

**Dell Chassis Management Controller Version
1.1 pour Dell PowerEdge FX2/FX2s
Guide d'utilisation**



Remarques, précautions et avertissements

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

Copyright © 2014 Dell Inc. Tous droits réservés. Ce produit est protégé par les lois sur les droits d'auteur et la propriété intellectuelle des États-Unis et des autres pays. Dell™ et le logo Dell sont des marques de Dell Inc. aux États-Unis et/ou dans d'autres juridictions. Toutes les autres marques et tous les noms de produits mentionnés dans ce document peuvent être des marques de leurs sociétés respectives.

2014 - 12

Rev. A00

Table des matières

1 Présentation.....	11
Principales fonctions.....	12
Nouveautés de cette version.....	12
Fonctions de gestion.....	12
Fonctionnalités de sécurité.....	13
Présentation du châssis.....	14
Connexions d'accès à distance prises en charge.....	15
Plates-formes prises en charge.....	16
Navigateurs Web pris en charge.....	16
Gestion des licences	16
Types de licence.....	16
Obtention de licences.....	17
Opérations de licence.....	17
Fonctions pouvant faire l'objet d'une licence dans le CMC.....	18
État ou condition de composant de licence et opérations disponibles.....	19
Affichage des versions traduites de l'interface Web CMC.....	19
Applications de console de gestion prises en charge.....	19
Utilisation du Guide d'utilisation.....	19
Autres documents utiles.....	20
Accès aux documents à partir du site de support Dell.....	21
2 Installation et configuration de CMC.....	22
Installation du matériel CMC.....	22
Liste de contrôle pour la configuration du châssis.....	22
Utilisation du logiciel d'accès à distance depuis une station de gestion.....	24
Installation de RACADM à distance.....	27
Installation de RACADM distante sur une station de gestion Windows.....	27
Installation de RACADM distante sur une station de gestion Linux.....	28
Désinstallation de RACADM à distance d'une station de gestion Linux.....	28
Configuration d'un navigateur Web.....	28
Téléchargement et mise à jour du micrologiciel CMC.....	29
Définition de l'emplacement physique et du nom du châssis.....	30
Définition de la date et de l'heure sur le CMC.....	30
Configuration des LED pour l'identification des composants du châssis.....	31
Configuration des propriétés de CMC.....	31
Configuration du panneau avant.....	31
Configuration de la gestion de châssis en mode Serveur.....	32
Configuration de gestion du châssis en mode Serveur à l'aide de l'interface Web du CMC.....	32

Configuration de la gestion de châssis en mode Serveur à l'aide de l'interface RACADM.....	33
3 Connexion au contrôleur CMC.....	34
Configuration de l'authentification par clé publique sur SSH.....	34
Génération de clés publiques pour des systèmes exécutant Windows.....	34
Génération de clés publiques pour des systèmes exécutant Windows.....	35
Accès à l'interface Web CMC.....	36
Connexion au contrôleur CMC comme utilisateur local, utilisateur Active Directory ou utilisateur LDAP.....	36
Connexion au contrôleur CMC avec une carte à puce.....	37
Connexion à CMC par connexion directe.....	38
Connexion au contrôleur CMC à l'aide de la console série, Telnet ou SSH.....	39
Connexion à CMC à l'aide de l'authentification par clé publique.....	39
Sessions CMC multiples.....	39
4 Mise à jour du micrologiciel.....	41
Image de micrologiciel de CMC signée.....	41
Téléchargement du micrologiciel du contrôleur CMC.....	42
Affichage des versions de micrologiciel actuellement installées.....	42
Affichage des versions du micrologiciel actuellement installées avec l'interface Web CMC....	42
Affichage des versions du micrologiciel actuellement installées à l'aide de RACADM.....	42
Mise à jour du micrologiciel du contrôleur CMC.....	42
Mise à jour du micrologiciel CMC à l'aide de l'interface Web.....	43
Mise à jour du micrologiciel CMC via RACADM.....	44
Mise à jour du micrologiciel CMC via DUP.....	44
Mise à jour du micrologiciel de l'infrastructure du châssis.....	44
Mise à jour du micrologiciel de l'infrastructure du châssis à l'aide de l'interface Web CMC....	45
Mise à jour du micrologiciel de l'infrastructure du châssis à l'aide de RACADM.....	45
Mise à jour du micrologiciel iDRAC du serveur.....	45
Mise à jour du micrologiciel du contrôleur iDRAC du serveur avec l'interface Web.....	46
Mise à jour du micrologiciel des composants de serveur.....	46
Activation du Lifecycle Controller.....	49
Sélection du type de mise à jour du micrologiciel des composants du serveur via l'interface Web CMC.....	50
Filtrage des composants pour les mises à jour micrologicielles.....	50
Affichage de l'inventaire des micrologiciels.....	51
Enregistrement du rapport d'inventaire du châssis à l'aide de l'interface Web CMC.....	52
Configuration du Partage réseau via l'interface Web du CMC.....	53
Opérations de tâche Lifecycle Controller.....	53
5 Affichage des informations de châssis et surveillance de l'intégrité du châssis et des composants.....	60

Affichage des récapitulatifs de châssis et de composants.....	60
Graphiques du châssis.....	60
Informations sur le composant sélectionné.....	61
Affichage du nom du modèle de serveur et du numéro de service.....	62
Affichage du résumé du châssis.....	63
Affichage des informations et de la condition du contrôleur de châssis.....	63
Affichage des informations et de la condition d'intégrité de tous les serveurs.....	63
Affichage des informations et de la condition d'intégrité du module IOM.....	63
Affichage des informations et de la condition d'intégrité des ventilateurs.....	64
Configuration des ventilateurs.....	65
Affichage des propriétés du panneau avant.....	65
Affichage des informations et de l'état d'intégrité KVM.....	65
Affichage des informations et de la condition d'intégrité des capteurs de température.....	66

6 Configuration de CMC..... 67

Activation ou désactivation de DHCP pour l'adresse d'interface réseau CMC.....	67
Activation de l'interface réseau CMC.....	68
Activation ou désactivation de la fonction DHCP pour les adresses IP DNS.....	69
Définition des adresses IP statiques du DNS.....	69
Affichage et modification des paramètres réseau (LAN) CMC.....	69
Affichage et modification des paramètres réseau (LAN) CMC dans l'interface Web CMC.....	70
Affichage et modification des paramètres réseau (LAN) CMC à l'aide de RACADM.....	70
Configuration des paramètres DNS (IPv4 et IPv6).....	70
Configuration de la négociation automatique, du mode duplex et de la vitesse réseau (IPv4 et IPv6).....	71
Configuration du port de gestion 2.....	71
Configuration du port de gestion 2 à l'aide de l'interface Web du CMC.....	72
Configuration du port de gestion 2 à l'aide de RACADM.....	72
Configuration des services.....	72
Configuration des services à l'aide de l'interface RACADM.....	73
Configuration de la carte de stockage étendu CMC.....	74
Configuration d'un groupe de châssis.....	74
Ajout de membres à un groupe de châssis.....	75
Retrait d'un membre du châssis maître.....	75
Dissolution d'un groupe de châssis.....	76
Désactivation d'un seul membre sur le châssis membre.....	76
Lancement de la page Web d'un châssis membre ou d'un serveur.....	76
Propagation des propriétés du châssis maître aux châssis membres.....	77
Synchronisation des propriétés d'un nouveau membre avec celles du châssis maître.....	77
Inventaire des serveurs pour un groupe CMC.....	78
Enregistrement de l'inventaire des serveurs.....	78
Configuration de plusieurs CMC à l'aide de RACADM.....	78

Règles d'analyse.....	79
Modification de l'adresse IP CMC.....	81
7 Configuration des serveurs.....	82
Définition des noms de logement.....	82
Configuration des paramètres réseau iDRAC.....	83
Configuration des paramètres réseau QuickDeploy (Déploiement rapide) iDRAC.....	83
Attributions d'adresses IP QuickDeploy pour les serveurs.....	86
Modification des paramètres réseau iDRAC de chaque iDRAC de serveur.....	87
Modification des paramètres réseau iDRAC avec RACADM.....	88
Configuration des paramètres de marquage VLAN iDRAC.....	88
Configuration des paramètres de marquage VLAN iDRAC dans l'interface Web.....	88
Configuration des paramètres de marquage VLAN iDRAC avec RACADM.....	88
Définition du premier périphérique de démarrage.....	89
Définition du premier périphérique d'amorçage pour plusieurs serveurs dans l'interface Web CMC.....	90
Définition du premier périphérique d'amorçage pour un seul serveur dans l'interface Web CMC.....	91
Définition du premier périphérique de démarrage à l'aide de l'interface RACADM.....	91
Configuration de liaison montante de réseau de chariot.....	91
Déploiement d'un partage de fichier à distance.....	92
Configuration de FlexAddress pour serveur.....	92
Configuration des paramètres de profil à l'aide de la réplication de la configuration de serveur.....	92
Accès à la page Profil.....	93
Gestion des profils stockés.....	93
Ajout ou enregistrement d'un profil.....	94
Application d'un profil.....	95
Importation de profil.....	95
Exportation de profil.....	95
Modification d'un profil.....	96
Affichage des paramètres de profil.....	96
Affichage des paramètres de profil stocké.....	97
Affichage du journal de profil.....	97
Statut d'achèvement et dépannage.....	97
Profils de déploiement rapide.....	98
Attribution de profils de serveur à des logements	98
Lancement d'iDRAC à l'aide d'une connexion directe (SSO).....	99
Lancement de la console distante depuis la page Condition du serveur.....	100
8 Configuration de CMC pour envoyer des alertes.....	101
Activation ou désactivation des alertes.....	101

Activation ou désactivation des alertes avec l'interface Web CMC.....	101
Activation ou désactivation des alertes à l'aide de l'interface RACADM.....	101
Filtrage des alertes.....	102
Configuration de destinations d'alerte.....	102
Configuration de destinations d'alerte pour interruption SNMP.....	102
Définition des paramètres d'alerte par e-mail.....	104
9 Configuration des comptes et des privilèges des utilisateurs.....	106
Types d'utilisateur.....	106
Modification des paramètres du compte administrateur de l'utilisateur root.....	110
Configuration des utilisateurs locaux.....	111
Configuration d'utilisateurs locaux à l'aide de l'interface Web CMC.....	111
Configuration d'utilisateurs locaux à l'aide de RACADM.....	111
Configuration des utilisateurs d'Active Directory.....	112
Mécanismes d'authentification Active Directory pris en charge.....	112
Présentation d'Active Directory avec le schéma standard.....	112
Configuration d'Active Directory avec le schéma standard.....	114
Présentation d'Active Directory avec schéma étendu.....	114
Configuration du schéma étendu Active Directory.....	114
Configuration d'utilisateurs LDAP générique.....	114
Configuration de l'annuaire LDAP générique pour accéder à CMC.....	115
Configuration du service d'annuaire LDAP générique à l'aide de l'interface Web CMC.....	115
Configuration du service d'annuaire LDAP générique à l'aide de RACADM.....	116
10 Configuration de CMC pour la connexion directe (SSO) ou la connexion par carte à puce.....	117
Configuration système requise.....	117
Systèmes clients.....	118
CMC.....	118
Prérequis pour la connexion directe ou par carte à puce.....	118
Génération d'un fichier Keytab Kerberos.....	118
Configuration du contrôleur CMC pour le schéma Active Directory.....	119
Configuration du navigateur pour la connexion directe (SSO).....	119
Internet Explorer.....	119
Mozilla FireFox.....	120
Configuration du navigateur pour la connexion avec une carte à puce.....	120
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.....	120
Configuration de la connexion directe ou par carte à puce CMC pour les utilisateurs Active Directory dans l'interface Web.....	120
Téléversement du fichier keytab.....	121

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.....	121
---	-----

11 Configuration du contrôleur CMC pour utiliser des consoles de ligne de commande.....123

Fonctions de la console de ligne de commande CMC.....	123
Commandes de la ligne de commande CMC.....	123
Utilisation d'une console Telnet avec CMC.....	124
Utilisation de SSH avec CMC.....	124
Schémas cryptographiques SSH pris en charge.....	125
Configuration de l'authentification par clé publique sur SSH.....	125
Configuration du logiciel d'émulation de terminal.....	126
Connexion aux serveurs ou au module d'E/S à l'aide de la commande connect.....	126
Configuration du BIOS du serveur géré pour la redirection de console série.....	128
Configuration de Windows pour la redirection de console série.....	128
Configuration de Linux pour la redirection de console série du serveur pendant le démarrage.....	128
Configuration de Linux pour la redirection de console série du serveur après l'amorçage....	129

12 Utilisation de cartes FlexAddress et FlexAddress Plus.....131

À propos de FlexAddress.....	131
À propos de FlexAddress Plus.....	132
Vérification de l'activation de FlexAddress.....	132
Désactivation de FlexAddress.....	133
Configuration de FlexAddress.....	134
Configuration de FlexAddress pour les structures et logements au niveau du châssis.....	134
Affichage des ID de nom universel/Contrôle de l'accès aux médias (WWN/MAC).....	135
Messages des commandes.....	135
CONTRAT DE LICENCE DES LOGICIELS DELL FlexAddress.....	136
Affichage des informations sur les adresses WWN/MAC.....	139
Affichage des informations de base sur les adresses WWN/MAC à l'aide de l'interface Web.....	140
Affichage des informations avancées sur les adresses WWN/MAC à l'aide de l'interface Web....	140
Affichage des informations sur les adresses WWN/MAC à l'aide de RACADM.....	141

13 Gestion des structures.....143

Surveillance de l'intégrité des modules d'E/S (IOM).....	143
Définition des paramètres réseau pour le module IOM.....	143
Définition des paramètres réseau du module IOM à l'aide de l'interface Web CMC.....	144
Définition des paramètres réseau d'un module IOM à l'aide de RACADM.....	144
Affichage de la condition des liaisons montantes et descendantes des modules d'E/S à l'aide de l'interface Web.....	144
Affichage des informations sur les sessions FCoE de modules d'E/S à l'aide de l'interface Web..	145

Restoration des paramètres IOM par défaut définis en usine.....	145
Mise à jour du logiciel IOM à l'aide de l'interface Web CMC.....	146
14 Utilisation du Gestionnaire VLAN.....	147
Affecter des VLAN au module d'E/S.....	147
Configuration des paramètres VLAN des IOM avec l'interface Web CMC	147
Affichage des paramètres VLAN des IOM avec l'interface Web CMC.....	148
Affichage des paramètres VLAN actuels des IOM avec l'interface Web CMC.....	148
Suppression de VLAN pour les IOM avec l'interface Web CMC.....	148
Mise à jour des VLAN non marqués pour les IOM avec l'interface Web CMC.....	149
Réinitialisation de VLAN pour les IOM avec l'interface Web CMC.....	149
15 Gestion et surveillance de l'alimentation.....	151
Stratégies de redondance.....	152
Règle de redondance de réseau.....	152
Stratégie Sans redondance.....	152
Stratégie Alertes de redondance uniquement.....	152
Défaillances du bloc d'alimentation.....	152
Configuration de redondance par défaut.....	153
Adaptation d'un chariot multi-nœuds.....	153
Surveillance de la consommation maximale du châssis.....	153
Affichage de la condition de la consommation électrique.....	153
Affichage de la condition de la consommation énergétique à l'aide de l'interface Web du CMC.....	153
Affichage de l'état de la consommation énergétique à l'aide de RACADM.....	153
Affichage de l'état du bilan de puissance avec l'interface Web CMC.....	154
Affichage de l'état du bilan de puissance avec RACADM.....	154
Condition de la redondance et intégrité énergétique globale.....	154
Gestion de l'alimentation après une défaillance de bloc d'alimentation.....	154
Modifications d'alimentation et de la règle de redondance dans le journal des événements système.....	155
Configuration du bilan d'alimentation et de la redondance.....	155
Exécution d'opérations de contrôle de l'alimentation.....	157
Exécution de tâches de contrôle de l'alimentation sur plusieurs serveurs avec l'interface Web CMC.....	158
Exécution d'opérations de contrôle de l'alimentation sur le module IOM.....	158
16 Affichage des logements PCIe.....	160
Affichage des propriétés des logements PCIe à l'aide de l'interface Web CMC.....	160
Affichage des propriétés des logements PCIe à l'aide de l'interface RACADM.....	161
17 Dépannage et restauration.....	162

Collecte des informations de configuration, de la condition du châssis et des journaux avec RACDUMP.....	162
Interfaces prises en charge.....	162
Téléchargement du fichier MIB (base d'information de gestion) SNMP.....	163
Premières étapes de dépannage d'un système distant.....	163
Dépannage des alertes.....	164
Affichage des journaux d'événements.....	165
Utilisation de la console de diagnostic.....	165
Réinitialisation des composants.....	166
Enregistrement ou restauration de la configuration de châssis.....	166
Résolution des erreurs de protocole de temps du réseau (NTP).....	166
Interprétation des couleurs des LED et séquences de clignotement.....	168
Dépannage des problèmes de réseau.....	171
Informations générales de dépannage.....	171
18 Questions fréquemment posées.....	172
RACADM.....	172
Gestion et restauration d'un système distant.....	173
Active Directory.....	174
Modules d'E/S.....	175
Messages d'erreur et d'événements.....	175

Présentation

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

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.
- Affiche les informations de mappage 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 les serveurs, notamment la gestion de l'alimentation et la gestion thermique. Voici d'autres fonctions CMC :

- 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 structure d'E/S entre le module d'E/S et les serveurs. Le contrôleur CMC désactive également les composants, si nécessaire, pour 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.

