puis cliquez sur **Configuration** > **Gestionnaire VLAN**.
   La page Gestionnaire VLAN s'affiche.
2. Dans la section **Sélectionner un module d'E/S**, sélectionnez les IOM voulus.
3. Dans la section **Modifier les VLAN**, sélectionnez **Réinitialiser les VLAN** dans la liste déroulante, puis cliquez sur **Appliquer**.
   Un message d'avertissement s'affiche, indiquant que les configurations des VLAN existants vont être écrasées par les configurations par défaut.
4. Cliquez sur **OK** pour confirmer.
   Les VLAN sont attribués aux IOM sélectionnés en fonction des configurations par défaut.

   Un message s'affiche pour signaler la réussite de l'opération. Les paramètres VLAN actuels attribués aux modules IOM s'affichent dans le champ Récapitulatif d'attribution des VLAN.

REMARQUE : L'option **Réinitialiser à tous les VLAN** n'est pas prise en charge avec les IOA en mode Jonction de liaisons virtuelles (Virtual Link Trunking, VLT).

16

Gestion et surveillance de l'alimentation

Le châssis Dell PowerEdge FX2/FX2s est l'enceinte de serveurs la plus économe en énergie. Il contient des blocs d'alimentation et ventilateurs très économes 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. Elles vous permettent de gérer encore plus efficacement l'environnement des serveurs économes en énergie.

La gestion de l'alimentation dans le serveur PowerEdge FX2/FX2s est relativement différente de celle du PowerEdge VRTX. L'une des différences majeures dans la technique de gestion électrique est l'utilisation d'une limitation du système en boucle fermée (CLST) pour maintenir les limites énergiques souhaitées du châssis. Cette technique offre un meilleur contrôle et permet au châssis d'utiliser l'alimentation du bloc d'alimentation disponible de manière optimale.

Les fonctions de gestion de l'alimentation du PowerEdge FX2/FX2s aident les administrateurs à configurer l'enceinte afin réduire la consommation électrique et à régler l'alimentation en fonction des besoins spécifiques de l'environnement.

L'enceinte PowerEdge FX2/FX2s consomme du courant CA et distribue la charge sur le bloc d'alimentation actif (PSU). Le système peut générer jusqu'à 3 371 watts d'alimentation CA allouée aux modules de serveurs et à l'infrastructure d'enceinte associée. Cependant, cette capacité varie en fonction de la stratégie de redondance d'alimentation que vous sélectionnez.

L'enceinte PowerEdge FX2/FX2s peut être configurée pour n'importe laquelle des trois stratégies 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

OMPC gère alors :

- l'alimentation du serveur
- Capacité maximale de l'alimentation d'entrée du système

REMARQUE : L'alimentation 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 :

- Afficher l'état 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 :

- Redondance de réseau d'alimentation
- Sans redondance

- Redondance des alertes uniquement

Règle de redondance de réseau d'alimentation

La règle de redondance de réseau d'alimentation est également appelée règle 1+1 (un bloc d'alimentation actif et un bloc d'alimentation de secours).

La règle de redondance de réseau d'alimentation a pour but de permettre à un système d'enceinte de fonctionner dans un mode où l'enceinte peut tolérer les pannes d'alimentation en CA. Ces pannes peuvent provenir du réseau électrique en CA, du câblage et de la distribution, ou du bloc d'alimentation proprement dit. Lorsque vous configurez un système pour la redondance de réseau d'alimentation, branchez les blocs d'alimentation 1 et 2 à des réseaux d'alimentation différents.

Dans ce mode, le CMC assure la conservation de la consommation énergétique, assurant ainsi le fonctionnement continu du système sans dégradation en cas de panne du réseau d'alimentation ou d'un bloc d'alimentation. L'option de mise sous tension du serveur dépend de l'énergie disponible dans un bloc d'alimentation. Si la redondance n'est pas maintenue pour quelque raison que ce soit et à tout moment (par exemple, lors du retrait ou de l'échec d'un bloc d'alimentation), des alertes sont envoyées et l'intégrité du châssis devient **Critique**.

Stratégie Sans redondance

La stratégie Sans redondance est également connue sous le nom de stratégie 2+0.

Dans ce mode, toute la puissance des deux blocs d'alimentation est disponible et utilisée, mais il n'y a aucune garantie qu'une panne de bloc d'alimentation ou de réseau n'aura aucune incidence sur le fonctionnement du système.

Stratégie Alertes de redondance uniquement

La stratégie Alertes de redondance uniquement permet d'utiliser la capacité de deux blocs d'alimentation lors de la mise sous tension du serveur, pendant le traitement des alertes sur les conditions réelles telles que la suppression ou la panne d'un bloc d'alimentation, ou la consommation électrique réelle dépassant les capacités d'un seul bloc d'alimentation. Il s'agit de la stratégie par défaut.

Redondance de tolérance aux pannes

Cette stratégie utilise les limites de capacité de puissance d'un seul bloc d'alimentation (PSU) similaire à la stratégie Redondance du réseau d'alimentation. Dans ce mode, la consommation électrique de pointe du sous-système de l'UC est remplacée par une nouvelle limite IccMax. Cette stratégie s'applique uniquement aux serveurs lames Dell de 14e génération.

Défaillances du bloc d'alimentation

Les défaillances de bloc d'alimentation de tout type génèrent toujours des alertes, quelle que soit la stratégie de redondance sélectionnée.

Configuration de redondance par défaut

Alertes de redondance uniquement est la configuration de redondance par défaut d'un châssis doté de deux blocs d'alimentation.