Principales fonctions

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

Nouveautés de cette version

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


- Serveurs lame de 13e génération.
- Inventaire des adresses WWN/MAC optimisées qui inclut des adresses WWN/MAC attribuées à un LOM/Select Network Adapter (SNA) à l'aide de la fonction d'Identité d'E/S de l'iDRAC.
- Affichage de l'état des partitions de carte réseau dans le cadre de l'Inventaire des adresses WWN/MAC indépendamment du système d'exploitation.
- Utilisation des répertoires dans le répertoire NFS/CIFS à distance pour les profils de serveur et l'espace de stockage personnalisé de DUP.
- Option permettant d'utiliser une bibliothèque externe (répertoire CIFS/NFS) pour mettre à jour les espaces de stockage et les profils.
- Option permettant d'afficher et d'utiliser des profils capturés stockés sur une bibliothèque externe.
- Inventaire des adresses WWN/MAC optimisées à l'aide de la fonction d'Identité d'E/S de l'iDRAC.
- Application de la vérification de signature pour les images de micrologiciel du CMC.
- Mise à jour du CMC via DUP

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 et de l'infrastructure du châssis.
- Mise à jour micrologicielle des composants des serveurs, tels que le BIOS, les contrôleurs de réseau, etc. sur plusieurs serveurs dans le châssis à l'aide du Lifecycle Controller.
- Intégration du logiciel Dell OpenManage : permet de lancer l'interface Web CMC à partir de Dell OpenManage Server Administrator ou d'OpenManage Essentials (OME) 1.2.
- Alertes CMC : signale les problèmes potentiels du nœud géré au moyen d'un message e-mail syslog distant ou d'une interruption SNMP.
- Gestion de l'alimentation à distance : offre des fonctionnalités de gestion de l'alimentation à distance, telles que la mise hors tension et la réinitialisation des composants du châssis, à partir d'une console de gestion.
- Rapport sur l'alimentation
- Cryptage SSL (Secure Sockets Layer) : permet une gestion sécurisée du système distant via l'interface Web.

- Point de lancement de l'interface Web iDRAC (Integrated Dell Remote Access Controller).
- Prise en charge de la gestion WS
- 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 d'Identité d'E/S de l'iDRAC pour l'Inventaire des adresses WWN/MAC optimisé.
- 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 de plusieurs châssis n'est pas prise en charge sur les réseaux IPv6.

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.

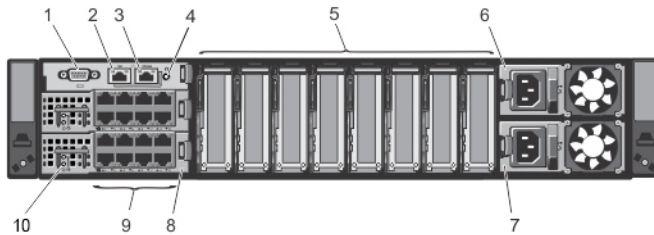
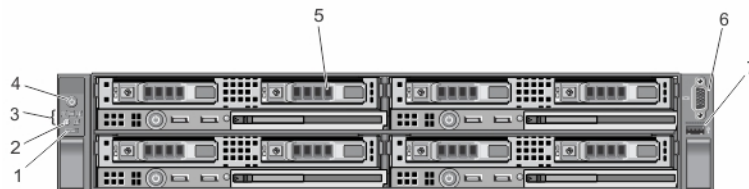


Figure 1.

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)
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.





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

Connexions d'accès à distance prises en charge

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

Tableau 1. Connexions d'accès à distance prises en charge

Connexion	Fonctions
Ports d'interface réseau CMC	<ul style="list-style-type: none"> • Ports Gb : interface réseau dédiée de l'interface Web du CMC. Le CMC possède deux ports Ethernet RJ-45 : <ul style="list-style-type: none"> – Gb1 (le port de liaison montante) – Gb2 (le port d'empilage ou port de consolidation des câbles). Le port STK/Gb2 peut aussi être utilisé pour le basculement de la carte réseau CMC. <p> REMARQUE : Vérifiez que le CMC est modifié pour passer du paramètre par défaut Empilage au paramètre Redondant pour la mise en œuvre du basculement de la carte réseau.</p> <p> PRÉCAUTION : La connexion du port STK/Gb2 au réseau de gestion peut provoquer des résultats imprévisibles si le paramètre CMC n'est pas modifié du paramètre par défaut Stacking (Empilage) au paramètre Redondant (Redondant) pour la mise en œuvre du basculement de la carte réseau. Dans 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. Une tempête de diffusion peut également se produire si le paramètre CMC est modifié pour passer au mode Redondant (Redondance), mais le câblage est connecté en boucle entre les châssis dans le mode Stacking (Empilage). Assurez-vous que le modèle de câblage correspond au paramètre CMC configuré pour l'utilisation prévue..</p> <ul style="list-style-type: none"> • Prise en charge de DHCP • Interruptions SNMP et notifications des événements par e-mail • Interface réseau pour le micrologiciel iDRAC et les modules d'E/S

Connexion	Fonctions
	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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).

Plates-formes prises en charge

Le CMC prend en charge les modèles de châssis **PowerEdge FX2** et **FX2s**. Les plateformes prises en charge sont l'PowerEdge FC630 et PowerEdge FM120x4. Pour en savoir plus sur la compatibilité avec CMC, consultez la documentation de votre périphérique.

Pour les dernières plateformes prises en charge, voir le document *Dell Chassis Management Controller (CMC) Version 1.1 for Dell PowerEdge FX2/FX2s Release Notes* (Notes de mise à jour de Dell Chassis Management Controller (CMC) Version 1.1 pour Dell PowerEdge FX2/FX2s) sur le site dell.com/support/manuals.

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 1.1 for Dell PowerEdge FX2/FX2s Release Notes* (Notes de mise à jour de Dell Chassis Management Controller (CMC) Version 1.1 pour Dell PowerEdge FX2/FX2s) sur le site dell.com/support/manuals.

Gestion des licences

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

Types de licence

Les types de licence proposés 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.


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, voir la section [Obtention de licences](#) et le Guide de présentation et des fonctions disponible sur le site support.dell.com.

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

Vous pouvez exécuter les opérations d'octroi de licences suivantes en utilisant le contrôleur CMC, RACADM et WS-MAN pour la gestion de licence individuelle, et Dell License Manager pour la gestion un-à plusieurs des licences :

- Afficher : affichage des informations de la licence en cours.
- Importer : après l'acquisition d'une licence, stockez la licence dans un emplacement de stockage local et importez-la vers le contrôleur CMC en utilisant l'une des interfaces prises en charge. La licence est importée si les vérifications de validation auxquelles elle est soumise aboutissent.
 -  **REMARQUE** : Pour un nombre limité de fonctions, il peut être nécessaire de redémarrer le contrôleur CMC pour activer les fonctions.
- Exporter : exportez la licence installée vers un périphérique de stockage externe pour disposer d'une sauvegarde ou la réinstaller après le remplacement d'un composant de service. Le nom de fichier et le format d'une licence exportée sont <EntitlementID>.xml.
- Supprimer : supprimez la licence affectée à un composant si le composant manque. Une fois la licence supprimée, elle n'est plus stockée dans le contrôleur CMC et les fonctions de base du produit sont activées.
- Remplacer : remplacement de la licence pour prolonger la période d'évaluation d'une licence, changer le type de licence (remplacement d'une licence d'évaluation par une licence achetée) ou étendre une licence expiré.
- Une licence d'évaluation peut être remplacée par une licence d'évaluation mise à niveau ou une licence achetée.
- Une licence achetée peut être remplacée par une licence mise à niveau ou une licence mise à jour. Pour en savoir plus, voir le Portail de gestion des licences de micrologiciel Dell à l'adresse [HTTPS://WWW.DELL.COM/SUPPORT/LICENSING/US/EN/19](https://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 plus d'informations, voir la documentation d'aide d'Internet Explorer.

 **REMARQUE** : Si vous tentez d'installer la licence PowerEdge FM120x4 sur un serveur PowerEdge FC630, l'installation de la licence échoue. Pour en savoir plus sur les licences, voir le *Integrated Dell Remote Access Controller (iDRAC) User's Guide* (Guide d'utilisation d'Integrated Dell Remote Access Controller).

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.

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
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 1. 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 traduites de l'interface Web 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.

Utilisation du Guide d'utilisation

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

- L'interface Web : seules les informations relatives aux tâches sont fournies ici. Pour plus d'informations sur les champs et les options, voir l'*Aide en ligne du contrôleur CMC pour Dell PowerEdge FX2/FX2s* que vous pouvez ouvrir depuis l'interface Web.

- Les commandes RACADM : la commande RACADM ou l'objet que vous devez utiliser sont fournis ici. Pour en savoir plus sur une commande 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.

Autres documents utiles

Pour accéder aux documents depuis le site d'assistance Dell. Outre ce guide de référence, vous pouvez accéder aux guides suivants sur le site dell.com/support/manuals.

- L'*aide en ligne de CMC FX2/FX2s* fournit des informations sur l'utilisation de l'interface Web. Pour accéder à l'aide en ligne, cliquez sur **Aide** dans l'interface Web de CMC.
- Le *Chassis Management Controller Version 1.1 for Dell PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller version 1.1 pour Dell PowerEdge FX2/FX2s) explique comment utiliser les fonctions RACADM de FX2/FX2s.
- Les *Dell Chassis Management Controller (CMC) for Dell PowerEdge FX2/FX2s Version 1.1 Release Notes* (Notes de mise à jour de Dell Chassis Management Controller (CMC) pour Dell PowerEdge FX2/FX2s version 1.1) contiennent les mises à jour de dernière minute du système ou de la documentation ou des informations de référence technique avancée destinées aux utilisateurs et techniciens expérimentés.
- Le *Integrated Dell Remote Access Controller 7 (iDRAC) User's Guide* (Guide d'utilisation d'Integrated Dell Remote Access Controller 7 (iDRAC7)) fournit des informations sur l'installation, la configuration et la maintenance de l'iDRAC7 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 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 PowerEdge 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 serveur contient des informations sur les fonctions du module du serveur et explique comment résoudre les problèmes associés au module et installer ou remplacer les composants du module. Ces 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.
- Les supports accompagnant le système qui fournissent la documentation et les outils de configuration et de gestion du système, y compris ceux du système d'exploitation, du logiciel de gestion du système, des mises à jour du système et les composants du système que vous avez achetés avec le système. Pour plus d'informations sur le système, scannez le QEL (Quick Resource Locator) disponible sur le système et la feuille d'informations concernant l'installation du système fourni avec le système. Téléchargez l'application QRL depuis votre plate-forme mobile pour disposer de l'application sur votre appareil mobile.

Des mises à jour sont parfois incluses dans le système pour décrire les changements apportés au système, au logiciel et/ou à la documentation. Lisez toujours ces documents en premier, car les informations qu'ils contiennent remplacent celles des autres documents.

Accès aux documents à partir du site de support Dell

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

- À l'aide des liens suivants :
 - Pour tous les documents Enterprise Systems Management : dell.com/softwaresecuritymanuals
 - Pour les documents Enterprise System Management : dell.com/openmanagemanuals
 - Pour les documents Remote Enterprise System Management : dell.com/esmmanuals
 - Pour les documents de gestion des systèmes OpenManage Connections Enterprise : dell.com/OMConnectionsEnterpriseSystemsManagement
 - Pour les documents Serviceability Tools : dell.com/serviceabilitytools
 - Pour les documents Client System Management : dell.com/clientsystemsmanagement
 - Pour les documents de gestion des systèmes OpenManage Connections Client : dell.com/connectionscientsystemsmanagement
- Sur le site de support Dell :
 - a. Rendez-vous sur dell.com/support/manuals.
 - b. Dans la section **General support** (Support général), cliquez sur **Software & Security** Logiciel et sécurité (Logiciels et sécurité).
 - c. Dans la zone de groupe **Software & Security** (Logiciels et sécurité), cliquez sur le lien approprié parmi les liens suivants :
 - **Enterprise Systems Management**
 - **Remote Enterprise Systems Management**
 - **Serviceability Tools**
 - **Client Systems Management**
 - **Connexions Client Systems Management**
 - d. Pour afficher un document, cliquez sur la version de produit requise.
- Avec les moteurs de recherche :
 - Saisissez le nom et la version du document dans la zone de recherche .

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.

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 CMC et la station de gestion où vous utilisez votre navigateur doivent se trouver sur le même réseau, appelé réseau de gestion. Connectez un câble réseau Ethernet du port étiqueté **GB** au réseau de gestion.

Réseau de gestion : le CMC et l'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 au module d'E/S (IOM). Cela permet d'isoler le réseau d'application du réseau de gestion. Il est important de séparer ce trafic pour garantir l'accès ininterrompu à la gestion du châssis.


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

2. Le port STK/Gb2 peut aussi être utilisé pour le basculement de la carte réseau du CMC. Vérifiez que le CMC est modifié pour passer du paramètre par défaut **Empilage** au paramètre **Redondant** pour la mise en œuvre du basculement de la carte réseau. Pour en savoir plus, 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 le paramètre CMC n'est pas modifié du paramètre par défaut **Stacking (Empilage)** au paramètre **Redondant (Redondant)** pour la mise en œuvre du basculement de la carte réseau. Dans 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. Une tempête de diffusion peut également se produire si le paramètre CMC est modifié pour passer au mode **Redondant (Redondance)**, mais le câblage est connecté en boucle entre les châssis dans le mode **Stacking (Empilage)**. **Assurez-vous que le modèle de câblage correspond au paramètre CMC configuré pour 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 sous tension le châssis, appuyez sur le bouton d'alimentation ou utilisez les interfaces suivantes après avoir effectué la tâche 6. À l'aide de l'interface Web CMC, accédez à **Présentation du châssis** → **Alimentation** → **Contrôle** → **Option de contrôle de l'alimentation** → **Mise sous tension du système**. Cliquez sur **Appliquer**.

Vous pouvez également mettre sous tension le châssis 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 CMC est Statique, et l'adresse IP CMC est 192.168.0.120. Si vous souhaitez que la configuration réseau devienne DHCP, connectez un câble série au port série du CMC. Pour plus d'informations sur la connexion série, reportez-vous à la rubrique concernant la configuration du protocole/d'interface série de la section [Utilisation du logiciel d'accès à distance depuis une station de gestion](#) .

Une fois la connexion série établie, connectez-vous et utilisez la commande `racadm setniccfg -d` pour changer la configuration du réseau à DHCP. Le contrôleur CMC prend de 30 à 60 secondes environ 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 :
 1. Connectez l'une des extrémités du câble modem null en série au connecteur série situé à l'arrière du châssis.
 2. Connectez l'autre extrémité du câble au port série du système de gestion.
 3. Une fois la connexion établie, connectez-vous au CMC à l'aide des références du compte root par défaut.
 4. 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 :
 1. 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 serveur à l'aide de KVM](#).


2. Allumez le serveur.
3. Assurez-vous que le serveur est configuré pour un amorçage en mode UEFI (Unified Extensible Firmware Interface).

4. Appuyez sur F2 pour accéder à la page Configuration du système.
5. Dans la page **Configuration du système**, cliquez sur **Paramètres iDRAC → 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 **Paramètres iDRAC** dans l'interface GUI de l'iDRAC, voir le *Dell Integrated Dell Remote Access Controller (iDRAC) User's Guide* (Guide d'utilisation d'Integrated Dell Remote Access Controller (iDRAC)).

8. Connectez-vous à l'adresse IP du CMC avec un navigateur Web en saisissant les références du compte root par défaut.
9. Configurez les paramètres réseau iDRAC selon vos besoins. Par défaut, le LAN iDRAC est activé avec une adresse IP statique. Pour déterminer l'adresse IP statique par défaut avec une **licence Enterprise**, accédez à **Présentation du serveur → Configurer → iDRAC**. Vous pouvez également déterminer l'adresse IP statique avec une **licence Express**. Accédez à **Présentation du serveur → Serveur-Logement → Configurer → iDRAC**.
10. Attribuez une adresse IP au module d'E/S (le cas échéant) dans l'interface Web CMC. Vous pouvez obtenir l'adresse IP en cliquant sur **Présentation du module d'E/S**, puis sur **Configurer**.
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).

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.

Interface/Protocole	Description
Série	<p>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.</p> <ul style="list-style-type: none"> • Linux Minicom • HyperTerminal Hilgraeve pour Windows <p>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.</p> <p>Configurez votre logiciel d'émulation de terminal avec les paramètres suivants :</p> <ul style="list-style-type: none"> • 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

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 le réseau. 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.

WS-MAN


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 <nom de communauté du CMC> <adresse IP du CMC>.  
1.3.6.1.4.1.674.10892.2.1.1.6.0
```

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 WS-MAN, 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 WS-MAN.

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 WS-MAN 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 DMTF : dmtf.org/standards/profiles/
- Fichier des notes de mise à jour WS-MAN
- www.wbemsolutions.com/ws_management.html
- 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 avec Dell Server Administrator, lancez Server Administrator sur la station de gestion. Dans le volet de gauche de la page d'accueil Server Administrator, cliquez sur **Système** → **Châssis principal du système** → **Contrôleur d'accès à distance**. Pour plus d'informations, voir le *Guide d'utilisation de Dell Server Administrator* sur le site 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 `<chemin>\SYSMGMT\ManagementStation\windows\DRAC\<nom du fichier .msi>`


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 avec 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 d'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](http://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 de Microsoft

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

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

### Téléchargement de fichiers à partir de CMC dans Internet Explorer

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

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

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

### Activation des animations dans Internet Explorer

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

Pour configurer Internet Explorer pour la lecture d'animations :

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

### 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](http://dell.com/support/manuals).

Par exemple : `racadm setractime -l 20140207111030`.

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

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

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

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

### Configuration du clignotement des LED avec l'interface Web CMC

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

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

 **REMARQUE** : Sur cette page, vous pouvez uniquement sélectionner des serveurs.

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 avec RACADM

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

`racadm setled -m <module> [-l <ledState>]`, où `<module>` 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 `<ledState>` 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** → **Configuration** .
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 l'interface 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 fournit la possibilité de gérer et de surveiller les composants partagés par le châssis et les nœuds du châssis en tant que serveurs rack. Lorsque cette fonction est activée, vous pouvez gérer et surveiller les ventilateurs du châssis, les blocs d'alimentation, les capteurs de température et vous pouvez mettre à jour et configurer le micrologiciel CMC via les composants suivants :

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

## Configuration de gestion du châssis en mode Serveur à l'aide de l'interface Web du 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 vous ne pouvez pas effectuer une mise à jour de micrologiciel au moyen d'iDRAC, du système d'exploitation 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 par le biais d'iDRAC, du système d'exploitation ou du Lifecycle Controller.

## Configuration de la gestion de châssis en mode Serveur à l'aide de l'interface 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`

## 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.

### 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 ou SSH-2 DSA 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 bits et la taille de la clé DSA recommandée est de 1 024 bits.

 **REMARQUE :**

- Le contrôleur CMC peut ne pas afficher de message si vous ajoutez des clés de moins de 768 bits ou de plus de 4 096 bits, mais lorsque vous essayez de vous connecter avec ces clés, la connexion échoue.
- Pour les clés DSA supérieures à 2 048 bits, utilisez la commande racadm suivante. CMC accepte les clés RSA de taille allant jusqu'à 4 096 bits, mais la taille de clé recommandée est de 1 024 bits.

```
racadm -r 192.168.8.14 -u <default root account username> -p <default root account password> sshpkauth -i svcacct -k 1 -p 0xffff -f dsa_2048,pub
```

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 passe pour sécuriser la clé. Veillez à bien enregistrer la clé privée.

4. Vous pouvez utiliser la clé publique de deux façons :
  - Enregistrer la clé publique dans un fichier à téléverser ultérieurement.
  - Copier/coller le texte de la fenêtre **Clé publique à coller** lors de l'ajout du compte à l'aide de l'option de texte.

## Génération de clés publiques pour des systèmes exécutant Windows

L'application ssh-keygen pour clients Linux est un outil de ligne de commande sans interface utilisateur graphique. Ouvrez une fenêtre de terminal et entrez la commande suivante à l'invite shell :

```
ssh-keygen -t rsa -b 1024 -C testing
```

où

L'option `-t` doit être `dsa` ou `rsa`.


`-b` spécifie la taille du cryptage binaire entre 768 et 4 096.

`-c` permet de modifier le commentaire de la clé publique ; l'option est facultative.

La valeur `<passphrase>` est facultative. Une fois la commande exécutée, utilisez le fichier public pour 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](http://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 comme 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 vivement 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, à, 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.

## 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 `<nomcmc.nom-de-domaine>:<numéro de port>`, où `nomcmc` est le nom d'hôte CMC du contrôleur CMC, `nom-de-domaine` 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 à 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 `cmcname` est le nom d'hôte CMC du contrôleur CMC, `domain-name` est le nom du domaine et `port number` est le numéro du port HTTPS.

Le contrôleur CMC vous connecte en utilisant les références Kerberos mises en cache par votre navigateur lorsque vous vous êtes connecté avec votre compte Active Directory valide. Si la connexion échoue, le navigateur est redirigé vers la page de connexion CMC normale.

 **REMARQUE** : Si vous n'êtes pas connecté au domaine Active Directory et que vous n'utilisez pas le navigateur Internet Explorer, la connexion échoue et le navigateur affiche une page vierge.

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

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

Une fois le logiciel d'émulation de terminal de la station de gestion 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 CMC, puis appuyez sur <Entrée>. Vous êtes connecté au contrôleur CMC.

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

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

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

Par exemple :

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

Lorsque vous vous connectez en utilisant le compte de service et qu'une 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 2. Sessions CMC multiples**

| Interface         | Nombre de sessions |
|-------------------|--------------------|
| Interface Web CMC | 4                  |
| RACADM            | 4                  |
| Telnet            | 4                  |

| <b>Interface</b> | <b>Nombre de sessions</b> |
|------------------|---------------------------|
| SSH              | 4                         |

## Mise à jour du micrologiciel

Vous pouvez mettre à jour le micrologiciel de :

- Contrôleur CMC
- Infrastructure du châssis
- Module d'E/S
- PERC
- Disque dur et Extenseur

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

- BIOS
- iDRAC7 sur FM120x4 (serveurs de 12e génération)
- iDRAC8 sur FC630 (serveurs de 13e génération)
- Lifecycle Controller
- Diagnostics 32 bits
- Pack de pilotes de système d'exploitation
- Contrôleurs d'interface réseau (NIC)
- Contrôleurs RAID

### Image de micrologiciel de CMC signée

Le micrologiciel CMC intègre une signature. Le micrologiciel CMC effectue une étape de vérification de signature afin de vérifier l'authenticité du micrologiciel téléchargé. La mise à jour du micrologiciel est réussie uniquement si l'image du micrologiciel est authentifiée par CMC pour être une image valide auprès du fournisseur de service n'a pas encore été modifiée. La mise à jour du microprogramme est interrompue si CMC ne peut pas vérifier la signature de l'image de micrologiciel téléchargée. Un événement d'avertissement est alors journalisé et un message d'erreur approprié s'affiche.

Lorsque vous tentez de mettre à niveau la version de micrologiciel du CMC, le processus de mise à jour du micrologiciel du CMC vérifie l'image de micrologiciel dans la version sélectionnée pour la signature auprès du fournisseur de service. La mise à jour du micrologiciel est arrêtée si la signature est introuvable ou si la vérification de l'image a échoué. Un événement d'avertissement est journalisé et un message d'erreur approprié s'affiche.

Lorsqu'une rétrogradation de micrologiciel vers une version antérieure est effectuée, le processus de mise à jour du micrologiciel du CMC vérifie l'image de micrologiciel des versions précédentes pour la présence de la signature auprès du fournisseur de services. La rétrogradation vers une version antérieure du micrologiciel est arrêtée si la signature de la version précédente n'est pas reconnue par le

micrologiciel CMC actuel. Le micrologiciel CMC journalise un événement d'avertissement et un message d'erreur approprié s'affiche.

## 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](http://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 avec l'interface Web CMC

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

- **Présentation du châssis** → **Mise à jour**
- **Présentation du châssis** → **Contrôleur de châssis** → **Mise à jour**
- **Présentation du châssis** → **Présentation du serveur** → **Mise à jour des composants serveur**

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




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

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

Vous pouvez afficher les versions du micrologiciel actuellement installées à l'aide de la commande `racadm getversion`. Pour en savoir plus sur les autres commandes RACADM, voir le *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (Guide de référence de ligne de commande de Chassis Management Controller pour PowerEdge FX2/FX2s).

## Mise à jour du micrologiciel du contrôleur CMC

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

-  **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 vous utilisez une session d'interface utilisateur Web pour mettre à jour le micrologiciel des composants système, le paramètre Délai d'attente en cas d'inactivité (**0, 60-10800**) doit avoir une valeur suffisamment élevée pour gérer la durée du transfert de fichiers. Dans certains cas, le transfert du fichier de micrologiciel peut prendre jusqu'à 30 minutes. Pour définir le délai d'attente en cas d'inactivité, voir [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 les autres utilisateurs au cours d'une réinitialisation, informez les utilisateurs autorisés susceptibles de se connecter au contrôleur CMC et vérifiez les sessions actives dans la page **Sessions**. Pour ouvrir la page **Sessions**, sélectionnez **Présentation du châssis** dans le volet de gauche, puis cliquez sur **Réseau** et sur **Sessions**.

Lors du transfert de fichiers vers et depuis le contrôleur CMC, l'icône de transfert tourne. Si l'icône n'est pas animée, vérifiez que le navigateur est configuré pour autoriser les animations. Pour plus d'informations sur l'autorisation des animations dans le navigateur, voir [Autoriser les animations dans Internet Explorer](#).

## Mise à jour du micrologiciel CMC à l'aide de 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> <image de micrologiciel>`.

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*.

## Mise à jour du micrologiciel CMC via DUP

Vous pouvez mettre à jour la version du micrologiciel du CMC à l'aide de DUP (Dell Update Package) via les éléments suivants :

- 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 *Integrated Dell Remote Access Controller User's Guide* (Guide d'utilisation d'iDRAC).

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

- Le progiciel du micrologiciel 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 du système d'exploitation ou Lifecycle Controller, l'option iDRAC **Activer la mise à jour des composants partagés via le SE/USC** doit être activée. Pour en savoir plus sur comment activer cette option, voir la section *Integrated Dell Remote Access Controller User's Guide* (Guide d'utilisation 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> <image de micrologiciel>`.

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 de type un-à-plusieurs dans le CMC vous permet de mettre à jour le micrologiciel de composants de serveur sur plusieurs serveurs. Vous pouvez mettre à jour les composants de serveur à l'aide des progiciels Dell Update Packages disponibles sur le système local ou sur un partage réseau. Cette opération est activée en tirant parti de la fonctionnalité du Lifecycle Controller sur le serveur.

Le service Lifecycle Controller est disponible sur chaque serveur et fourni par l'iDRAC. Vous pouvez gérer le micrologiciel des composants et périphériques des 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.

Le Lifecycle Controller prend en charge les mises à jour des modules pour les serveurs iDRAC7 et versions supérieures. Vous devez utiliser le micrologiciel iDRAC version 2.3 ou supérieure pour mettre le micrologiciel à jour avec le Lifecycle Controller.

Les modules DUP (Dell Update Packages) permettent de mettre à jour le micrologiciel en utilisant le service Lifecycle Controller. Le DUP du composant Operating System Driver Pack dépasse cette limite et doit être mis à jour séparément en utilisant la fonction de stockage étendu.

 **REMARQUE :** Avant d'utiliser la fonction de mise à jour basée sur le service Lifecycle Controller, vous devez mettre à jour les versions du micrologiciel des serveurs. Vous devez également mettre à jour le micrologiciel du contrôleur CMC avant de mettre à jour les modules de micrologiciel des composants des serveurs.

 **REMARQUE** : Pour mettre à jour le micrologiciel de composants, l'option CSIOR doit être activée pour les serveurs. Pour activer l'option CSIOR sur :

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

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

 **REMARQUE** : Notez les points suivants :

- Lors de la sélection des composants de serveur individuels en vue de la mise à jour, assurez-vous qu'il n'existe aucune dépendance entre les composants sélectionnés. Si ce n'est pas le cas, la sélection de certains composants qui ont des dépendances avec d'autres composants par rapport à la mise à jour peut provoquer un arrêt brutal de fonctionnement du serveur.
- Assurez-vous de mettre à jour les composants de serveur dans l'ordre prescrit. Sinon, le processus de mise à jour du micrologiciel de 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 des serveurs lames par la fonction Clic unique ou la méthode **Mettre à jour depuis le partage réseau** vous permet de mettre à jour le micrologiciel des composants du serveur à l'aide des fichiers DUP stockés sur le partage réseau. Vous pouvez utiliser la fonction de mise à jour du Dell Repository Manager (DRM) pour accéder aux fichiers DUP stockés sur un partage réseau et mettre à jour les composants du serveur en une seule opération. Vous pouvez définir un espace de stockage distant personnalisé de DUP de micrologiciels et des images binaires à l'aide du Dell Repository Manager et le partager sur le partage réseau. Vous pouvez également utiliser le Dell Repository Manager (DRM) afin de vous procurer les dernières mises à jour de micrologiciel disponibles. Le Dell Repository Manager (DRM) permet de s'assurer que les systèmes Dell sont à jour avec la dernière version du BIOS, des pilotes, des micrologiciels et des logiciels. Vous pouvez rechercher les toutes dernières mises à jour disponibles sur le site de support ([support.dell.com](http://support.dell.com)) pour les plateformes prises en charge en fonction de la marque et le modèle ou du numéro de service. Vous pouvez télécharger les mises à jour ou créer un espace de stockage à partir des résultats de la recherche. Pour en savoir plus sur l'utilisation du DRM pour rechercher les dernières mises à jour du micrologiciel, voir [http://en.community.dell.com/TECHCENTER/EXTRAS/M/WHITE\\_PAPERS/20438118/DOWNLOAD](http://en.community.dell.com/TECHCENTER/EXTRAS/M/WHITE_PAPERS/20438118/DOWNLOAD) sur le Dell Tech Center. Pour en savoir plus sur l'enregistrement du fichier d'inventaire que le DRM utilise comme entrée pour créer les référentiels, voir la section [Enregistrement du rapport d'inventaire du châssis à l'aide de l'interface Web du 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 fournies dans un répertoire. Cela évite d'avoir à télécharger individuellement le micrologiciel de chaque composant.
- Méthode plus rapide et cohérente de mise à jour des composants du serveur.
- Permet de maintenir une image standard avec les versions de mises à jour requises pour les composants de serveur qui peuvent être utilisés pour mettre à jour plusieurs serveurs en une seule opération.
- Vous pouvez copier les répertoires des mises à jour depuis le DVD de téléchargement Dell Server Update Utility (SUU) ou créer et personnaliser les versions de mise à jour requises dans le Dell Repository Manager (DRM). Vous n'avez pas besoin de la version la plus récente du Dell Repository Manager pour créer ce répertoire. Cependant, la version 1.8 de Dell Repository Manager fournit une option permettant de créer un espace de stockage (répertoire de mises à jour) en fonction de l'inventaire qui a été exporté des serveurs dans le châssis. Pour obtenir des informations sur la création d'un espace de stockage à l'aide du Dell Repository Manager, voir le *Dell Repository Manager Data Center Version 1.8 User's Guide* (Guide d'utilisation du Dell Repository Manager Data Center version 1.8) et le *Dell Repository Manager Business Client Version 1.8 User's Guide* (Guide d'utilisation de Dell Business Client version 1.8) disponible à l'adresse [dell.com/support/manuals](http://dell.com/support/manuals).

Il vous est recommandé de mettre à jour le micrologiciel du CMC avant de mettre à jour les modules de micrologiciel des composants de serveur. Après la mise à jour du micrologiciel du CMC, dans l'interface Web du CMC, vous pouvez mettre à jour le micrologiciel du composant de serveur à la page **Présentation du châssis** → **Présentation du serveur** → **Mise à jour** → **Mise à jour du composant de serveur**. Il vous est également recommandé de sélectionner ensemble tous les modules des composants d'un serveur devant être mis à jour. Ceci permet au Lifecycle Controller d'utiliser ses algorithmes optimisés pour mettre à jour le micrologiciel, ce qui permet de réduire le nombre de redémarrages.

Pour mettre à jour le micrologiciel des composants des serveurs, 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 **Inventaire des micrologiciels des composants/périphériques** affiche la mention **Non pris en charge**. Pour les serveurs de 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 d'ancienne génération, cette mise à niveau n'est pas toujours possible.

Normalement, le micrologiciel Lifecycle Controller est installé à l'aide d'un progiciel d'installation dédié exécuté dans le système d'exploitation du serveur. Pour les serveurs pris en charge, un progiciel de réparation ou d'installation particulier est disponible ; il porte l'extension de fichier **.usc**. Il permet d'installer le micrologiciel Lifecycle Controller via l'utilitaire de mise à jour du micrologiciel disponible dans l'interface de navigateur Web iDRAC native.

Vous pouvez également installer le micrologiciel Lifecycle Controller à l'aide du progiciel d'installation approprié, exécuté dans le système d'exploitation du serveur. Pour plus d'informations, voir le manuel « *Dell Lifecycle Controller User's Guide* » (Guide d'utilisation de 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](http://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 dans l'interface Web CMC

Pour afficher l'inventaire des micrologiciels :

1. Dans le volet de gauche, cliquez sur **Présentation du serveur** et sur **Mettre à jour**.
2. Sur la page **Mise à jour des composants du serveur**, consultez les informations d'inventaire des micrologiciels dans la section **Inventaires des micrologiciels des composants/périphériques**. Cette page contient les informations suivantes :
  - 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 :

1. Dans la console d'amorçage, appuyez sur <F2> pour accéder à la **Configuration du système**.
  2. 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 3. Informations sur les composants et périphériques**

| Champ                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Logement                      | <p>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 :</p> <ul style="list-style-type: none"><li>• 1, 1a, 1b, 1c, 1d</li><li>• 2, 2a, 2b, 2c, 2d</li><li>• 3, 3a, 3b, 3c, 3d</li><li>• 4, 4a 4b, 4c, 4d,</li></ul> <p>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.</p>                                                             |
| Nom                           | Affiche le nom du serveur dans chaque logement.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Modèle                        | Affiche le modèle du serveur.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Composant/<br>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<br>actuelle           | Affiche la version actuelle du composant ou du périphérique sur le serveur.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Version de la<br>restauration | Affiche la version de restauration du composant ou du périphérique sur le serveur.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Condition de<br>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](http://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** : L'application Dell Repository Manager utilise le fichier *Inventory.xml* comme des entrée pour créer un espace de stockage de mises à jour pour toutes les lames disponibles dans le châssis. Cet espace de stockage peut être exporté ultérieurement vers un partage réseau. Le mode **Mise à jour depuis le partage réseau** de la mise à jour du micrologiciel utilise ce partage réseau pour mettre à jour les composants de tous les serveurs. CSIOR doit être activé sur les serveurs individuels et vous devez enregistrer le rapport d'inventaire du châssis à chaque fois qu'une modification est apportée à la configuration matérielle et logicielle du châssis.

## Configuration du Partage réseau via l'interface Web du CMC


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

1. Dans l'interface Web du CMC, ouvrez l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **Partage réseau**.

La section **Modifier le partage réseau** s'affiche.

2. Dans la section **Modifier le partage réseau**, configurez les paramètres suivants au besoin :

- 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 le **Répertoire de tests** 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 **Retour** pour revenir à la page **Mise à jour des composants du serveur**.

## Opérations de tâche Lifecycle Controller

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

Vous pouvez réaliser les opérations Lifecycle Controller suivantes :

- Réinstallation

- Restauration
- Mettre à jour
- Suppression de tâches

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

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

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

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

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

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

### **Réinstallation du micrologiciel des composants des serveurs**

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


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

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

1. Dans le volet de gauche, cliquez sur **Présentation du serveur** → **Mettre à jour**.
2. 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 souhaitez 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'hypothèse 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 d'un fichier utilisant l'interface Web du CMC

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


1. Dans l'interface Web du CMC, ouvrez l'arborescence système, accédez à **Présentation du serveur**, puis cliquez sur **Mise à jour** → **Mise à jour des composants de serveur**.  
La page **Mise à jour des composants de serveur** s'affiche.
2. Dans la section **Choisir le type de mise à jour**, sélectionnez **Mettre à jour depuis 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 en 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 un espace de stockage personnalisé pour vos systèmes connectés à l'aide du Dell Repository Manager et du fichier d'inventaire du châssis exporté à l'aide de l'interface Web du CMC. DRM vous permet de créer un espace de stockage personnalisé qui inclut uniquement les progiciels de mise à jour pour la configuration spécifique du système. Vous pouvez également créer des espaces de stockage contenant des mises à jour uniquement pour les périphériques qui ne sont pas à jour, ou un espace de stockage de ligne de base 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 l'espace de stockage vers un partage CIFS ou NFS. L'interface Web du CMC vous permet de configurer les références et les détails de l'emplacement du partage. À l'aide de l'interface Web du CMC, vous pouvez ensuite effectuer la mise à jour des composants du serveur pour un seul serveur ou plusieurs serveurs.

## Conditions requises pour l'utilisation du mode de mise à jour de partage réseau

Les conditions requises suivantes sont requises pour mettre à jour le micrologiciel des composants du serveur à l'aide du mode 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 version ultérieure doit être installé sur votre système.
- Vous devez détenir des privilèges d'administrateur CMC.

## Mise à niveau du micrologiciel 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 micrologiciel 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 du partage réseau**. Pour en savoir plus, reportez-vous à la section Sélection du type de mise à jour des composants du serveur
3. Si le Partage réseau n'est pas connecté, configurez le Partage réseau pour le châssis. Pour configurer ou modifier les détails du partage réseau, dans le tableau Propriétés du partage réseau cliquez sur **Modifier**. Pour en savoir plus, voir la section Configuration du partage réseau via l'interface Web du CMC.
4. Cliquez sur l'option **Enregistrer le rapport d'inventaire** pour exporter le fichier d'inventaire du châssis qui contient les informations sur les composants et le micrologiciel.

Le fichier *Inventory.xml* est enregistré sur un système externe. Le Dell Repository Manager utilise le fichier *inventory.xml* pour créer des groupes personnalisés de mises à jour. Cet inventaire est stocké


dans le partage CIFS ou NFS configurée par le CMC. Pour en savoir plus sur la création d'un espace de stockage à l'aide du *Dell Repository Manager*, voir le *Dell Repository Manager Data Center Version 1.8 User's Guide* (Guide d'utilisation du Centre de données Dell Repository Manager version 1.8) et le *Dell Repository Manager Business Client Version 1.8 User's Guide* (Guide d'utilisation du Client commercial Dell Repository Manager version 1.8) disponible à l'adresse **dell.com/support/manuals**.

5. Cliquez sur l'option **Rechercher les mises à jour** pour afficher les mises à jour du micrologiciel disponibles dans le partage réseau.


La section **Inventaire du micrologiciel des composants/périphériques** affiche les versions actuelles du micrologiciel des composants et périphériques répartis sur tous les serveurs présents dans le châssis et les versions du micrologiciel des progiciels DUP disponibles dans le Partage réseau.

 **REMARQUE** : Cliquez sur **Réduire** en regard d'un emplacement pour réduire les détails sur les composants ou périphériques de l'emplacement spécifique. Vous pouvez également afficher tous les détails à nouveau en cliquant sur **Développer**.

6. Dans la section **Inventaire du micrologiciel des composants/périphériques**, sélectionnez la case à cocher **Sélectionner/Désélectionner tout** pour sélectionner tous les serveurs pris en charge. Vous pouvez également sélectionner la case du serveur pour lequel vous souhaitez mettre à jour le micrologiciel des composants de 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 micrologiciel 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 micrologiciel pour les serveurs sélectionnés.

 **REMARQUE** : La colonne d'État des tâches affiche l'état de la tâche des opérations planifiées sur le serveur. L'état de la tâche est mis à jour de façon 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).

# 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

## Affichage des récapitulatifs de châssis et de composants

Lorsque vous vous connectez à l'interface Web CMC, la page **Intégrité du châssis** affiche l'intégrité du châssis et de ses composants. Elle contient une vue graphique du châssis et de ses composants. Elle est mise à jour dynamiquement et les sous-graphiques des composants, ainsi que les info-bulles texte, sont automatiquement mis à jour 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 et des périphériques PCIe. Des informations détaillées sur chaque composant s'affichent lorsque vous cliquez sur le composant. En outre, les derniers événements consignés dans le journal du matériel CMC s'affichent. Pour en savoir plus, voir l'*Aide en ligne de Dell 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 arrière. 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 : contient des liens permettant de naviguer vers les pages les plus fréquemment consultées, ainsi que vers les actions les plus souvent exécutées. Seuls les liens applicables au composant sélectionné s'affichent dans cette section.

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

| Composant                                     | Propriétés des performances et de l'intégrité                                                                                                                                             | Propriétés                                                                                                                                                                                                                                                       | Liens rapides                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CMC                                           | <ul style="list-style-type: none"> <li>• Adresse MAC</li> <li>• IPv4</li> <li>• IPv6</li> </ul>                                                                                           | <ul style="list-style-type: none"> <li>• Micrologiciel</li> <li>• Micrologiciel auxiliaire</li> <li>• Dernière mise à jour</li> <li>• Matériel</li> </ul>                                                                                                        | <ul style="list-style-type: none"> <li>• Condition du CMC</li> <li>• Mise en réseau</li> <li>• Mise à jour du micrologiciel</li> </ul>                                                                                                                                                                                                                           |
| Tous les serveurs et les serveurs individuels | <ul style="list-style-type: none"> <li>• État de l'alimentation</li> <li>• Consommation électrique</li> <li>• Intégrité</li> <li>• Alimentation allouée</li> <li>• Température</li> </ul> | <ul style="list-style-type: none"> <li>• Nom</li> <li>• Modèle</li> <li>• Numéro de service</li> <li>• Nom d'hôte</li> <li>• iDRAC</li> <li>• CPLD</li> <li>• BIOS</li> <li>• SE</li> <li>• Informations sur l'UC</li> <li>• Total de mémoire système</li> </ul> | <ul style="list-style-type: none"> <li>• Condition du serveur</li> <li>• Lancer la console distante</li> <li>• Lancer l'interface utilisateur d'iDRAC</li> <li>• Mettre le serveur hors tension</li> <li>• Arrêt normal</li> <li>• Partage de fichier à distance</li> <li>• Déployer le réseau iDRAC</li> <li>• Mise à jour des composants de serveur</li> </ul> |

| Composant                     | Propriétés des performances et de l'intégrité                                                                                       | Propriétés                                                                                                                                                                                                                                                   | Liens rapides                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                               |                                                                                                                                     |                                                                                                                                                                                                                                                              |  <b>REMARQUE</b> : Les liens rapides des fonctions Mettre le serveur hors tension et Arrêt normal s'affichent uniquement si l'état de l'Alimentation du serveur est Sous tension. Lorsque l'état de l'Alimentation du serveur est Hors tension, le lien rapide de la fonction Mettre le serveur sous tension s'affiche à la place. |
| Unités de bloc d'alimentation | État de l'alimentation                                                                                                              | Capacité                                                                                                                                                                                                                                                     | <ul style="list-style-type: none"> <li>• Condition des blocs d'alimentation</li> <li>• Consommation énergétique</li> <li>• Bilan de puissance du système</li> </ul>                                                                                                                                                                                                                                                   |
| Périphériques PCIe            | <ul style="list-style-type: none"> <li>• Installé</li> <li>• Attribué</li> </ul>                                                    | <ul style="list-style-type: none"> <li>• Modèle</li> <li>• Adressage</li> <li>• Numéro/ID fournisseur)</li> <li>• ID de périphérique</li> <li>• Type de logement</li> <li>• Type de module</li> <li>• Structure</li> <li>• État de l'alimentation</li> </ul> | <ul style="list-style-type: none"> <li>• État PCIe</li> <li>• Configuration du PCIe</li> </ul>                                                                                                                                                                                                                                                                                                                        |
| Ventilateurs                  | <ul style="list-style-type: none"> <li>• Vitesse</li> <li>• PWM (% de la valeur max.)</li> <li>• Décalage de ventilateur</li> </ul> | <ul style="list-style-type: none"> <li>• Seuil d'avertissement</li> <li>• Seuil critique</li> </ul>                                                                                                                                                          | <ul style="list-style-type: none"> <li>• Condition des ventilateurs</li> <li>• Configuration de ventilateur</li> </ul>                                                                                                                                                                                                                                                                                                |
| Logement IOM                  | <ul style="list-style-type: none"> <li>• État de l'alimentation</li> <li>• Rôle</li> </ul>                                          | <ul style="list-style-type: none"> <li>• Modèle</li> <li>• Numéro de service</li> </ul>                                                                                                                                                                      | 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 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 du module IOM

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


1. Cliquez sur **Présentation du châssis**.  
La page **Intégrité du châssis** s'affiche. Le graphique dans le volet de gauche affiche les vues arrière, avant et 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*.

## 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>]
```