Adaptation d'un traîneau multi-nœuds

Le PowerEdge FM120x4 est un traîneau demi largeur à plusieurs nœuds capable de prendre en charge quatre serveurs dotés de processeurs indépendants et d'un iDRAC associé. Il est conçu pour obtenir une efficacité énergétique optimale et les processeurs ne peuvent pas être supprimés. Les processeurs du PowerEdge FM120 partagent la même infrastructure d'alimentation ; par exemple, chacun dispose d'une seule source d'alimentation et de capteurs de température.

Surveillance de la consommation maximale du châssis

OpenManage Power Center (OMPC) peut être utilisé pour surveiller et contrôler la consommation énergétique des ordinateurs d'un centre de données. PowerEdge FX2/FX2s active OMPC en fournissant une disposition permettant de définir la valeur de puissance maximale pour le châssis et des limites pour guider la configuration de cette valeur maximale. Les limites inférieure et supérieure de puissance sont définies par le CMC et ne peuvent pas être configurées.

REMARQUE : La limite inférieure correspond à l'alimentation minimale nécessaire pour faire fonctionner le châssis en fonction de la configuration actuelle. La limite supérieure correspond à la puissance maximale disponible dans la stratégie de redondance actuelle.

REMARQUE : Si le mode Conservation de puissance maximale (MPCM) est activé sur le châssis, toutes les demandes d'alimentation à partir d'un serveur lame sont refusées. Le serveur lame n'est pas sous tension s'il existe une raison quelconque dans l'iDRAC ou le serveur lame exigeant que l'hôte démarre le cycle d'alimentation.

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
```

Affichage de l'état du bilan de puissance avec l'interface Web CMC

Pour afficher l'état du bilan de puissance à l'aide de l'interface Web du 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 avec les attributs **Limite de la puissance d'entrée système**, **Stratégie de redondance**, les détails du bilan de puissance avec les attributs **Capacité maximale d'alimentation d'entrée du système**, **Réserve de redondance d'entrée**, **Alimentation disponible pour la mise sous tension du serveur** et des informations concernant les blocs d'alimentation dans le cadre de l'alimentation du châssis. Pour en savoir plus, voir l'*Aide en ligne de CMC pour Dell PowerEdge FX2/FX2s*.

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 en savoir plus sur la commande **getpbinfo**, y compris les détails de sortie, voir la section concernant la commande **getpbinfo** dans le *Guide de référence de la ligne de commande RACADM de Dell Chassis Management Controller pour PowerEdge FX2/FX2s*.

Condition de la redondance et intégrité de l'alimentation globale

L'état de redondance est un facteur déterminant de l'intégrité d'alimentation globale. Lorsque la stratégie de redondance d'alimentation est par exemple définie sur Redondance de réseau d'alimentation et que la condition de redondance indique que le système fonctionne en mode redondant, l'intégrité d'alimentation globale est généralement **OK**. Si le bloc d'alimentation installé sur un châssis connaît une panne pour une raison quelconque, l'intégrité globale de l'alimentation du châssis affiche l'état **Non critique**. Toutefois, si les conditions de fonctionnement en mode de Redondance de réseau d'alimentation ne peuvent pas être remplies, la condition de la redondance est **Non**, et l'intégrité globale de l'alimentation devient **Critique**. En effet, le système ne peut pas fonctionner conformément à la stratégie de redondance configurée.

REMARQUE : Le CMC ne vérifie pas ces conditions au préalable lorsque vous modifiez la stratégie de redondance pour activer ou désactiver l'option Redondance de l'alimentation de réseau. Ainsi, la configuration de la stratégie de redondance peut provoquer une perte ou un rétablissement instantané de la redondance.

Gestion de l'alimentation après une défaillance de bloc d'alimentation

En cas de défaillance ou de retrait du bloc d'alimentation, l'alimentation fournie aux serveurs peut être réduite. Dans de rares cas, les serveurs peuvent être mis hors tension pour tenter de maintenir le fonctionnement. Configurer et maintenir la redondance de réseau permet d'éviter tout impact sur les serveurs lorsqu'une panne de bloc d'alimentation survient.

Modifications des règles de bloc d'alimentation et de redondance dans le journal des événements système

Les modifications apportées à l'état du bloc d'alimentation et à la stratégie de redondance de l'alimentation sont enregistrées comme des événements. Les événements liés aux blocs d'alimentation qui entraînent la consignation d'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 d'une sortie d'alimentation.

Le tableau suivant répertorie les entrées de journal SEL liées aux modifications des blocs d'alimentation :

Tableau 27. 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 modifications de l'état de la redondance de l'alimentation qui entraînent la consignation d'entrées dans le journal SEL sont la perte de la redondance et le rétablissement de la redondance pour un boîtier configuré avec la stratégie d'alimentation **Redondance du réseau d'alimentation** ou **Alertes de redondance uniquement**. Le tableau suivant répertorie les entrées de journal SEL liées aux modifications apportées à la stratégie de redondance de l'alimentation.

Tableau 28. Événements du journal SEL relatifs aux modifications de la stratégie de redondance d'alimentation

Événement de stratégie d'alimentation	Entrée du journal des événements système (SEL)
Perte de la redondance	Perte de la redondance du bloc d'alimentation.
Regain de la redondance	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, modules d'E/S, CMC, PCIe, et infrastructure du châssis). 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
- 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
- Désactiver la récupération de l'alimentation secteur

Économie d'énergie et bilan de puissance

Si la consommation d'énergiessance dépasse la limite de la puissance d'entrée système, l'alimentation fournie aux serveurs par le bloc d'alimentation est réduite de manière à maintenir le niveau nominal.

Configuration du bilan de puissance et de la redondance à l'aide de 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*.
   - **Règle de redondance**
   - **Désactiver le bouton d'alimentation du châssis**
   - **Mode d'économie d'énergie maximum**
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*> est égale à 0 (Sans redondance), 1 (Redondance de réseau d'alimentation) et 3 (Alertes de redondance uniquement). La valeur par défaut est 3.

     Par exemple, la commande suivante définit la stratégie de redondance sur :

     ```
     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*> représente un nombre compris entre la charge actuelle du châssis et 3371, qui représente la limite de puissance maximale en watts. La valeur par défaut est 3371.

  Par exemple, la commande suivante définit 3371 watts comme bilan de puissance maximal :

  ```
  racadm config -g cfgChassisPower -o
  cfgChassisPowerCap 3371
  ```

- Pour afficher la limite supérieure et la limite inférieure, tapez :

  ```
  racadm getconfig -g cfgchassispower -o cfgchassispowercap <lower,upper> bound
  ```

  où <*inférieure et supérieure*> représente la limite inférieure et la limite supérieure.

  ```
  racadm config -g cfgChassisPower -o
  cfgChassisPowerCap 3000
  ```

- 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 fonctionnalité de journalisation à distance de l'alimentation dépend des hôtes syslog distants précédemment configurés. La journalisation sur un ou plusieurs hôtes syslog distants doit être activée, sinon la consommation électrique est consignée. Cela peut être effectué via l'interface Web ou l'interface de ligne de commande (CLI) RACADM. Pour plus d'informations, reportez-vous aux instructions de configuration du journal syslog distant.

- Pour restaurer la gestion de l'alimentation CMC, entrez :

  ```
  racadm config -g cfgChassisPower -o
  cfgChassisServerBasedPowerMgmtMode 0
  ```

Pour en savoir plus sur les commandes RACADM relatives à l'alimentation du châssis, voir les sections **config**, **getconfig**, **getpbinfo** et **cfgChassisPower** du *Guide de référence de la ligne de commande RACADM de Dell Chassis Management Controller pour PowerEdge FX2/FX2s*.

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).

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 de tâches 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 de contrôle de l'alimentation suivantes pour les serveurs voulus :
   - **Aucune opération**
   - **Arrêt normal**
   - **Mettre le serveur sous tension**
   - **Mettre le serveur hors tension**
   - **Réinitialiser le serveur (redémarrage à chaud)**
   - **Exécuter un cycle d'alimentation sur le serveur (redémarrage à froid)**

   Pour en savoir plus sur les options, voir l'*Aide en ligne de CMC pour Dell PowerEdge FX2/FX2s*.
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 contrôle du châssis** pour effectuer 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 <action>
```

, où <*action*> indique l'opération à exécuter : cycle d'alimentation.

Pour plus d'informations sur les commandes RACADM, voir le *Guide de référence de la ligne de commande RACADM de Dell Chassis Management Controller pour PowerEdge FX2/FX2s*. disponible à l' adresse dell.com/support/manuals.

Configuration du bouton d'alimentation du traîneau

Vous pouvez définir le bouton d'alimentation du traîneau sur Désactivé, de sorte que lorsque vous appuyez sur le bouton d'alimentation du traîneau, rien ne se produit. Pour configurer le bouton d'alimentation du traîneau, accédez à **Présentation du châssis** > **Présentation du serveur** > **Alimentation** > **Contrôle**.

Dans **Propriétés**, cochez la case pour désactiver le bouton, ou décochez-la pour l'activer.

REMARQUE : Ce paramètre s'applique uniquement aux traîneaux multi-nœuds présents dans le châssis. Les autres traîneaux ne sont pas affectés.

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.

17

Configuration des logements PCIe

Le châssis PowerEdge FX2/FX2s contient huit logements PCIe en option, où chaque logement PCIe est attribué à un traîneau spécifique. Par défaut, tous les logements PCIe sont mappés. Vous pouvez activer ou désactiver l'attribution des logements PCIe aux serveurs à l'aide de l'interface Web CMC ou de commandes RACADM.

Les tableaux suivants répertorient les mappages PCIe pour les traîneaux de calcul pleine largeur, demi-largeur et quart de largeur.

Tableau 29. Mappage PCIe pour les traîneaux de calcul pleine largeur

Logement PCIe	Mappage pour les traîneaux pleine largeur (PowerEdge FC830)
Logement PCIe 1	3
Logement PCIe 2	3
Logement PCIe 3	1
Logement PCIe 4	1
Logement PCIe 5	3
Logement PCIe 6	3
Logement PCIe 7	1
Logement PCIe 8	1

Tableau 30. Mappage PCIe pour les traîneaux de calcul demi-largeur

Logement PCIe	Mappage pour les traîneaux demi-largeur (PowerEdge FC630)
Logement PCIe 1	4
Logement PCIe 2	4
Logement PCIe 3	2
Logement PCIe 4	2
Logement PCIe 5	3
Logement PCIe 6	3
Logement PCIe 7	1
Logement PCIe 8	1

Tableau 31. Mappage PCIe pour les traîneaux de calcul quart de largeur

Logement PCIe	Mappage pour les traîneaux quart de largeur (PowerEdge FC430)
Logement PCIe 1	3d
Logement PCIe 2	3c
Logement PCIe 3	1d
Logement PCIe 4	1c
Logement PCIe 5	3b
Logement PCIe 6	3a
Logement PCIe 7	1b
Logement PCIe 8	1a

REMARQUE : La gestion PCIe est uniquement prise en charge pour les systèmes PowerEdge FX2s et non PowerEdge FX2.