 **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`.

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](http://dell.com/support/manuals).

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

**Compensation du ventilateur** : cette fonction permet d'augmenter la distribution d'air aux logements de carte PCIe. Cette fonction est plus particulièrement utile lorsque vous utilisez des cartes PCIe haute puissance ou personnalisées exigeant plus de refroidissement que la normale. La fonction de compensation de ventilation comporte les paramètres suivants : Désactivé, Faible, Moyen et Élevé. Ces paramètres correspondent à un décalage de vitesse de ventilateur (augmentation) de 20 %, 50 % et 100 % de la vitesse maximale. Il existe également des vitesses minimales pour chaque option de configuration, lesquelles sont 35 % pour Faible, 65 % pour Moyen et 100 % pour Élevé.

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

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

Pour définir la fonction de compensation, accédez à **Présentation du châssis** → **Ventilateurs** → **Configurer**. Dans la page **Configuration de ventilation avancée**, dans le menu déroulant **Valeur** correspondant à **Compensation de ventilation**, sélectionnez la valeur appropriée.

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

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

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

## 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.

## 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 contrôleur 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.

 **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)

## 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 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 du CMC, l'opération de désactivation effectue les actions suivantes :

- Désactive l'accès de l'interface réseau à la gestion du châssis hors bande, y compris la gestion d'iDRAC et des modules d'E/S (IOM).
- Empêche la détection de l'état de liaison descendante.

Pour désactiver l'accès réseau de CMC, désactivez les adresses IPv4 et IPv6 du CMC.

### 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 DHCP et utiliser le serveur DHCP sur le réseau afin d'attribuer une adresse IPv4, un masque de sous-réseau et une passerelle à l'iDRAC ou au CMC, tapez :

```
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>
```

## 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 du DNS

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

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

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


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


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

## 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 dans l'interface Web CMC

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

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

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

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

- `getniccfg`
- `getconfig`

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

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

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

## Configuration des paramètres DNS (IPv4 et IPv6)

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

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

  - **REMARQUE** : Certains serveurs DNS n'enregistrent que les noms comportant 31 caractères ou moins. Assurez-vous que le nom désigné se trouve dans la limite requise par le DNS.
  - **REMARQUE** : les paramètres suivants ne sont valides que si vous avez enregistré CMC sur le serveur DNS en définissant la variable `cfgDNSRegisterRac` sur la valeur 1.
- **Nom CMC** : par défaut, le nom CMC sur le serveur DNS est `cmc-<numéro de service>`. Pour modifier le nom CMC sur le serveur DNS, entrez :  

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

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

  - **REMARQUE** : Si un nom de domaine DNS n'est pas spécifié, le nombre maximum de caractères est 63. Si un nom de domaine est spécifié, le nombre de caractères dans le nom CMC ainsi que 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 espace. Pour définir un nom de domaine DNS, entrez :  

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

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

## Configuration de la négociation automatique, du mode duplex et de la vitesse réseau (IPv4 et IPv6)

Lorsqu'elle est activée, la fonction de 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. La négociation automatique est activée par défaut.

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

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

où :

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

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


où :


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

## Configuration 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 du 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.

## 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.

## Configuration des services à l'aide de l'interface RACADM

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

- `cfgRacTuning`
- `cfgRacTuneRemoteRacadmEnable`

Pour plus d'informations sur ces objets, voir le *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](http://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 # cfgSsnMgtSSTimeout=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 maître.

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 huit membre, exécutez les tâches des étapes 4 à 8. Les noms de châssis des nouveaux membres apparaissent dans la boîte de dialogue **Membres**.

 **REMARQUE** : Les références entrées pour un membre sont transmises en mode sécurisé au châssis membre afin d'établir une relation de confiance entre les châssis membres et le châssis maître. Les références ne sont pas conservées dans chaque châssis et ne sont plus jamais échangées après l'établissement de la relation de confiance.

## Retrait d'un membre du châssis maître

Vous pouvez supprimer un membre de groupe à partir du châssis maître. Pour supprimer un membre :

1. Connectez-vous au châssis maître en utilisant les privilèges d'administrateur.
2. Dans le volet de gauche, sélectionnez le châssis maître.
3. Cliquez sur **Configuration** → **Administration des groupes**.
4. Dans la liste **Suppression de membres**, sélectionnez le nom du membre à supprimer, puis cliquez sur **Appliquer**.

Le châssis maître communique avec le ou les membres, si vous en avez sélectionné plusieurs, supprimés du groupe. Le nom de membre est supprimé. Les châssis membres ne reçoivent pas le message si un problème réseau empêche le châssis maître de contacter les membres. Dans ce cas, désactivez le membre à partir du châssis membre pour achever la suppression.

## Dissolution d'un groupe de châssis

Pour dissoudre un groupe de châssis depuis le châssis maître :

1. Connectez-vous au châssis maître avec les privilèges d'Administrateur.
2. Sélectionnez le châssis maître dans le volet de gauche.
3. Cliquez sur **Configuration** → **Administration des groupes**.
4. Dans la page **Groupe du châssis**, sous **Rôle**, sélectionnez **Aucun**, puis cliquez sur **Appliquer**.  
Le châssis maître indique alors à tous les membres qu'ils ont tous été supprimés du groupe. Le châssis maître peut être défini comme maître ou membre d'un nouveau groupe.

Si un problème de réseau empêche le contact entre le maître et le membre, le châssis membre peut ne pas recevoir les 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 sur **Présentation du châssis** → **Configuration** → **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 d'un châssis membre, la console distante du serveur ou la page Web du serveur iDRAC depuis la page du groupe du châssis maître. Si le périphérique membre a les mêmes références de connexion que le châssis maître, vous pouvez utiliser les mêmes références pour accéder au périphérique membre.

 **REMARQUE** : L'Ouverture de session unique et l'ouverture de session par carte à puce ne sont pas prises en charge dans la Gestion de plusieurs châssis. Le lancement de membres par l'authentification unique à partir d'un châssis maître requiert un nom d'utilisateur/mot de passe entre le maître et les membres. L'utilisation d'un nom d'utilisateur/mot de passe courant fonctionne uniquement avec les utilisateurs Active Directory, locaux et LDAP.

Pour naviguer vers les périphériques membres :

1. Connectez-vous au châssis maître.
2. Sélectionnez **Groupe : nom** dans l'arborescence.
3. Si un CMC membre correspond à la destination requise, sélectionnez **Lancer CMC** en regard du châssis requis.

Si l'un des serveurs d'un châssis correspond à la destination requise :

- a. Sélectionnez l'image du châssis de destination.
- b. Dans l'image du châssis qui s'affiche dans la section **Intégrité**, sélectionnez le serveur.
- c. Dans la zone **Liens rapides**, sélectionnez le périphérique de destination. La nouvelle fenêtre qui s'ouvre affiche la page de destination ou l'écran de connexion.

## 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 des propriétés d'un nouveau membre avec celles 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 4. Propriétés du service de configuration

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

## 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 de l'inventaire des serveurs


Pour enregistrer le rapport d'inventaire des serveurs en utilisant l'interface Web CMC :

1. Dans le volet de gauche, sélectionnez **Groupe**.
2. Sur la page **Intégrité du groupe de châssis**, cliquez sur **Enregistrer le rapport d'inventaire**. La boîte de dialogue **Téléchargement de fichier** qui s'affiche vous invite à ouvrir ou enregistrer le fichier.
3. Cliquez sur **Enregistrer** et spécifiez le chemin et le nom du fichier de rapport d'inventaire des modules serveur.


 **REMARQUE** : Le maître du groupe de châssis, les châssis membres du groupe de châssis et le module serveur dans le châssis associé doivent être sous tension pour pouvoir obtenir le rapport d'inventaire de module serveur le plus précis.

## 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 à la colonne 1. Tout caractère « # » dans une autre colonne est traité comme tel.