Pour plus d'informations sur le mappage de logements PCIe, voir le *Manuel du propriétaire Dell PowerEdge FD332*.

Pour en savoir plus sur la gestion des logements PCIe, voir l'*Aide en ligne de CMC pour Dell PowerEdge FX2/FX2s*.

REMARQUE : La fonctionnalité de surveillance sans agent n'est pas disponible pour les cartes réseau et PERC PCIe placées dans les logements PCIe du châssis. La surveillance sans agent est la solution de gestion de systèmes destinée aux serveurs PowerEdge de 12e génération de Dell. Il s'agit d'une solution hors bande, sans dépendance aux agents du système d'exploitation. La surveillance sans agent vous permet de surveiller le stockage rattaché au serveur (contrôleurs PERC, disques durs, boîtiers, etc.) à l'aide d'iDRAC sans avoir à installer d'agent sur le système géré ou la station de gestion. Pour plus d'informations sur la surveillance sans agent, consultez le livre blanc *Inventaire et surveillance sans agent des périphériques de stockage et réseau dans les serveurs Dell PowerEdge 12G* (en anglais) disponible sur le **Dell TechCenter**.

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 panneau de gauche, cliquez sur **Présentation du châssis** > **Présentation de PCIe**. Cliquez sur + pour afficher toutes les propriétés du logement requis.
- Pour afficher les informations d'un logement PCIe spécifique, cliquez sur **Présentation du châssis** > **Logement PCIe <numéro>** > **Propriétés** > **Condition**.

Affichage des propriétés des logements PCIe à l'aide de RACADM

Vous pouvez afficher une attribution de logement PCIe à un serveur à l'aide des commandes RACADM. Certaines commandes sont fournies ici. Pour en savoir plus sur les commandes RACADM, voir le *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Dell Chassis Management Controller pour PowerEdge FX2/FX2s) disponible sur le site **dell.com/support/manuals**.

REMARQUE : Le nom de la carte PCIe ne s'affiche qu'une fois que le BIOS a terminé l'auto-test de démarrage (`POST`) dans le traîneau associé. En attendant, le nom du périphérique est **Inconnu**.

- Pour afficher l'affectation en cours des périphériques PCIe aux serveurs, exécutez la commande suivante :

```
racadm getpciecfg -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 afficher les paramètres de configuration PCIe existantes, exécutez la commande suivante :

```
racadm getconfig -g cfgPCIe
```

REMARQUE : La carte PCIe n'est pas activée si la carte mezzanine ne se trouve pas dans le traîneau associé.

Réattribuation PCIe

La fonction de réattribution PCIe vous permet de mapper des logements PCIe attribués aux traîneaux de calcul situés dans les baies inférieures sur les traîneaux de calcul situés dans les baies supérieures.

Vous pouvez activer ou désactiver l'option de réattribution PCIe à l'aide de l'interface Web CMC, CMC WSMan ou RACADM. Vous devez disposer du privilège de configuration du châssis pour configurer ou modifier les paramètres de réattribution. Mettez hors tension tous les traîneaux de calcul situés dans le châssis avant de modifier les paramètres de réattribution. Lorsque les traîneaux de calcul sont mis sous tension après les modifications de réattribution, les logements attribués précédemment aux traîneaux de calcul situés dans la baie inférieure sont mappés sur les traîneaux de calcul situés dans la baie supérieure. Voici quelques exemples de réattribution PCIe :

- **Réattribution PCIe en pleine largeur (FW) FC830 :**
  - Les logements PCIe mappés sur le traîneau FW 3 (logements PCIe 1 à 4) sont réattribués au traîneau-1. Le traîneau-1 est mappé désormais sur les logements PCIe 1 à 8.
- **Réattribution PCIe en demi-largeur (HW) FC630 :**
  - Les logements PCIe mappés sur le traîneau HW 3 (logements PCIe 5 à 6) sont réattribués au traîneau-1. Le traîneau-1 est mappé désormais sur les logements PCIe 1 à 8.
  - Les logements PCIe mappés sur le traîneau HW 4 (logements PCIe 1 à 2) sont réattribués au traîneau-2. Le traîneau-2 est mappé désormais sur les logements PCIe 1 à 4.
- **Réattribution PCIe en quart de largeur (QW) FC430 :**
  - Le logement PCIe mappé sur le traîneau QW 3a (logement PCIe 6) est réattribué au traîneau-1a. Le traîneau-1a est mappé désormais sur les logements PCIe 6 à 8.
  - Le logement PCIe mappé sur le traîneau QW 3b (logement PCIe 5) est réattribué au traîneau-1b. Le traîneau-1b est mappé désormais sur les logements PCIe 5 à 7.
  - Le logement PCIe mappé sur le traîneau QW 3c (logement PCIe 2) est réattribué au traîneau-1b. Le traîneau-1b est mappé désormais sur les logements PCIe 2 à 4.
  - Le logement PCIe mappé sur le traîneau QW 3d (logement PCIe 1) est réattribué au traîneau-1d. Le traîneau-1d est mappé désormais sur les logements PCIe 1 à 3.

Pour plus d'informations, reportez-vous au *Dell PowerEdge FX2 and FX2s Enclosure Owner's Manual (Manuel du propriétaire de l'enceinte Dell PowerEdge FX2 et FX2s Enclosure)*.

Activation ou désactivation des réattributions PCIe à l'aide de l'interface Web CMC

1. Dans le volet de gauche, cliquez sur **Présentation de PCIe**.
   La page **État de PCIe** s'affiche.
2. Cliquez sur **Configuration**.
   La page **Mappage : Réattribution de logement PCIe** s'affiche.
3. Activez ou désactivez la case à cocher **Activer la réattribution de logements PCIe** et cliquez sur **Appliquer**.

Activation ou désactivation de l'interface PCIe distante en utilisant RACADM

Les valeurs d'entrée pour l'activation et la désactivation de la réattribution à un logement PCIe sont les suivantes :

- 1 (Activer)
- 0 (Désactiver)

Pour renoncer à une licence PCIe, exécutez la commande suivante :