Certains paramètres de modem peuvent inclure le caractère # dans leur chaîne. Aucun caractère d'échappement n'est nécessaire. Vous pouvez être amené à générer un fichier **.cfg** à partir de la commande `racadm getconfig -f <filename> .cfg`, puis à exécuter la commande `racadm config -f <filename> .cfg` sur un autre CMC, sans ajouter de caractère 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 signale un nom de groupe doit se trouver dans la colonne 1. Vous devez spécifier le nom du groupe avant celui des objets de ce groupe. Les objets qui n'incluent aucun nom de groupe associé génèrent une erreur. Les données de configuration sont organisées en groupes, comme l'indique le chapitre traitant des propriétés de base de données dans le manuel « RACADM

*Command Line Reference Guide for iDRAC and CMC* » (Guide de référence de l'interface de 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 sous la forme de paires « objet=valeur » sans aucun espace entre les trois éléments (objet, signe = et valeur). Les espaces figurant après la valeur sont ignorés. Un espace dans une chaîne de valeur reste inchangé. Tout caractère à droite du signe égal (=), notamment un autre signe égal (=), un signe dièse (#), des crochets ([ ]), etc., est considéré comme du texte. Ces caractères sont des caractères de script de discussion (chat) par modem valides.

```
[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 du fichier **.cfg**. Si vous supprimez cette ligne dans un éditeur de texte, RACADM s'arrête pendant l'analyse du fichier de configuration et vous avertit de 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 d'ancrage (anchor) doit être le premier objet après la paire « [ ] ». Voici des exemples des groupes indexés actuels :

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

- Lorsque vous utilisez l'interface RACADM distant 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 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 entrer manuellement les propriétés manquantes dans le fichier de configuration après avoir exécuté la commande `getconfig -f`. Cela s'applique à tous les groupes indexés par RACADM.

La liste suivante répertorie les groupes indexés qui présentent ce comportement ainsi que leurs propriétés de clé correspondantes :

- `cfgUserAdmin` — `cfgUserAdminUserName`
- `cfgEmailAlert` — `cfgEmailAlertAddress`
- `cfgTraps` — `cfgTrapsAlertDestIPAddr`
- `cfgStandardSchema` — `cfgSSADRoleGroupName`

– cfgServerInfo – cfgServerBmcMacAddress

## Modification de l'adresse IP CMC

Lorsque vous modifiez l'adresse IP CMC dans le fichier de configuration, supprimez toutes les entrées `<variable>=<value>` inutiles. Seule l'étiquette contenant « [ » et « ] » du groupe de variables réel est conservée, y compris les deux entrées `<variable>=<value>` qui concernent le changement d'adresse IP.

Exemple :

```
Object Group "cfgLanNetworking" # [cfgLanNetworking]
cfgNicIpAddress=10.35.10.110 cfgNicGateway=10.35.10.1
```

Ce fichier est mis à jour comme suit :

```
Object Group "cfgLanNetworking" # [cfgLanNetworking]
cfgNicIpAddress=10.35.9.143 # commentaire, le reste de cette ligne est ignoré
cfgNicGateway=10.35.9.1
```

La commande `racadm config -f <myfile>.cfg` analyse le fichier et identifie les erreurs par leur 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 vérifier la mise à jour.

Utilisez ce fichier pour télécharger des modifications à l'échelle de l'entreprise ou pour configurer de nouveaux systèmes sur le réseau à l'aide de la commande `racadm getconfig -f <myfile>.cfg`.

 **REMARQUE** : « *Anchor* » est un mot réservé qui ne doit pas être utilisé dans le fichier `.cfg`.

# Configuration 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

## Définition 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). Les caractères standard et spéciaux sont également 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- (Commutateur-)
  - Fan- (Ventilateur-)
  - PS-
  - DRAC-
  - MC-
  - Châssis
  - Housing-Left (Boîtier-Gauche)
  - Housing-Right (Boîtier-Droite)
  - Housing-Center (Boîtier-Centre)
- 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** → **Configurer** → **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 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 iDRAC

Pour utiliser cette fonction, vous devez disposer d'une licence d'entreprise. Vous pouvez définir la 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](http://dell.com/support/manuals).

## Configuration des paramètres réseau QuickDeploy (Déploiement rapide) 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** → **Configurer** → **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 5. Paramètres de QuickDeploy

| Paramètre                       | Description                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Action à l'insertion du serveur | Sélectionnez l'une des options suivantes dans la liste : <ul style="list-style-type: none"><li>• <b>Aucune action</b> : aucune action n'est effectuée lors de l'insertion du serveur.</li><li>• <b>QuickDeploy uniquement</b> : sélectionnez cette option pour appliquer les paramètres réseau de l'iDRAC lorsqu'un nouveau serveur</li></ul> |

| Paramètre                                                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                            | <p>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 <b>Modifier le mot de passe Root</b> est sélectionnée.</p> <ul style="list-style-type: none"> <li>• <b>Profil de serveur uniquement</b> : sélectionnez cette option pour appliquer un profil de serveur attribué lorsqu'un nouveau serveur est inséré dans le châssis.</li> <li>• <b>Déploiement rapide et profil de serveur</b> : 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.</li> </ul> |
| <b>Définir le mot de passe Root d'iDRAC lors de l'insertion du serveur</b> | Sélectionnez l'option de changement du mot de passe root iDRAC pour qu'il corresponde au mot de passe du champ <b>Mot de passe root iDRAC</b> lorsqu'un serveur est inséré.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Mot de passe Root d'iDRAC</b>                                           | Si vous sélectionnez les options <b>Définir le mot de passe root iDRAC lors de l'insertion du serveur</b> et <b>QuickDeploy activé</b> , 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).                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Confirmez le mot de passe Root d'iDRAC</b>                              | Permet d'entrer de nouveau le mot de passe fourni dans le champ <b>Mot de passe</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Activer le LAN pour iDRAC</b>                                           | Permet d'activer ou de désactiver le canal LAN iDRAC. Par défaut, cette option est désactivée.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Activer IPv4 pour iDRAC</b>                                             | Permet d'activer ou de désactiver IPv4 sur iDRAC. Par défaut, cette option est sélectionnée.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Activer IPMI sur le LAN pour iDRAC</b>                                  | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Activer le protocole DHCP IPv4 pour iDRAC</b>                           | Permet d'activer ou de désactiver DHCP pour chaque iDRAC présent dans le châssis. Si vous activez cette option, les champs <b>Adresse IP QuickDeploy</b> , <b>Masque de sous-réseau QuickDeploy</b> et <b>Passerelle QuickDeploy</b> 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 <b>Activer IPv4 pour iDRAC</b> .                                                                                                                                                                                                                               |


| Paramètre                                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                          | L'option Adresse IP Quick Deploy est fournie avec les valeurs 4 et 2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Adresse IP QuickDeploy réservée</b>                   | Sélectionnez le nombre d'adresses IPv4 statiques réservées aux iDRAC dans le châssis. Les adresses IPv4 commençant à partir de l' <b>adresses IPv4 de l'iDRAC de départ (Logement 1)</b> 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Première adresse IPv4 d'iDRAC (logement 1)</b>        | 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.<br><br> <b>REMARQUE</b> : Le masque de sous-réseau et la passerelle ne sont pas incrémentés comme l'adresse IP.<br><br>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 <b>Enregistrer les paramètres QuickDeploy</b> ou <b>Remplir automatiquement avec les paramètres QuickDeploy</b> . |
| <b>Masque de réseau IPv4 d'iDRAC</b>                     | Spécifie le masque de sous-réseau QuickDeploy assigné à tout serveur nouvellement inséré.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Passerelle IPv4 d'iDRAC</b>                           | Définit la passerelle par défaut QuickDeploy affectée à l'ensemble du module DRAC présent dans le châssis.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Activer IPv6 pour iDRAC</b>                           | Active l'adressage IPv6 pour chaque contrôleur iDRAC présent dans le châssis prenant en charge IPv6.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Activer la configuration automatique IPv6 d'iDRAC</b> | Permet à l'iDRAC d'obtenir les paramètres IPv6 (adresse et longueur de préfixe) auprès d'un                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| Paramètre                               | Description                                                                                                                     |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
|                                         | serveur DHCPv6 et autorise également la configuration automatique des adresses sans état. Par défaut, cette option est activée. |
| <b>Passerelle IPv6 d'iDRAC</b>          | Spécifie la passerelle IPv6 à attribuer aux iDRAC. La valeur par défaut est « :: ».                                             |
| <b>Longueur du préfixe IPv6 d'iDRAC</b> | Spécifie la longueur de préfixe à attribuer pour les adresses IPv6 de l'iDRAC. La valeur par défaut est 64.                     |

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 pour les 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 :

|                      |
|----------------------|
| START IP + 0 (SLOT1) |
| START IP + 2 (SLOT3) |

- Quatre chariots demi-largeur dans le châssis :

 **REMARQUE** : Pour que la fonction QuickDeploy attribue des adresses IP au chariot du bas, le champ **Adresses IP QuickDeploy réservées** doit être défini sur 4 pour l'iDRAC du chariot du bas.

|                      |                      |
|----------------------|----------------------|
| START IP + 0 (SLOT1) | START IP + 1 (SLOT2) |
| START IP + 2 (SLOT3) | START IP + 3 (SLOT4) |

- Huit chariots quart de largeur dans le châssis :

|                       |                       |                       |                       |
|-----------------------|-----------------------|-----------------------|-----------------------|
| START IP + 0 (SLOT1a) | START IP + 4 (SLOT1b) | START IP + 1 (SLOT1c) | START IP + 5 (SLOT1d) |
| START IP + 2 (SLOT3a) | START IP + 6 (SLOT3b) | START IP + 3 (SLOT3c) | START IP + 7 (SLOT3d) |

- Quatre chariots FM120x4 dans le châssis :

|                       |                       |                        |                        |                       |                       |                        |                        |
|-----------------------|-----------------------|------------------------|------------------------|-----------------------|-----------------------|------------------------|------------------------|
| STARTIP+0<br>(SLOT1a) | STARTIP+4<br>(SLOT1b) | STARTIP+8<br>(SLOT1c)  | STARTIP+12<br>(SLOT1d) | STARTIP+1<br>(SLOT2a) | STARTIP+5<br>(SLOT2b) | STARTIP+9<br>(SLOT2c)  | STARTIP+13<br>(SLOT2d) |
| STARTIP+2<br>(SLOT3a) | STARTIP+6<br>(SLOT3b) | STARTIP+10<br>(SLOT3c) | STARTIP+14<br>(SLOT3d) | STARTIP+3<br>(SLOT4a) | STARTIP+7<br>(SLOT4b) | STARTIP+11<br>(SLOT4c) | STARTIP+15<br>(SLOT4d) |

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

|                       |                      |                      |                      |
|-----------------------|----------------------|----------------------|----------------------|
| START IP + 0 (SLOT1a) | START IP + 4(SLOT1b) | START IP + 1(SLOT1c) | START IP + 5(SLOT1d) |
| START IP + 2 (SLOT3)  |                      | START IP + 3 (SLOT4) |                      |

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

|                      |  |                      |  |
|----------------------|--|----------------------|--|
| START IP + 0 (SLOT1) |  |                      |  |
| START IP+ 2 (SLOT3)  |  | START IP + 3 (SLOT4) |  |

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


|                       |                     |                     |                     |
|-----------------------|---------------------|---------------------|---------------------|
| START IP + 0 (SLOT1)  |                     |                     |                     |
| START IP + 2 (SLOT3a) | STARTIP+ 6 (SLOT3b) | STARTIP + 3(SLOT3c) | STARTIP + 7(SLOT3d) |

## 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 :

- 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.
- 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*.

- 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 avec RACADM

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

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

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

## Configuration des paramètres de marquage VLAN iDRAC

Les VLAN servent à autoriser plusieurs réseaux LAN virtuels à coexister sur le même câble réseau physique et à séparer le trafic réseau pour des raisons de sécurité ou de gestion de la charge de traitement. Lorsque vous activez la fonction VLAN, chaque paquet réseau reçoit un marquage VLAN. Ce marquage correspond à des propriétés de châssis. Il demeure associé au châssis même si un composant est retiré.

### 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 entre 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 6. 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 dans l'interface Web CMC

 **REMARQUE** : Pour définir le premier périphérique d'amorçage des serveurs, vous devez disposer des privilèges **Administrateur de serveur** ou **Administrateur de configuration du châssis**, ainsi que les privilèges **Connexion à l'iDRAC**.

Pour définir le premier périphérique d'amorçage de plusieurs serveurs :

1. Dans le volet de gauche, cliquez sur **Présentation du serveur** → **Configurer** → **Premier périphérique d'amorçage**. La liste des serveurs s'affiche.
2. Dans la colonne **Premier périphérique d'amorçage**, dans le menu déroulant d'un serveur, sélectionnez le périphérique d'amorçage à utiliser pour le serveur.
3. Si vous souhaitez que le serveur s'amorce sur le périphérique sélectionné à chaque amorçage, désélectionnez l'option **Démarrer une seule fois** pour le serveur. Pour que le serveur s'amorce sur le périphérique sélectionné uniquement pour le prochain cycle d'amorçage, sélectionnez l'option **Démarrer une seule fois** pour le serveur concerné.
4. Cliquez sur **Appliquer** pour enregistrer les paramètres.

## Définition du premier périphérique d'amorçage pour un seul serveur dans l'interface Web CMC

 **REMARQUE** : Pour définir le premier périphérique d'amorçage pour les serveurs, vous devez posséder les privilèges **Administrateur du serveur** ou **Administrateur de configuration du châssis**, ainsi que les privilèges **Connexion à l'iDRAC**.

Pour définir le premier périphérique d'amorçage de chaque serveur :

1. Dans le volet de gauche, cliquez sur **Présentation du serveur** et sur le serveur dont vous voulez définir le premier périphérique d'amorçage.
2. Accédez à **Configuration** → **Périphérique de démarrage initial**. La page **Premier périphérique de démarrage** s'affiche.
3. Dans le menu déroulant **Périphérique de démarrage initial**, sélectionnez le périphérique d'amorçage à utiliser pour chaque serveur.
4. Si vous souhaitez que le serveur s'amorce sur le périphérique sélectionné à chaque amorçage, désélectionnez l'option **Démarrer une seule fois** pour le serveur. Pour que le serveur s'amorce sur le périphérique sélectionné uniquement pour le prochain cycle d'amorçage, sélectionnez l'option **Démarrer une seule fois** pour le serveur concerné.
5. Cliquez sur **Appliquer** pour enregistrer les paramètres.

## Définition du premier périphérique de démarrage à l'aide de l'interface RACADM

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

Pour activer un seul démarrage pour un périphérique, utilisez l'objet `cfgServerBootOnce`.

Pour en savoir plus sur ces objets, voir le document *Chassis Management Controller for PowerEdge FX2s RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge FX2s) accessible sur le site [dell.com/support/manuals](http://dell.com/support/manuals).

## Configuration de liaison montante de réseau de chariot

Vous pouvez configurer la liaison montante de réseau de chariot uniquement sur les chariots PowerEdge FM120x4 qui contiennent un commutateur de réseau interne.

Pour configurer la liaison montante de réseau de chariot, accédez à **Présentation du châssis** → **Présentation du serveur** → **Configuration** → **Liaison montante de réseau de chariot**

Sélectionnez l'une des valeurs suivantes pour la propriété de configuration de liaison montante de réseau de chariot :

- **Standard (regroupé)** : la configuration de liaison montante où quatre ports de liaison montante 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 liaison montante semblable à la configuration standard, mais l'acheminement entre les nœuds locaux n'est pas autorisée.
- **Réseaux isolés** : configuration de liaison montante où le LOM1 de chaque nœud est adressé au Module d'E/S A1 et le LOM2 est adressé au module d'E/S A2.

## Déploiement d'un partage de fichier à distance

La fonction de partage de fichiers sur support virtuel distant associe un fichier d'un lecteur de partage du réseau à un ou plusieurs serveurs via le contrôleur CMC pour déployer ou 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 supports sont pris en charge : les disquettes et les lecteurs de CD/DVD.

Pour exécuter une opération de partage de fichiers distants (connexion, déconnexion ou déploiement), vous devez disposer des privilèges **Administrateur de configuration de châssis** ou **Administrateur de serveur**. Pour pouvoir utiliser cette fonction, vous devez disposer d'une licence d'entreprise.

Pour configurer le partage de fichier distant :

1. Dans le volet de gauche, cliquez sur **Présentation du serveur** → **Configurer** → **Partage de fichiers distants**.
2. Dans la page **Déployer le partage de fichiers distant**, entrez les données appropriées dans les champs. Pour en savoir plus sur les champs, voir l'*Aide en ligne de CMC pour Dell PowerEdge FX2/FX2s*.
3. Pour vous connecter à un partage de fichiers distant, cliquez sur **Connecter**. Pour cette connexion, vous devez indiquer le chemin, le nom d'utilisateur et le mot de passe. Si l'opération réussit, vous pouvez accéder au support.

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 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 réplique 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 une station de gestion ou un partage de fichiers distant.
- Modifier le nom du profil et sa description.
- Exporter les profils stockés vers une station 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 cloner 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 sur des serveurs, l'option CSIOR doit être activée sur les serveurs. Si l'option CSIOR est désactivée, un message d'avertissement s'affiche indiquant que CSIOR n'est pas activé sur les serveurs. Pour terminer l'opération de clonage des lames, assurez-vous que l'option CSIOR est activée 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 un profil de serveur qui est stocké sur une station de gestion vers le CMC.

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 **Profil 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, puis la description est perdue. Appuyez sur **OK** pour continuer l'exportation du profil.

Un message s'affiche vous invitant à sélectionner la destination du fichier :

- Partage local ou partage réseau si le fichier source se trouve 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 d'un Partage réseau à l'aide de l'interface Web du CMC](#)

- Carte locale ou carte SD si le fichier source se trouve sur le partage réseau.

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

3. Sélectionnez **Local**, **Stockage étendu** ou **Partage réseau** comme emplacement de destination en fonction des options qui s'affichent.

- Si vous sélectionnez l'option **Local**, la boîte de dialogue qui s'affiche vous permet d'enregistrer le profil dans un répertoire local.
- Si vous sélectionnez **Stockage étendu** ou **Partage réseau**, la boîte de dialogue **Enregistrer le profil** s'affiche.

4. Cliquez sur **Enregistrer le profil** pour enregistrer le profil vers l'emplacement sélectionné.

## 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 **Profil 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 réplification 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 modifications.

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 **Collecter l'inventaire système au redémarrage**.

## Affichage des paramètres de profil stocké

Pour afficher les paramètres des profils de serveur stockés, accédez à la page **Profils de serveur**. Dans la section **Profils 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 réplification de la configuration du serveur, ainsi que la description du message du journal de réplification. 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 *Aide en ligne*.


## Statut d'achèvement et dépannage

Pour vérifier la condition d'achèvement de l'application d'un profil BIOS :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** → **Présentation du serveur** → **Configurer** → **Profils**.
2. Dans la page **Profils de serveur**, notez l'ID de tâche (JID) de la tâche soumise, affiché 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 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](#).

## Profils de déploiement rapide

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** → **Configurer** → **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 QuickDeploy**.

Les attributions de profil actuelles s'affichent pour des logements dans les cases de sélection contenues dans la colonne **Attribuer un profil**.

 **REMARQUE** : Vous pouvez effectuer l'action Quick Deploy uniquement si l'option **Action lorsque le serveur est inséré** dans la page **Déployer iDRAC** est définie sur **Profil de serveur** ou **Quick Deploy puis Profil de 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.


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 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](#)


## Lancement d'iDRAC à l'aide d'une connexion directe (SSO)


Le contrôleur CMC offre des fonctions limitées de gestion des composants de châssis, tels que les serveurs. Pour la gestion complète de ces composants, le contrôleur CMC offre un point de lancement de l'interface Web du contrôleur de gestion (iDRAC) du serveur.

Un utilisateur peut lancer l'interface Web iDRAC sans avoir à se reconnecter, car cette fonctionnalité utilise la connexion directe (SSO). Les règles de connexion directe sont les suivantes :

- Tout utilisateur CMC possédant le privilège Administrateur de serveur est automatiquement connecté à l'iDRAC par connexion directe (SSO). Une fois sur le site de l'iDRAC, cet utilisateur reçoit automatiquement des privilèges Administrateur, même s'il ne possède pas de compte sur l'iDRAC ou si son compte n'a pas de privilèges Administrateur.
- Un utilisateur CMC **SANS** privilège Administrateur de serveur mais possédant le même compte sur l'iDRAC est automatiquement connecté à l'iDRAC par connexion directe. Une fois sur le site de l'iDRAC, cet utilisateur reçoit les privilèges créés pour le compte iDRAC.
- Un utilisateur CMC qui ne possède ni le privilège Administrateur de serveur, ni le même compte sur l'iDRAC n'est **PAS** automatiquement connecté à l'iDRAC par connexion directe (SSO). Cet utilisateur est acheminé vers la page de connexion à l'iDRAC lorsqu'il clique sur l'option **Lancer l'interface utilisateur iDRAC**.

 **REMARQUE :** Dans ce contexte, l'expression « le même compte » signifie que l'utilisateur dispose du même nom de connexion et du même mot de passe pour le CMC et pour l'iDRAC. Un utilisateur qui emploie 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 le serveur est retiré du châssis, que l'adresse IP iDRAC est modifiée ou qu'un problème de connexion survient au niveau du réseau iDRAC, une page d'erreur peut s'afficher lorsque l'utilisateur clique sur l'icône Lancer l'interface utilisateur iDRAC.

## 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 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.

# 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 le CMC afin qu'il envoie des alertes :

1. Activez l'option **Alertes d'événement de châssis**.
2. Vous pouvez également filtrer les alertes en fonction d'une catégorie ou d'un niveau de gravité.
3. Configurez les paramètres d'alerte par e-mail ou par interruption SNMP.
4. Activez les alertes d'événement de châssis pour envoyer une alerte par e-mail ou des interruptions SNMP à des destinations définies.

## 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 l'interface RACADM

Pour activer ou désactiver la génération d'alertes, utilisez l'objet RACADM **cfgIpmiLanAlertEnable**. Pour en savoir plus, 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 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 interruption SNMP

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

#### Configuration des destinations d'alerte pour interruption SNMP à l'aide de l'interface Web CMC

Pour configurer les paramètres de destination d'alerte IPv4 ou IPv6 en utilisant l'interface Web CMC :

1. Dans 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>
```

## Définition 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 des alertes par e-mail à l'aide de l'interface Web CMC

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

1. Dans 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 des alertes par e-mail à l'aide de RACADM

Pour envoyer un e-mail test à une destination d'alerte par e-mail :

1. Ouvrez une console série/Telnet/SSH d'accès à CMC, puis ouvrez une session.
2. Activez la génération d'alertes :

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

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 qui doit recevoir l'alerte par e-mail, et `<index>` est la valeur d'index spécifiée aux étapes 4 et 5. Le nom du destinataire d'e-mail peut contenir jusqu'à 32 caractères alphanumériques, tirets, caractères de soulignement et points. Les espaces ne sont pas valides.

6. Configurez l'hôte SMTP :

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

Où `host.domain` est le nom FQDN (Fully Qualified Domain Name - Nom de domaine entièrement qualifié).

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



**REMARQUE** : Les commandes des étapes 2 à 5 écrasent les paramètres existants configurés pour l'index que vous indiquez (1 à 4). Pour déterminer si un index possède des valeurs déjà configurées, tapez : `xracadm getconfig -g cfgEmailAlert - I <index>`. Si l'index est déjà configuré, des valeurs apparaissent pour les objets **cfgEmailAlertAddress** et **cfgEmailAlertEmailName**.

Pour en savoir plus, voir le *RACADM Command Line Reference Guide for iDRAC and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC et de CMC) disponible à l'adresse [dell.com/support/manuals](https://dell.com/support/manuals).

# 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.

## 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.

À l'exception des utilisateurs CMC disposant du privilège **Administrateur de serveur**, les privilèges attribués à un utilisateur CMC ne sont pas transférés automatiquement vers l'utilisateur de serveur correspondant, car les utilisateurs de serveur sont créés indépendamment des utilisateurs CMC. Autrement dit, les utilisateurs Active Directory CMC et les utilisateurs Active Directory iDRAC résident dans deux branches distinctes de l'arborescence Active Directory. Pour créer un utilisateur de serveur local, vous devez vous connecter dans l'écran Configurer les utilisateurs directement sur le serveur. La fonction Configurer les utilisateurs ne peut pas créer d'utilisateur de serveur depuis CMC et inversement. Cette règle préserve la sécurité et l'intégrité des serveurs.

**Tableau 7. Types d'utilisateurs**


| Droits                                      | Description                                                                                                                                           |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Ouverture de session utilisateur CMC</b> | L'utilisateur peut se connecter au CMC et afficher toutes les données CMC, mais ne peut pas ajouter ni modifier de données, ni exécuter de commandes. |

| Droits                                                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                           | <p>Il est possible qu'un utilisateur dispose d'autres privilèges même s'il ne possède pas le privilège Utilisateur de connexion CMC. Cette fonction est utile si un utilisateur n'est temporairement plus autorisé à se connecter. Lorsque vous restaurez le privilège Utilisateur de connexion CMC de cet utilisateur, il récupère tous les autres privilèges qui lui avaient précédemment été attribués.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Administrateur de configuration du châssis</b>                         | <p>L'utilisateur peut ajouter ou modifier des données qui :</p> <ul style="list-style-type: none"> <li>• Identifient le châssis, tels que le nom du châssis et son emplacement.</li> <li>• 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.</li> <li>• Fournissent des services au châssis, telles que la date et heure, la mise à jour de micrologiciel et la réinitialisation du CMC.</li> <li>• Sont associées au châssis, comme le nom de logement et la priorité de logement. Bien que ces propriétés s'appliquent aux serveurs, ce sont strictement des propriétés de châssis relatives aux logements, plutôt qu'aux serveurs proprement dits. C'est pourquoi il est possible d'ajouter et de modifier des noms et priorités de logement même si aucun serveur n'est présent dans le logement concerné.</li> </ul> <p>Lorsque vous transférez un serveur vers un autre châssis, il hérite du nom et de la priorité de logement qu'il occupe dans le nouveau châssis. Le nom et la priorité de logement précédents restent associés au châssis précédent.</p> <p> <b>REMARQUE</b> : Les utilisateurs CMC dotés du privilège d'<b>Administrateur de configuration du châssis</b> peuvent définir les paramètres d'alimentation. Toutefois, ils doivent disposer du privilège d'<b>Administrateur de contrôle de châssis</b> pour pouvoir effectuer les opérations d'alimentation de châssis, notamment mise sous tension ou hors tension et cycle d'alimentation).</p> |
| <b>Administrateur de configuration des utilisateurs</b>                   | <p>L'utilisateur peut :</p> <ul style="list-style-type: none"> <li>• Ajouter un nouvel utilisateur.</li> <li>• Changer le mot de passe d'un utilisateur</li> <li>• Changer les privilèges d'un utilisateur</li> <li>• 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.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Administrateur des effacements de journaux</b>                         | <p>L'utilisateur peut effacer le journal matériel et le journal CMC.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Administrateur de contrôle du châssis</b> (contrôle de l'alimentation) | <p>Les utilisateurs CMC dotés du privilège <b>Administrateur de contrôle du châssis</b> peuvent effectuer toutes les opérations liées à l'alimentation. Ils peuvent contrôler l'alimentation du châssis (allumage, extinction ou cycle d'alimentation).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

| Droits                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Server Administrator</b> | <p data-bbox="646 247 1374 338"> <b>REMARQUE</b> : Le privilège d'<b>Administrateur de configuration du châssis</b> est nécessaire pour configurer des paramètres d'alimentation.</p> <p data-bbox="646 369 1385 489">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.</p> <p data-bbox="646 499 1374 659">Lorsqu'un utilisateur possédant le privilège d'<b>Administrateur de serveur</b> émet une action à exécuter sur un serveur, le micrologiciel CMC envoie la commande au serveur ciblé sans vérifier les privilèges de l'utilisateur sur le serveur. Autrement dit, le privilège d'<b>Administrateur de serveur</b> permet de passer outre à l'absence de privilèges d'administrateur sur le serveur.</p> <p data-bbox="646 686 1374 764">Sans les droits d'<b>Administrateur de serveur</b>, un utilisateur créé sur le châssis ne peut exécuter une commande sur un serveur que lorsque les conditions suivantes sont réunies :</p> <ul data-bbox="646 774 1382 894" style="list-style-type: none"> <li>• Le même nom d'utilisateur est utilisé sur le serveur.</li> <li>• Le même nom d'utilisateur doit avoir exactement le même mot de passe sur le serveur.</li> <li>• L'utilisateur doit avoir le droit d'exécuter la commande.</li> </ul> <p data-bbox="646 919 1382 1079">Lorsqu'un utilisateur CMC sans privilège d'<b>Administrateur de serveur</b> émet une action à réaliser sur un serveur, CMC envoie une commande au serveur ciblé avec le nom et le mot de passe de connexion de cet utilisateur. Si l'utilisateur n'existe pas sur le serveur ou si le mot de passe ne correspond pas, l'utilisateur ne peut pas réaliser l'action.</p> <p data-bbox="646 1104 1374 1239">Si l'utilisateur existe sur le serveur cible et que le mot de passe correspond, le serveur répond en indiquant les droits accordés à l'utilisateur sur le serveur. En fonction des droits indiqués par le serveur, le micrologiciel du CMC décide si l'utilisateur a le droit de réaliser l'action.</p> <p data-bbox="646 1274 1369 1396">La liste ci-dessous indique les droits et les actions que l'administrateur du serveur a le droit de réaliser sur le serveur. Ces droits s'appliquent uniquement lorsque l'utilisateur du châssis ne dispose pas du droit Administrateur de serveur sur le châssis.</p> <p data-bbox="646 1407 1126 1434">Administration et configuration du serveur :</p> <ul data-bbox="646 1444 1155 1575" style="list-style-type: none"> <li>• Définir l'adresse IP</li> <li>• Définir la passerelle</li> <li>• Définir le masque de sous-réseau</li> <li>• Définir le périphérique de démarrage initial</li> </ul> <p data-bbox="646 1600 943 1627">Configurer les utilisateurs :</p> <ul data-bbox="646 1638 1086 1694" style="list-style-type: none"> <li>• Définir le mot de passe root d'iDRAC</li> <li>• Réinitialisation d'iDRAC</li> </ul> <p data-bbox="646 1719 1078 1747">Administration de contrôle du serveur :</p> <ul data-bbox="646 1757 882 1785" style="list-style-type: none"> <li>• Mise sous tension</li> </ul> |

| Droits                                         | Description                                                                                                                                             |
|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                | <ul style="list-style-type: none"> <li>Mise hors tension</li> <li>Cycle d'alimentation</li> <li>Arrêt normal</li> <li>Redémarrage du serveur</li> </ul> |
| <b>Utilisateur d'alertes de test</b>           | L'utilisateur peut envoyer des messages d'alerte d'essai.                                                                                               |
| <b>Administrateur de commandes de débogage</b> | L'utilisateur peut exécuter des commandes de diagnostic système.                                                                                        |
| <b>Administrateur de structure A</b>           | 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 8. Privilèges de groupe CMC**

| Groupe d'utilisateurs         | Privilèges accordés                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Administrateur</b>         | <ul style="list-style-type: none"> <li>Ouverture de session utilisateur CMC</li> <li>Administrateur de configuration du châssis</li> <li>Administrateur de configuration des utilisateurs</li> <li>Administrateur des effacements de journaux</li> <li>Server Administrator</li> <li>Utilisateur d'alertes de test</li> <li>Administrateur de commandes de débogage</li> <li>Administrateur de structure A</li> </ul> |
| <b>Utilisateur privilégié</b> | <ul style="list-style-type: none"> <li>Connexion</li> <li>Administrateur des effacements de journaux</li> <li>Administrateur de contrôle du châssis (contrôle de l'alimentation)</li> <li>Server Administrator</li> <li>Utilisateur d'alertes de test</li> <li>Administrateur de structure A</li> </ul>                                                                                                               |
| <b>Utilisateur invité</b>     | Connexion                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Personnalisé</b>           | <p>Sélectionnez n'importe quelle combinaison des autorisations suivantes :</p> <ul style="list-style-type: none"> <li>Ouverture de session utilisateur CMC</li> <li>Administrateur de configuration du châssis</li> <li>Administrateur de configuration des utilisateurs</li> <li>Administrateur des effacements de journaux</li> <li>Administrateur de contrôle du châssis (contrôle de l'alimentation)</li> </ul>   |

| Groupe d'utilisateurs | Privilèges accordés                                                                                                                                                                                       |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <ul style="list-style-type: none"> <li> Server Administrator</li> <li> Utilisateur d'alertes de test</li> <li> Administrateur de commandes de débogage</li> <li> Administrateur de structure A</li> </ul> |
| <b>Aucun</b>          | Aucun droit attribué                                                                                                                                                                                      |

**Tableau 9. Comparaison des privilèges des administrateurs CMC, des utilisateurs privilégiés et des utilisateurs invités**

| Privilège défini                                                   | Droits d'administrateur | Droits d'utilisateur privilégié | Droits d'utilisateur invité |
|--------------------------------------------------------------------|-------------------------|---------------------------------|-----------------------------|
| Ouverture de session utilisateur CMC                               | Oui                     | Oui                             | Oui                         |
| Administrateur de configuration du châssis                         | Oui                     | Non                             | Non                         |
| Administrateur de configuration des utilisateurs                   | Oui                     | Non                             | Non                         |
| Administrateur des effacements de journaux                         | Oui                     | Oui                             | Non                         |
| Administrateur de contrôle du châssis (contrôle de l'alimentation) | Oui                     | Oui                             | Non                         |
| Server Administrator                                               | Oui                     | Oui                             | Non                         |
| Utilisateur d'alertes de test                                      | Oui                     | Oui                             | Non                         |
| Administrateur de commandes de débogage                            | Oui                     | Non                             | Non                         |
| Administrateur de structure A                                      | Oui                     | Oui                             | Non                         |

## Modification des paramètres du compte administrateur de l'utilisateur root

Pour renforcer la sécurité, il est vivement recommandé de modifier le mot de passe par défaut du compte racine (Utilisateur 1). Le compte racine est le compte administratif par défaut fourni avec le contrôleur CMC.

Pour changer le mot de passe par défaut du compte racine :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** et sur **Authentification des utilisateurs**.
2. Sur la page **Utilisateurs**, dans la colonne **ID utilisateur**, cliquez sur **1**.



**REMARQUE** : L'ID utilisateur **1** correspond au compte utilisateur racine fourni par défaut avec le contrôleur CMC. Vous ne pouvez pas le modifier.

3. Sur la page **Configuration de l'utilisateur**, sélectionnez l'option **Changer le mot de passe**.
4. Entrez le nouveau mot de passe dans le champ **Mot de passe**, puis entrez-le de nouveau dans le champ **Confirmer le mot de passe**.
5. Cliquez sur **Appliquer**. Le mot de passe de l'utilisateur ayant l'ID **1** est modifié.