```
racadm config -g cfgPCIe -o cfgPCIeReassignmentEnable 1
```

Pour renoncer à une licence PCIe, exécutez la commande suivante :

```
racadm config -g cfgPCIe -o cfgPCIeReassignmentEnable 0
```

Pour plus d'informations, voir le *Guide de référence de la ligne de commande RACADM de Dell Chassis Management Controller pour PowerEdge FX2/FX2s* disponible à l'adresse **dell.com/support/manuals**.

18

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

Sujets :

Collecte des informations de configuration, de la condition du châssis et des journaux avec RACDUMP

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`, voir le *Guide de référence de la ligne de commande RACADM de Dell Chassis Management Controller pour PowerEdge FX2/FX2s*.

Tableau 32. Commandes racadm pour les sous-systèmes

Sous-système	Commande RACADM
Informations générales sur le système/RAC	`getsysinfo`

Tableau 32. Commandes racadm pour les sous-systèmes (suite)

Sous-système	Commande RACADM
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 de NIC (module CMC)	`getniccfg`
Information du journal de suivi	`gettracelog`
Journal des événements RAC	`getraclog`
Journal des événements système	`getsel`

Téléchargement du fichier MIB 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 (Management Information Base) SNMP du contrôleur CMC à l'aide de l'interface Web 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` CMC vers votre système local.

   Pour plus d'informations sur le fichier `MIB` SNMP, voir le *Guide de référence SNMP de Dell OpenManage Server Administrator* à l'adresse **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 que le bloc d'alimentation du côté 1 (le logement de gauche) et le bloc d'alimentation du côté 2 (le logement de droite) soient présents et fonctionnels dans l'enceinte. En outre, la capacité de chaque bloc d'alimentation doit être suffisante pour prendre en charge les allocations de puissances totales pour que le châssis maintienne la **Redondance de réseau d'alimentation**.
  - **Solution B :** vérifiez que tous les blocs d'alimentation sont correctement connectés aux deux réseaux d'alimentation en CA : le bloc d'alimentation du côté 1 doit être connecté à l'un des réseaux d'alimentation en CA, et celui du côté 2 doit être connecté à l'autre réseau d'alimentation en CA, et les deux réseaux d'alimentation en CA doivent fonctionner. La **Redondance de réseau d'alimentation** est perdue si l'un des réseaux d'alimentation en 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 :** 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.
- **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 :** 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 suivi pour dépanner les incidents qui génèrent des alertes CMC. La réussite ou l'échec de chaque tentative de distribution par e-mail et/ou interruption SNMP est consigné dans le journal CMC. Des informations supplémentaires concernant chaque erreur sont journalisées dans le journal de suivi. Toutefois, comme SNMP ne confirme pas la transmission des interruptions, utilisez un analyseur de réseau ou un outil comme 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 CMC de manière à ce qu'il envoie des e-mails ou des interruptions SNMP lorsque des événements spécifiques se produisent.

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 du journal du châssis

CMC génère un journal des événements liés au châssis.

REMARQUE : Pour effacer le journal du châssis, vous devez disposer de droits d'**Administrateur d'effacement des journaux**.

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 CMC, ou réinstaller virtuellement les serveurs afin qu'ils fonctionnent comme s'ils avaient été retirés et réinsérés.

REMARQUE : Pour réinitialiser les composants, vous devez disposer du privilège **Administrateur de commandes de débogage**.

REMARQUE : La réinstallation virtuelle n'est pas disponible pour les nœuds individuels du PowerEdge FM120x4.

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 CMC, dans la section **État du CMC** , cliquez sur **Réinitialiser le CMC**. Le contrôleur CMC disponible est redémarré.

Pour en savoir plus, consultez l'*Aide en ligne de CMC pour Dell PowerEdge FX2/FX2s*.

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 :

REMARQUE : Les informations sur FlexAddress, les profils de serveur et le stockage étendu ne sont pas enregistrés ou restaurés avec la Configuration de châssis. Il est recommandé d'enregistrer les profils de serveur qui sont importants séparément du châssis à l'aide d'un partage de fichiers distant ou une copie enregistrée sur un poste de travail local. Pour en savoir plus sur l'exécution de ces opérations, voir la section Ajout ou enregistrement d'un profil

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.

Résolution des erreurs de protocole Network Time Protocol (NTP)

Il peut s'écouler entre 2 et 3 minutes entre la configuration du contrôleur CMC en vue de synchroniser l'horloge avec un serveur de temps distant sur le réseau et la modification réelle de la date et de l'heure. En l'absence de changement passé ce délai, un problème peut exister. Le contrôleur CMC peut ne pas pouvoir synchroniser l'horloge pour les motifs suivants :

- Problème de paramétrage du serveur NTP 1, du serveur NTP 2 et du 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 de protocole NTP, consultez les informations du journal de suivi du contrôleur CMC. Ce journal contient un message d'erreur pour les anomalies liées au protocole NTP. Si le contrôleur CMC ne peut se synchroniser avec l'un des serveurs NTP distants configurés, l'heure du contrôleur CMC se synchronise avec l'horloge du système local et le journal de suivi comporte 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
```

Si l'astérisque (*) n'apparaît pas pour l'un des serveurs configurés, ses paramètres sont peut-être incorrects. 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 être utile d'augmenter la valeur du paramètre `MaxDist` associé à `ntpd`. Avant de modifier ce paramètre, vérifiez bien ses conséquences, 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 la section Utilisation de la console de diagnostic.