## Configuration des utilisateurs locaux


Vous pouvez définir jusqu'à 16 utilisateurs locaux dans le contrôleur CMC avec des privilèges d'accès spécifiques. Avant de créer un utilisateur CMC local, vérifiez s'il existe déjà des utilisateurs. Vous pouvez définir des noms d'utilisateur, des mots de passe et des rôles avec des privilèges pour ces utilisateurs. Les noms d'utilisateur et les mots de passe peuvent être changés dans n'importe quelle interface sécurisée CMC (telle que l'interface Web, RACADM ou WS-MAN).

### 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.

### Configuration d'utilisateurs locaux à l'aide de RACADM

 **REMARQUE** : Vous devez vous connecter comme utilisateur `root` pour pouvoir exécuter des commandes RACADM sur un système Linux distant.


Vous pouvez configurer jusqu'à 16 utilisateurs dans la base de données de propriétés CMC. Avant d'activer manuellement un utilisateur CMC, vérifiez s'il existe déjà des utilisateurs.

Si vous configurez un nouveau 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 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 10. : Privilèges par défaut des groupes de rôles**

| Groupe de rôles | Niveau de privilège par défaut | Droits accordées                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Masque binaire |
|-----------------|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| 1               | Aucun                          | <ul style="list-style-type: none"> <li>• Ouverture de session utilisateur CMC</li> <li>• Administrateur de configuration du châssis</li> <li>• Administrateur de configuration des utilisateurs</li> <li>• Administrateur des effacements de journaux</li> <li>• Administrateur de contrôle du châssis (contrôle de l'alimentation)</li> <li>• Server Administrator</li> <li>• Utilisateur d'alertes de test</li> <li>• Administrateur de commandes de débogage</li> <li>• Administrateur de structure A</li> </ul> | 0x00000fff     |
| 2               | Aucun                          | <ul style="list-style-type: none"> <li>• Ouverture de session utilisateur CMC</li> <li>• Administrateur des effacements de journaux</li> <li>• Administrateur de contrôle du châssis (contrôle de l'alimentation)</li> <li>• Server Administrator</li> <li>• Utilisateur d'alertes de test</li> <li>• Administrateur de structure A</li> </ul>                                                                                                                                                                      | 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 avec le schéma standard

Pour configurer le contrôleur CMC pour la connexion Active Directory :

1. Sur un serveur Active Directory (contrôleur de domaine), ouvrez le **snap-in Utilisateurs et ordinateurs Active Directory**.
2. 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

CMC fournit une solution générique permettant de prendre en charge l'authentification LDAP (Lightweight Directory Access Protocol - Protocole léger d'accès aux annuaires). Cette fonction ne requiert aucune extension de schéma dans les services d'annuaire.

L'administrateur CMC peut désormais intégrer les connexions aux serveurs LDAP dans CMC. Cette intégration nécessite des opérations de configuration à la fois sur le serveur LDAP et sur le CMC. Sur le serveur LDAP, vous utilisez un objet de groupe standard comme groupe de rôles. Tout utilisateur possédant un accès à CMC devient membre du groupe de rôles. Les privilèges sont toujours stockés dans CMC pour l'autorisation, comme avec la configuration de schéma standard Active Directory prise en charge.

Pour autoriser l'utilisateur LDAP à accéder à une carte CMC spécifique, vous devez configurer le nom du groupe de rôles et son nom de domaine sur la carte CMC concernée. Vous pouvez configurer un maximum de cinq groupes de rôles pour chaque CMC. Il est possible d'ajouter un utilisateur à plusieurs groupes dans le service d'annuaire. Si un utilisateur est membre de plusieurs groupes, il obtient les privilèges de tous les groupes concernés.

## Configuration de l'annuaire LDAP générique pour accéder à CMC

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


### 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.

3. Paramétrez les options suivantes :

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

- Paramètres communs
- Serveur à utiliser avec LDAP :
  - Serveur statique : spécifiez le nom FQDN (Fully Qualified Domain Name, nom de domaine entièrement qualifié) ou l'adresse IP, et le numéro du port LDAP.
  - Serveur DNS : spécifiez le serveur DNS afin de récupérer la liste des serveurs LDAP d'après leur enregistrement SRV dans DNS.

La requête DNS suivante est effectuée pour les enregistrements SRV :

```
_[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`.

Vous disposez d'un grand nombre d'options pour la configuration des connexions LDAP. La plupart du temps, certaines options peuvent être utilisées avec les paramètres par défaut.

 **REMARQUE** : Il est fortement recommandé d'utiliser la commande RACADM `testfeature -f LDAP` pour tester les paramètres LDAP pour les installations initiales. Cette fonction prend en charge à la fois 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=com4`

Le contrôleur CMC peut, si vous le souhaitez, être configuré pour interroger un serveur DNS pour récupérer les enregistrements SRV. Si vous activez la propriété `cfgLDAPSrvLookupEnable`, la propriété `cfgLDAPServer` est ignorée. La requête suivante est utilisée pour rechercher les enregistrements SRV dans le DNS :

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

`ldap` dans la requête ci-dessus est la propriété `cfgLDAPSrvLookupServiceName`.

`cfgLDAPSrvLookupDomainName` est configuré comme **nomdedomaine.com**.


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) sur le site [dell.com/support/manuals](http://dell.com/support/manuals).

# 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.

## 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, veuillez 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

## Systemes 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](http://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.

## Prerequis 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 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 de confiance dans un fichier keytab Kerberos de type MIT. Pour plus d'informations sur l'utilitaire ktpass, voir le site Web Microsoft.

Avant de générer un fichier keytab, vous devez créer le compte utilisateur Active Directory à utiliser avec l'option **-mapuser** de la commande `ktpass`. Vous devez utiliser le même nom que le nom DNS du CMC vers lequel vous téléversez le fichier keytab généré.


Pour générer un fichier keytab à l'aide de l'outil `ktpass` :

1. Exécutez l'utilitaire `ktpass` sur le contrôleur de domaine (serveur Active Directory) où vous souhaitez associer le contrôleur CMC à un compte utilisateur dans Active Directory.
2. Utilisez la commande `ktpass` suivante pour créer le fichier keytab Kerberos :

```
C:\>ktpass -princ HTTP/nom_cmc.nom_domaine.com@NOM_ROYAUME.COM - mapuser
dracname -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 le type de cryptage DES-CBC-MD5 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 le 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 -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 ces 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 utilisateur Active Directory valide.

La réussite d'une commande indique que le CMC parvient à acquérir les références Kerberos et à accéder au compte Active Directory de l'utilisateur. Si la commande échoue, corrigez l'erreur et exécutez la commande à nouveau. Pour en savoir plus, consultez 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) sur le site [dell.com/support/manuals](http://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 -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 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*.

## 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 la ligne de commande CMC

Lorsque vous vous connectez à la ligne de commande CMC, vous pouvez entrer les commandes suivantes :

**Tableau 11. Commandes de la ligne de commande CMC**

| Commande            | Description                                                                                                                                                                                                                                                                         |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>racadm</code> | Les commandes RACADM commencent par le mot-clé <code>racadm</code> suivi d'une sous-commande. Pour en savoir plus, voir le <i>Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide</i> (Guide de référence de la ligne de commande RACADM) |

| Commande                                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>connect</code>                                         | <p>de Dell Chassis Management Controller pour PowerEdge FX2/FX2s).</p> <p>Permet de se connecter à la console série d'un serveur ou d'un module d'E/S. Pour en savoir plus, voir <a href="#">Connexion aux serveurs ou un module d'E/S à l'aide de la commande connect</a>.</p> <p> <b>REMARQUE</b> : Vous pouvez également utiliser la commande RACADM <code>connect</code>.</p> |
| <code>exit</code> , <code>logout</code> et <code>quit</code> | <p>Toutes les commandes exécutent la même opération. Elles mettent fin à la session actuelle et affichent de nouveau une interface de ligne de commande de connexion.</p>                                                                                                                                                                                                                                                                                          |

## 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 le problème, téléchargez le hotfix 824810 depuis le site [support.microsoft.com](http://support.microsoft.com). Pour plus d'informations, vous pouvez également consulter l'article 824810 de 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 cryptage 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 au cours de la connexion à CMC, le client SSH affiche un message d'erreur. Le texte de ce message dépend du client et n'est pas contrôlé par le CMC. Consultez les messages du journal RACLog pour déterminer la cause de l'incident.

 **REMARQUE** : Vous devez exécuter `OpenSSH` depuis un émulateur de terminal VT100 ou ANSI sous Windows. Vous pouvez également exécuter `OpenSSH` en utilisant **Putty.exe**. L'exécution d'`OpenSSH` depuis l'invite de commande Windows offre des fonctionnalités limitées (certaines touches ne répondent pas et aucun graphique n'est affiché). Sous Linux, exécutez les services client SSH pour vous connecter au contrôleur CMC avec n'importe quel shell.

Quatre sessions SSH simultanées sont prises en charge à la fois. Le délai d'expiration des sessions est contrôlé par la propriété `cfgSsnMgtSshIdleTimeout`. 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 Chassis Management Controller pour PowerEdge FX2/FX2s) sur le site [dell.com/support/Manuals](http://dell.com/support/Manuals).

CMC prend également en charge l'authentification PKA (Public Key Authentication, Authentification par clé publique) sur SSH. Cette méthode d'authentification améliore l'automatisation des scripts SSH en rendant inutile l'incorporation ou l'affichage d'une invite pour la saisie de l'ID utilisateur/du 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 12. Schémas de cryptographie**

| Type de schéma            | Couleurs                                                                                                                                                                                                                                                     |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cryptographie asymétrique | Spécification de bits (aléatoire) Diffie-Hellman DSA/DSS 512-1024 par NIST                                                                                                                                                                                   |
| Cryptographie symétrique  | <ul style="list-style-type: none"><li>• AES256-CBC</li><li>• RIJNDAEL256-CBC</li><li>• AES192-CBC</li><li>• RIJNDAEL192-CBC</li><li>• AES128-CBC</li><li>• RIJNDAEL128-CBC</li><li>• BLOWFISH-128-CBC</li><li>• 3DES-192-CBC</li><li>• ARCFOUR-128</li></ul> |
| Intégrité du message      | <ul style="list-style-type: none"><li>• HMAC-SHA1-160</li><li>• HMAC-SHA1-96</li><li>• HMAC-MD5-128</li><li>• HMAC-MD5-96</li></ul>                                                                                                                          |
| 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 `sshpkeyauth`, 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 :

- La commande `connect` de l'interface de ligne de commande ou de RACADM du CMC. 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 module d'E/S. La console série de serveur contient les écrans de démarrage BIOS et de configuration et la console série de système d'exploitation. Pour le module d'E/S, la console série de commutation est disponible. Le châssis contient un seul IOM.

 **PRÉCAUTION :** Lorsque vous l'exécutez depuis la console série CMC, l'option `connect -b` reste connectée jusqu'à la réinitialisation du contrôleur CMC. Cette connexion est un risque potentiel de sécurité.

 **REMARQUE :** La commande `connect` fournit l'option `-b` (binaire). L'option `-b` transmet des données binaires brutes et `cfgSerialConsoleQuitKey` n'est pas utilisé. De plus, lorsque vous vous connectez à un serveur avec la console série CMC, les transitions du signal DTR (par exemple, si le câble série est retiré pour connecter un module de débogage) ne provoquent aucune déconnexion.

 **REMARQUE :** Si un module IOM ne prend pas en charge la redirection de console, la commande `connect` affiche une console vide. Dans ce cas, pour revenir à la console CMC, entrez une séquence d'échappement. La séquence d'échappement par défaut de la console est `<Ctrl>\`.

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


```
connect switch-n
```


, où `n` est une étiquette IOM A1.

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

**Tableau 13. 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 de serveur géré, 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 en utilisant l'option `-b`, la communication binaire est utilisée par défaut et le caractère d'échappement est désactivé. Si le contrôleur 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 BIOS, vous devez activer la redirection série dans la configuration BIOS du serveur. Vous devez également définir la résolution 80 x 25 de la fenêtre d'émulation de terminal. Autrement les caractères sur la page ne s'affichent pas correctement.
-  **REMARQUE** : Certaines touches ne fonctionnent pas sur les pages de configuration du BIOS. Par conséquent, entrez les raccourcis clavier appropriés pour <Ctrl> <Alt> <Supprimer> et les autres. 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 d'utilisation du *Dell Integrated Dell Remote Access Controller (iDRAC) User's Guide* (Guide d'utilisation d'iDRAC) à l'adresse [dell.com/support/manuals](http://dell.com/support/manuals)).

La communication série dans le BIOS est désactivée par défaut. Pour rediriger les données de console texte de l'hôte vers SOL (Serial over LAN), vous devez activer la redirection de console via COM1. Pour modifier le paramètre BIOS :

1. Mettez le serveur géré sous tension.
2. Appuyez sur la touche <F2> pour accéder à l'utilitaire de configuration du BIOS pendant le test POST.
3. Accédez à **Communication série** et appuyez sur <Entrée>. Dans la boîte de dialogue, la liste des communications série affiche les options suivantes :
  - **désactivé**
  - **activé sans redirection de console**
  - **activé avec redirection de console via COM1**

Pour naviguer entre ces options, appuyez sur les touches fléchées.

-  **REMARQUE** : Vérifiez que l'option **Activer avec la redirection de console via COM1** est sélectionnée.


4. Activez l'option **Redirection après démarrage** (la valeur par défaut est **Désactivé**). Cette option permet la redirection de console BIOS pour les redémarrages suivants.
5. Enregistrez les modifications et quittez.  
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 x 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 # # Notez qu'il est inutile d'exécuter de
nouveau grub après modification # de ce fichier. # REMARQUE : vous n'avez
pas de partition /boot. Ceci signifie que tous # les chemins kernel et
initrd sont relatifs par rapport à /, ex. : # root (hd0,0) # kernel /boot/
vmlinuz-version ro root= /dev/sdal # initrd /boot/initrd-version.img #
#boot=/dev/sda default=0 timeout=10 #splashimage=(hd0,2)/grub/splash.xpm.gz
serial --unit=1 --speed=57600 terminal --timeout=10 serial title Red Hat Linux Advanced
Server (2.4.9-e.3smp) root (hd0,0) kernel /boot/vmlinuz-2.4.9-e.3smp ro
root= /dev/sdal 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/sdal initrd /boot/
initrd-2.4.9-e.3.img
```

Lors de la modification du fichier `/etc/grub.conf`, appliquez les consignes suivantes :

- Désactivez l'interface graphique GRUB et utilisez l'interface texte. Sinon, l'écran GRUB ne s'affiche pas pour la redirection de console. Pour désactiver l'interface graphique, mettez en commentaire la ligne qui commence par `splashimage`.
- Pour activer plusieurs options GRUB afin de démarrer les sessions de console via la connexion série, ajoutez la ligne suivante à toutes les options :

```
console=ttyS1,57600
```

Dans l'exemple, `console=ttyS1,57600` est ajouté à la première option uniquement.

## Configuration de Linux pour la redirection de console série du serveur après l'amorçage

Modifiez le fichier `/etc/inittab` de la manière suivante :

Ajoutez une nouvelle ligne pour configurer `agetty` sur le port série COM2 :

```
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
```

L'exemple suivant montre le fichier avec la nouvelle ligne.