Interprétation des couleurs des LED et des séquences de clignotement

Les voyants du châssis fournissent l'état suivant d'un composant :

- Une LED orange clignotant sur un module indique une panne de ce module.
- Les voyants bleus clignotants peuvent être configurés par l'utilisateur et utilisés à des fins d'identification. Pour plus d'informations sur la configuration, voir la section CMC_Stmp_Configuration des voyants pour identifier les composants du châssis.

Tableau 33. Couleur des LED et séquences de clignotement

Composant	Couleur de la LED, séquence de clignotement	État
CMC		Sous tension
		Micrologiciel en cours de téléversement
		Hors tension
	Bleu, continu	En activité
	Bleu, clignotant	Identificateur d'un module activé par l'utilisateur
	Orange, continu	Inutilisé
	Orange, clignotant	Panne
Serveur		Sous tension
		Micrologiciel en cours de téléversement
		Hors tension
	Bleu, continu	Serveur sélectionné sur le KVM
	Bleu, clignotant	Identificateur 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	Micrologiciel en cours de téléversement
	Vert, foncé	Hors tension
	Bleu, continu	Normal/maître de la pile
	Bleu, clignotant	Identificateur 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
	Bleu, continu	Normal
	Bleu, clignotant	Identificateur d'un module activé par l'utilisateur
	Orange, continu	Inutilisé
	Orange, clignotant	Panne
	Bleu, foncé	Pas de panne
Ventilateur	Vert, continu	Ventilateur en marche
	Vert, clignotant	Inutilisé
	Vert, foncé	Hors tension
	Orange, continu	Type de ventilateur non reconnu ; mettre à jour le micrologiciel CMC
	Orange, clignotant	Défaillance du ventilateur ; tachymètre hors de portée
	Orange, foncé	Inutilisé

Tableau 33. Couleur des LED et séquences de clignotement (suite)

Composant	Couleur de la LED, séquence de clignotement	État
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
PCI	Bleu, foncé	Sous tension
	Bleu, clignotant	L'identification PCI est en cours.
	Orange, clignotant	Panne
Traîneau de stockage	Orange, clignotant	Panne
	Bleu uni	Pas de panne

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, en obtenant les informations de restauration à l'aide du port série DB-9 ou en restaurant l'image de micrologiciel CMC.

Observation des LED afin d'isoler le problème

Le CMC est équipé d'un voyant qui change de couleur pour indiquer :

Tableau 34. Voyants d'état en couleur

Couleur	Description
Bleu	Fonctionnement normal
Bleu, clignotant	ID (allumé pendant 0,5 seconde, éteint pendant 0,5 seconde)
Orange	Résumé des erreurs du châssis
Orange, clignotant	Erreur du châssis et ID correspondant

Obtention des informations de récupération à partir du port série DB-9

Lorsque le voyant du CMC est orange, les informations de restauration sont disponibles via le port série DB-9 situé à l'avant du CMC.

Pour obtenir les informations de récupération :

1. Installez un NULL modem entre un système CMC et un système client.
2. Ouvrez un émulateur de terminal de votre choix (HyperTerminal, Minicom, etc.). Configurez-le ainsi : 8 bits, aucune parité, aucun contrôle de flux, débit en bauds 115 200.
   Un échec de la mémoire du noyau affichera un message d'erreur toutes les cinq secondes.
3. Appuyez sur la touche <Entrée>.

   Si une invite de restauration s'affiche, des informations supplémentaires sont disponibles. L'invite indique le numéro de logement CMC et le type d'échec.

   Pour afficher la cause de l'échec et la syntaxe de quelques commandes, entrez `recover`, puis appuyez sur <Entrée>.

Exemples d'invites :

```
recover1[self test] CMC self test failure
```

```
recover1[Bad FW images] CMC has corrupted images
```

- Si l'invite signale un échec de l'auto-test, il n'existe aucun composant CMC pouvant être dépanné. Le CMC est défectueux et doit être renvoyé à Dell.
- Si l'invite indique **Images FW erronée**, exécutez les tâches de la rubrique Récupération de l'image de micrologiciel 1.

Restauration d'une image de micrologiciel

Le CMC passe en mode de restauration lorsque l'amorçage de fonctionnement normal du CMC n'est pas possible. En mode de restauration, seul un petit sous-ensemble des commandes est disponible. Il permet de reprogrammer les périphériques Flash en téléversant le fichier de mise à jour du micrologiciel, `fx2_cmc.bin`. Il s'agit du même fichier d'image de micrologiciel que celui utilisé pour les mises à jour ordinaires du micrologiciel. Le processus de restauration affiche ses activités en cours et effectue l'amorçage dans le système d'exploitation du CMC à la fin du processus.

Lorsque vous entrez la commande recover et appuyez sur <Entrée> à l'invite de restauration, la cause de la restauration et les sous-commandes disponibles sont affichées. Voici un exemple de séquence de restauration :

```
recover getniccfg recover setniccfg 192.168.0.120 255.255.255.0 192.168.0.1 recover ping
192.168.0.100 recover fwupdate -g -a 192.168.0.100
```

REMARQUE : Connectez le câble réseau au port RJ45 le plus à gauche.

REMARQUE : En mode de restauration, vous ne pouvez pas envoyer normalement la commande ping au CMC car aucune pile réseau n'est active. La commande `recover ping <TFTP server IP>` vous permet d'envoyer la commande ping au serveur TFTP afin de vérifier la connexion réseau (LAN). Vous pouvez être contraint d'utiliser la commande `recover reset` après `setniccfg` sur certains systèmes.

Dépannage des problèmes de réseau

Le journal de suivi interne CMC vous permet de dépanner les alertes CMC et le réseau. Vous accédez au journal de suivi dans l'interface Web du CMC ou dans RACADM. Voir la section traitant de la commande `gettracelog` dans le manuel « *RACADM Command Line Reference Guide for iDRAC and CMC* » (Guide de référence de la ligne de commande RACADM pour iDRAC et CMC).

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 micrologiciel CMC (micrologiciel CMC interne) et non pas au système d'exploitation du système géré.

Informations générales de dépannage

Lorsqu'un message de réussite s'affiche après la fin d'une opération, comme un enregistrement d'un profil de serveur, il peut arriver que l'action ne soit pas mise en oeuvre.

Pour résoudre ce problème, vérifiez si l'un des ports de service du module CMC pour SSH, Telnet, HTTP ou HTTPS utilise les ports couramment utilisés par les services des systèmes d'exploitation tels que 111. S'il est utilisé par des ports de service CMC, définissez les paramètres sur un port non réservé. Pour en savoir plus sur les ports réservés, voir http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

Dépannage d'un module de stockage dans un châssis FX2

Les informations suivantes vous aident à résoudre les problèmes liés aux traîneaux de stockage dans le châssis FX2.

- **Problème :** Le module de stockage n'est pas détecté à l'insertion. Le module de stockage a été inséré et le serveur correspondant sous tension n'est pas détecté

  Résolution : Assurez-vous que le serveur associé est exécuté en cycle d'alimentation après l'insertion du module de stockage.

- **Problème :** Le module de stockage est inséré et le serveur associé est remis en cycle d'alimentation, mais le module de stockage n'est pas détecté.

  Solution : Consultez le journal du châssis pour obtenir plus de détails sur l'échec. Vérifiez s'il y a une défaillance matérielle, telle que l'absence de détection de bobine de câble ou de RAID.

- **Problème :** Le voyant orange du stockage clignote.

  Solution : Assurez-vous que le module de stockage est correctement inséré et consultez les messages d'avertissement dans le journal du châssis. Ce message d'erreur peut être désactivé uniquement si l'erreur sous-jacente est traitée et l'hôte associé est exécuté en cycle d'alimentation sans traîneau ou via le repositionnement virtuel du traîneau.

  Problème : La mise à jour du micrologiciel RAID du module de stockage n'a pas pris effet.

  Solution : En mode de fractionnement à deux hôtes, chaque hôte connecté au RAID du traîneau de stockage doit être mis progressivement sous tension pour que les modifications apportées au micrologiciel RAID prennent effet.

- **Problème :** L'option de réattribution de logements PCIe est désactivée dans l'interface GUI.

  Solution : Assurez-vous que tous les hôtes présents dans le châssis sont sous tension. Si vous tentez de modifier ce paramètre à partir de RACADM pendant qu'un hôte est sous tension, un message d'erreur s'affiche. Le privilège d'Administrateur de configuration du châssis est nécessaire pour changer ce paramètre.

- **Problème :** La réattribution de logements PCIe est activée et l'hôte est sous tension, mais les logements PCIe ne sont pas mis sous tension.

  Solution : Dans le journal du châssis, consultez les messages d'avertissement associés aux anciennes versions du BIOS, d'iDRAC ou d'hôtes non pris en charge.

- **Problème :** Impossible d'importer, exporter ou supprimer des licences du module de stockage.

  Résolution : Vous devez disposer du privilège Configuration de châssis pour importer, exporter et supprimer des licences du module de stockage.

Réinitialisation de mot de passe administrateur oublié

PRÉCAUTION : La plupart des réparations ne peuvent être effectuées que par un technicien de maintenance agréé. Effectuez les opérations de dépannage et les petites réparations autorisées par la documentation de votre produit, ou selon les instructions fournies en ligne ou par téléphone par l'équipe de maintenance et d'assistance technique. Tout dommage provoqué par une réparation non autorisée par Dell est exclu de votre garantie. Consultez et respectez les consignes de sécurité fournies avec votre produit.

Pour réaliser une opération de gestion, vous devez disposer de droits d'**Administrateur**. Le logiciel du contrôleur CMC intègre une fonctionnalité de protection par mot de passe que vous pouvez désactiver lorsque vous oubliez le mot de passe du compte administrateur. En cas d'oubli du mot de passe du compte administrateur, celui-ci peut être récupéré à l'aide du cavalier J_PWORD sur la carte du contrôleur CMC.

La carte du contrôleur CMC utilise un connecteur de réinitialisation de mot de passe à deux broches comme indiqué dans la figure suivante. Lorsque le cavalier est installé dans le connecteur de réinitialisation, le compte administrateur et le mot de passe par défaut sont réactivés et définis sur les valeurs par défaut `password: calvin` et `mot de passe : calvin`. Le compte administrateur est réinitialisé, que le compte ait été supprimé ou le mot de passe modifié.

REMARQUE : Assurez-vous que le module CMC est en mode passif avant de démarrer.

Pour réaliser une opération de gestion, vous devez disposer de droits d'**Administrateur**. En cas d'oubli du mot de passe du compte administrateur, celui-ci peut être réinitialisé à l'aide du cavalier J_PWORD sur la carte du contrôleur CMC.

Le cavalier J_PWORD utilise un connecteur à deux broches comme indiqué dans la figure suivante.

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 temporairement 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
```

1. Appuyez sur le loquet de verrouillage de la poignée du contrôleur CMC et tirez sur le panneau avant du module. Faites glisser le module CMC hors du boîtier.

   REMARQUE : Les décharges électrostatiques peuvent endommager le contrôleur CMC. Dans certains cas, de l'électricité statique peut s'accumuler sur votre corps ou sur un objet, puis de se décharger sur votre contrôleur CMC. Pour éviter les dommages causés par les décharges électrostatiques, prenez soin de décharger l'électricité statique de votre corps avant d'accéder au contrôleur CMC et de le manipuler hors du châssis.

2. Retirez la fiche de cavalier du connecteur de réinitialisation de mot de passe, puis insérez le cavalier à deux broches afin de réactiver le compte administrateur par défaut. Pour identifier le cavalier de mot de passe sur la carte du contrôleur CMC, voir la figure suivante.

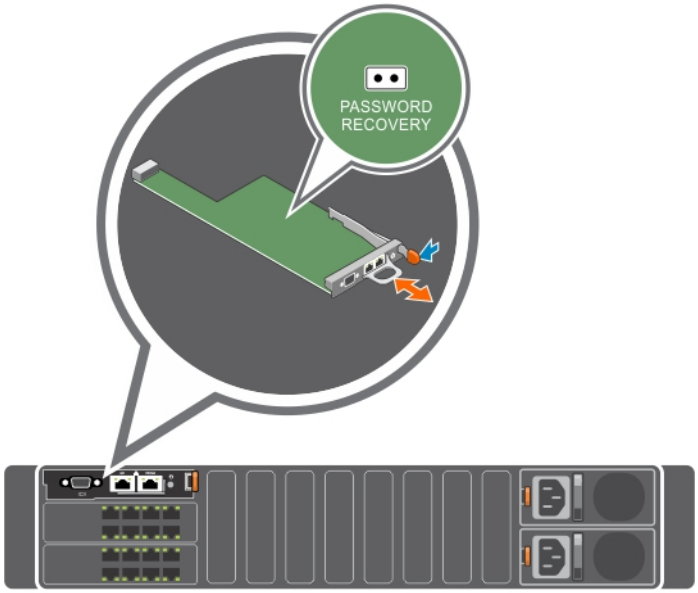


Tableau 35. Paramètres du cavalier de mot de passe CMC

J_PWORD		(par défaut)	La fonction de réinitialisation du mot de passe est désactivée.
			La fonction de réinitialisation du mot de passe est activée.

3. Faites glisser le module CMC dans le châssis. Rebranchez les câbles qui ont été débranchés.

   REMARQUE : Assurez-vous que le module CMC est actif jusqu'à la fin des étapes restantes.

4. Attendez que le réamorçage du contrôleur CMC soit terminé. Dans l'interface web, dans l'arborescence système, accédez à **Chassis Overview (Présentation du châssis)** et cliquez sur **Power (Alimentation)** > **Control (Contrôle)** ; puis, sélectionnez **Reset CMC (warm boot) [Réinitialiser le contrôleur CMC (amorçage à chaud)]**, puis cliquez sur **Apply (Appliquer)**.
5. Connectez-vous au contrôleur CMC à l'aide du nom d'utilisateur et du mot de passe par défaut de l'administrateur (root et calvin), puis restaurez les paramètres de compte nécessaires. Les comptes et mots de passe existants ne sont pas désactivés (ils restent actifs).

6. Effectuez les opérations de gestion requises, y compris la création d'un mot de passe administrateur.
7. Retirez le cavalier J_PWORD à 2 broches, puis replacez la fiche de cavalier.
   a. Appuyez sur le loquet de verrouillage de la poignée du contrôleur CMC et tirez sur le panneau avant du module. Faites glisser le module CMC hors du boîtier.
   b. Retirez le cavalier 2 broches et remettez en place la fiche de cavalier.
   c. Faites glisser le module CMC dans le châssis. Rebranchez les câbles qui ont été débranchés. Répétez l'étape 4 pour définir le module CMC ouvert comme contrôleur CMC actif.

19

Questions fréquemment posées

Cette section répertorie les questions courantes sur les éléments suivants :

- RACADM
- Gestion et restauration d'un système distant
- Active Directory
- 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'erreur 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

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 parce que le certificat par défaut envoyé au contrôleur CMC ne correspond pas au nom d'hôte du contrôleur CMC (avec 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**.

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.

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}
```

Modules d'E/S

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.

Messages d'erreur et d'événements

Après la rétrogradation du micrologiciel CMC de la dernière version du CMC aux versions antérieures, pourquoi le Journal du châssis affiche-t-il le message suivant pour certains journaux ?

```
USR8513 - MessageID missing from message registry.
```

Ce que vous voyez correspond à un nouveau message introduit dans la version actuelle du micrologiciel que les anciennes versions de micrologiciel ne peuvent pas interpréter. Pour en savoir plus sur l'ID de message, voir le *Event and Error Messages*

Reference Guide (Guide de référence des messages d'événement et d'erreur) sous OpenManage Software à l'adresse **www.dell.com/openmanagemanuals**.