```
inittab 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 10:0:wait:/etc/rc.d/rc 0 11:1:wait:/etc/
rc.d/rc 1 12:2:wait:/etc/rc.d/rc 2 13:3:wait:/etc/rc.d/rc 3 14:4:wait:/etc/
rc.d/rc 4 15:5:wait:/etc/rc.d/rc 5 16:6: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
```

# 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.

## 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`  
Aucune fonction active sur le châssis

```
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 14. Messages d'état renvoyés par la commande `featurecard -s`**

| Message de condition                                                                                                                                                              | Actions                                                                                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>No feature card inserted.</code>                                                                                                                                            | Vérifiez que la carte SD est correctement insérée dans le contrôleur CMC.                                                                                                                                                                                                            |
| <code>The feature card inserted is valid and contains the following feature(s)<br/>FlexAddress: bound.</code>                                                                     | Aucune action n'est requise.                                                                                                                                                                                                                                                         |
| <code>The feature card inserted is valid and contains the following feature(s)<br/>FlexAddress: bound to another chassis,<br/>svctag=ABC1234, SD card SN =<br/>1122334455.</code> | Retirez la carte SD, localisez et installez la carte SD du châssis actuel.                                                                                                                                                                                                           |
| <code>The feature card inserted is valid and contains the following feature(s)<br/>FlexAddress: not bound.</code>                                                                 | Vous pouvez déplacer la carte de fonction SD vers un autre châssis ou la réactiver dans le châssis actuel. Pour la réactiver dans le châssis actuel, entrez <code>racadm racreset</code> jusqu'à ce que le module CMC dans lequel la carte de fonction est installée devienne actif. |


Les cartes de fonction Dell peuvent contenir plusieurs fonctions. Une fois que vous avez activé une fonction depuis une carte de fonction Dell sur le châssis, aucune des autres fonctions figurant sur la même carte de fonction Dell ne peut être activée sur un autre châssis. Dans ce cas, la commande « `racadm feature -s` » affiche le message suivant pour les fonctions concernées :

```
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 *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de Chassis Management Controller pour PowerEdge FX2/FX2s).

## Désactivation de FlexAddress

La fonction FlexAddress peut être désactivée et vous pouvez rétablir l'état qui existait avant l'installation de la carte SD, à l'aide d'une commande RACADM. L'interface Web n'offre aucune fonction de désactivation. La désactivation rétablit l'état d'origine de la carte SD, ce qui permet de l'installer et de l'activer sur un autre châssis. Dans ce contexte, le terme FlexAddress, désigne à la fois FlexAddress et FlexAddress Plus.

 **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 *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de 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'une CMC à sa configuration d'usine par défaut à l'aide de la sous-commande `racresetcfg`. Il s'agit de la configuration « désactivé ». La syntaxe RACADM est :

```
racadm racresetcfg -c flex
```

Pour en savoir plus sur les commandes RACADM liées à FlexAddress et les données concernant les autres propriétés définies en usine, voir le *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 à l'adresse [dell.com/support/manuals](http://dell.com/support/manuals).

Vous devez mettre hors tension le serveur avant de commencer la configuration. Vous pouvez activer ou désactiver FlexAddress séparément pour chaque structure. De plus, vous pouvez activer ou désactiver la fonction pour chaque logement. Après avoir activé la fonction selon chaque structure, vous pouvez sélectionner les logements à activer. Par exemple, si vous activez Structure-A, FlexAddress est activé uniquement pour Structure-A dans tous les logements activés. Toutes les autres structures utilisent l'adresse WWN/MAC définie en usine sur le serveur.

 **REMARQUE** : Lorsque vous déployez la fonction FlexAddress pour la première fois sur un module de serveur donné, vous devez éteindre et rallumer ce serveur pour que FlexAddress prenne effet. Sur les périphériques Ethernet, FlexAddress est programmé par le BIOS du module de serveur. Pour que le BIOS du module de serveur programme l'adresse, il doit être opérationnel, ce qui exige que ce module de serveur soit allumé. Une fois la séquence extinction-allumage terminée, les ID MAC attribués par le châssis sont disponibles pour la fonction Wake-On-LAN (WOL).

## Configuration de FlexAddress pour les structures et logements au niveau du châssis

Au niveau du châssis, vous pouvez activer ou désactiver la fonction FlexAddress pour les structures et logements. FlexAddress est activé en fonction de chaque structure, puis vous sélectionnez les logements à inclure dans la fonction. Vous devez activer à la fois des structures et des logements pour configurer correctement FlexAddress.

## Affichage des ID de nom universel/Contrôle de l'accès aux médias (WWN/MAC)

La page **Résumé WWN/MAC** affiche la configuration WWN et l'adresse 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 15. Commandes et sortie FlexAddress**

| Problème                                                                                                                                                                                        | Commande                                                                                                                                              | Sortie                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| La carte SD du module du contrôleur CMC est liée à un autre numéro de service.                                                                                                                  | <code>\$racadm featurecard -s</code>                                                                                                                  | La carte de fonction insérée est valide et contient la ou les fonction(s) suivante(s)<br><br>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.                                                                                                                     | <code>\$racadm featurecard -s</code>                                                                                                                  | La carte de fonction insérée est valide et contient la ou les fonction(s) suivante(s)<br><br>FlexAddress: bound                                                                                                   |
| La carte SD du module du contrôleur CMC n'est liée à aucun numéro de service.                                                                                                                   | <code>\$racadm featurecard -s</code>                                                                                                                  | The feature card inserted is valid and contains the following feature(s)<br><br>FlexAddress : non lié                                                                                                             |
| 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) | <code>\$racadm setflexaddr [-f &lt;fabricName&gt; &lt;slotState&gt;]</code><br><code>\$racadm setflexaddr [-i &lt;slot#&gt; &lt;slotstate&gt;]</code> | ERROR: Flexaddress feature is not active on the chassis                                                                                                                                                           |
| L'utilisateur invité tente de définir FlexAddress sur des logements/des structures.                                                                                                             | <code>\$racadm setflexaddr [-f &lt;fabricName&gt; &lt;slotState&gt;]</code><br><code>\$racadm setflexaddr [-i &lt;slot#&gt; &lt;slotstate&gt;]</code> | ERROR: Insufficient user privileges to perform operation                                                                                                                                                          |

| Problème                                                                                                                          | Commande                                                                                                                                    | Sortie                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Désactivation de la fonctionnalité FlexAddress alors que le châssis est sous tension                                              | <code>\$racadm feature -d -c flexaddress</code>                                                                                             | ERROR: Unable to deactivate the feature because the chassis is powered ON                                                                                                               |
| L'utilisateur invité essaie de désactiver la fonctionnalité sur le châssis                                                        | <code>\$racadm feature -d -c flexaddress</code>                                                                                             | ERROR: Insufficient user privileges to perform operation                                                                                                                                |
| Modification des paramètres FlexAddress de logement/structure pendant que les modules de serveur sont sous tension.               | <code>\$racadm setflexaddr -i 1 1</code>                                                                                                    | 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. | <code>\$racadm setflexaddr -i&lt;slotnum&gt; &lt;status&gt;</code><br><code>\$racadm setflexaddr -f&lt;FabricName&gt; &lt;status&gt;</code> | ERREUR : SWC0242 : il manque une licence requise ou la licence a expiré. Obtenez une licence appropriée et recommencez ou contactez le fournisseur de service pour plus d'informations. |



**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 sur les adresses WWN/MAC

Vous pouvez afficher l'inventaire des adresses WWN/MAC des Adaptateurs réseau pour chaque logement de serveur ou tous les serveurs présents dans le châssis. L'inventaire comprend 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 inoccupés 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 en regard du composant indique que la structure est activée pour FlexAddress ou FlexAddressPlus.
- Protocole utilisé sur le port d'adaptateur de carte réseau (NIC). Par exemple, LAN, iSCSI, FCoE et ainsi de suite.
  - Configuration Fibre Channel World Wide Name (WWN) et adresses MAC (Media Access Control d'un logement dans le châssis).
  - Type d'affectation d'adresse MAC et type d'adresse active actuelle : affecté par le serveur, FlexAddress ou MAC d'identité d'E/S. Une coche verte indique le type d'adresse active, soit attribué 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 la CLI RACADM. En fonction de l'interface, vous pouvez filtrer l'adresse MAC et savoir quelle adresse WWN/MAC est en cours d'utilisation pour cette fonction ou partition. Si la fonction NPAR de l'adaptateur est activée, vous pouvez afficher quelles partitions sont activées ou désactivées.

À l'aide de l'interface Web, vous pouvez afficher les informations des adresses WWN/MAC de logements spécifiques à l'aide de la page **FlexAddress** (Cliquez sur **Présentation des serveurs** → **Logement <x>** → **Configuration** → **FlexAddress**). Vous pouvez afficher les informations des adresses WWN/MAC pour tous les logements et le serveur à l'aide de la page **Résumé WWN/MAC** (cliquez sur **Présentation du serveur** → **Propriétés** → **WWN/MAC**). Dans les deux pages vous pouvez afficher les informations des adresses WWN/MAC en mode de Base ou en mode Avancé :

- **Mode de base** : dans ce mode, vous pouvez afficher Logement du serveur, Structure, Protocole, les adresses WWN/MAC et État de partition. Seules les adresses MAC actives s'affichent dans le champ de l'adresse WWN/MAC. Vous pouvez filtrer à l'aide de certains ou tous les champs affichés.
- **Mode avancé** : dans ce mode, vous pouvez afficher tous les champs affichés en mode de Base et tous les types d'adresses MAC (affecté par le serveur, Flex Address et Identité d'E/S). Vous pouvez filtrer à l'aide de certains ou tous les champs affichés.

Dans le mode de Base et le mode Avancé, les informations des adresses WWN/MAC s'affichent dans une forme réduite. Cliquez sur l'  en regard d'un logement ou cliquez sur le bouton **Tout développer/réduire** pour afficher les informations d'un logement spécifique ou tous les emplacements.

Vous pouvez également exporter les informations des adresses WWN/MAC pour tous les serveurs dans le châssis vers 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 de base sur les adresses WWN/MAC à l'aide de l'interface Web

Pour afficher les informations sur les adresses WWN/MAC de chaque logement de serveur ou tous les serveurs présents dans le châssis, en mode de Base :

1. Cliquez sur **Présentation du serveur** → **Propriétés** → **WWN/MAC**  
La page **Résumé WWN/MAC** affiche les informations sur les adresses WWN/MAC.  
Vous pouvez également cliquer sur **Présentation du serveur** → **Logement <x>** → **Configuration** → **FlexAddress** pour afficher les informations relatives à l'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 **Tout développer/réduire** 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 **Base** 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 pour tous les serveurs ou les serveurs dans des emplacements spécifiques uniquement.
6. Dans le menu déroulant **Structure**, sélectionnez l'un des types de structure pour afficher les détails de certains ou tous les types de structures de gestion ou 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 l'adresse MAC spécifique, saisissez l'adresse MAC exacte. Sinon, entrez des adresses MAC partielles pour afficher les logements associés. Par exemple, saisissez 4A pour afficher les logements avec des adresses MAC qui contiennent 4A.
9. Dans le menu déroulant **État de partition**, sélectionnez l'état des partitions pour afficher les serveurs avec l'état de partition sélectionné.  
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 sur les adresses WWN/MAC à l'aide de l'interface Web

Pour afficher les informations sur les adresses WWN/MAC de chaque logement de serveur ou tous les serveurs présents dans le châssis, en mode Avancé :

1. Cliquez sur **Présentation du serveur** → **Propriétés** → **WWN/MAC**

La page **Résumé WWN/MAC** affiche les informations sur les adresses WWN/MAC.

2. Dans le menu déroulant **Afficher**, sélectionnez **Avancé** pour afficher les attributs des adresses WWN/MAC dans une vue détaillée.

Le tableau **Adresses WWN/MAC** affiche Logement de serveur, Structure, Protocole, Adresses WWN/MAC, Type d'affectation d'adresse MAC (Affecté par le serveur, FlexAddress ou MAC d'identité d'E/S) et État de partition. Une coche verte indique le type de l'adresse active, soit attribuée par le serveur, par le châssis ou à distance. MAC. Si la fonction FlexAddress ou Identité d'E/S d'un serveur n'est pas activée, l'état de **FlexAddress (affecté par le châssis)** ou de **Identité d'E/S (affecté à distance)** est **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 **Tout développer/réduire** 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 pour tous les serveurs ou les serveurs dans des emplacements spécifiques uniquement.
6. Dans le menu déroulant **Structure**, sélectionnez l'un des types de structure pour afficher les détails de certains ou tous les types de structures de gestion ou 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**, saisissez l'adresse MAC pour afficher uniquement les logements associés à l'adresse MAC spécifique. Vous pouvez également saisir des adresses MAC partielles pour afficher les logements associés. Par exemple, entrez **4A** pour afficher les logements dont les adresses MAC contiennent **4A**.
9. Dans le menu déroulant **État de partition**, sélectionnez l'état des partitions pour afficher les serveurs avec l'état de partition sélectionné.  
Si une partition donnée est désactivée, l'état 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 sur les adresses WWN/MAC à l'aide de RACADM

Pour afficher les informations sur les adresses WWN/MAC pour tous les serveurs ou des serveurs spécifiques à l'aide de RACADM, utilisez les sous-commandes **getmacaddress** et **getflexaddr**.

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 l'adresse MAC iSCSI d'un serveur spécifique, utilisez la commande RACADM suivante :

```
racadm getmacaddress [-m <module> [-x]] [-t iscsi]
```

Pour afficher les adresses MAC et WWN définis 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 tous les LOM ou cartes mezzanine, utilisez la commande RACADM suivante :

```
racadm getmacaddress -c all
```

Pour afficher l'adresse WWN/MAC attribué par le châssis, utilisez la commande RACADM suivante :

```
racadm getmacaddress -c flexaddress
```


Pour afficher l'adresse MAC/WWN de tous les LOM ou cartes mezzanine, utilisez la commande RACADM suivante :

```
racadm getmacaddress -c factory
```

Pour en savoir plus sur les sous-commandes **getflexaddr** et **getmacaddress**, 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 Chassis Management Controller pour PowerEdge FX2/FX2s*).

## 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 (disponible dans PowerEdge FX2/FX2s)

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.

## Surveillance de l'intégrité des modules d'E/S (IOM)


Pour plus d'informations sur la surveillance de l'intégrité IOM, voir Affichage des informations et de l'état d'intégrité des modules IOM.


## Définition des paramètres réseau pour le module IOM

Vous pouvez spécifier les paramètres réseau de l'interface utilisée pour gérer le module d'E/S (IOM). Pour les commutateurs Ethernet, le port de gestion hors bande (adresse IP) est configuré. Le port de gestion intrabande (VLAN1) n'est pas configuré avec cette interface.

Avant de définir les paramètres réseau pour le module IOM, vérifiez que ces modules sont sous tension.

Pour pouvoir définir les paramètres réseau pour le module IOM dans le groupe A, vous devez disposer des privilèges d'administrateur de structure A.

 **REMARQUE** : Pour les commutateurs Ethernet, les adresses IP de gestion intrabande (VLAN1) et hors bande doivent être différentes et sur des réseaux différents. Par conséquent, l'adresse IP hors bande n'est pas définie. Consultez la documentation IOM pour connaître l'adresse IP de gestion intrabande par défaut.

 **REMARQUE** : Ne configurez pas les paramètres réseau des modules d'E/S pour les commutateurs d'intercommunication Ethernet et Infiniband.


## Définition des paramètres réseau du module IOM à l'aide de l'interface Web CMC

Pour définir les paramètres réseau du module d'E-S :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis**, **Présentation du module d'E/S**, 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.

3. Cliquez sur **Appliquer**.

Les paramètres réseau sont définis pour le module IOM.

 **REMARQUE** : Si vous y êtes autorisé, vous pouvez réinitialiser les valeurs de configuration par défaut des réseaux VLAN, des propriétés réseau et des ports d'E/S.

## Définition des paramètres réseau d'un module IOM à l'aide de RACADM

Pour définir les paramètres réseau d'un module IOM à l'aide de RACADM, définissez la date et l'heure. Voir la section relative aux commandes de déploiement dans 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).


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'E/S à l'aide de 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 État du module d'E/S spécifique au logement du module d'E/S s'affiche. Les tableaux État des liaisons montantes de module d'E/S et État des données descendantes de module d'E/S s'affichent.

Ces tableaux affichent les informations concernant les ports de liaisons descendantes (1 à 8) et les ports de liaisons montantes (9 à 12). Pour en savoir plus, voir 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 l'agrégateur d'E/S Dell PowerEdge M à l'aide de l'interface Web CMC comme suit :

1. Accédez à **Présentation du châssis** → **Présentation du module d'E/S**.  
Tous les modules d'E/S (1–6) apparaissent dans la liste développée.
2. Cliquez sur le module d'E/S (logement) que vous voulez afficher, puis 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 permet d'extraire les informations relatives à la session FCoE du commutateur et de les présenter 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 sous tension.
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).

## 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.

### 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 avec 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 non marqués pour les IOM avec l'interface Web CMC

Pour mettre à jour les VLAN non marqués des modules d'E/S (IOM) avec 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 pour les IOM avec 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.

## 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

## 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

La règle de redondance de réseau a pour but de permettre à un système d'enceinte de fonctionner dans un mode où il peut tolérer les pannes de l'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, branchez les blocs d'alimentation 1 et 2 pour séparer les réseaux d'alimentation.

Dans ce mode, le CMC assure la conservation de la consommation d'énergie, assurant ainsi le fonctionnement continu du système sans dégradation, qu'une panne du réseau d'alimentation ou d'un bloc d'alimentation survienne ou non. L'option de mise sous tension du serveur dépend de l'alimentation 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

Dans ce mode, toute la puissance des blocs d'alimentation est disponible et utilisée, mais il n'y a aucune garantie que la défaillance d'un bloc d'alimentation ou du réseau n'affectera pas le fonctionnement du système. L'état de redondance du châssis est toujours **Sans redondance**.

### Stratégie Alertes de redondance uniquement

La stratégie Alertes de redondance uniquement permet de mettre le serveur sous tension de manière à utiliser les deux blocs d'alimentation, tout en envoyant des alertes concernant la perte de redondance basées sur des conditions réelles. La perte de redondance est signalée lorsqu'un bloc d'alimentation est retiré ou échoue, ou si la consommation d'énergie dépasse les capacités d'un seul bloc d'alimentation. Il s'agit de la stratégie par défaut.

### 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 chariot multi-nœuds

Le PowerEdge FM120x4 est un chariot 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

Open Manage 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, mais 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.

## 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 *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).

## Condition de la redondance et intégrité énergétique globale

La condition de redondance est un facteur déterminant dans l'intégrité de l'alimentation globale. Par exemple, si vous définissez la stratégie de redondance sur Redondance de l'alimentation de réseau et si la condition de redondance indique que le système fonctionne en mode redondant, l'intégrité d'alimentation globale est généralement **OK**. Toutefois, s'il est impossible de réunir les conditions du fonctionnement en mode de redondance d'alimentation de réseau, la condition de redondance est **Non** et l'intégrité globale de l'alimentation devient **Critique**. En effet, le système ne peut pas fonctionner en accord avec 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 d'alimentation et de la règle de redondance dans le journal des événements système

Les changements d'état des blocs d'alimentation et de stratégie de redondance de l'alimentation sont enregistrés en tant qu'événements. Les événements liés à l'alimentation qui journalisent des entrées dans le journal d'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 confirmation ou déconfirmation de la sortie d'alimentation.

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

**Tableau 16. Événements du journal SEL relatifs aux modifications des blocs d'alimentation**

| <b>Événement d'alimentation</b>     | <b>Entrée du journal d'événements système (SEL)</b> |
|-------------------------------------|-----------------------------------------------------|
| Insertion                           | Alimentation électrique présente.                   |
| Retrait                             | Alimentation absente.                               |
| Alimentation alternative reçue      | L'entrée de l'alimentation a été restaurée.         |
| perte de l'alimentation alternative | L'entrée de l'alimentation est perdue               |
| sortie CC produite                  | L'alimentation électrique fonctionne correctement.  |
| Perte de sortie en CC               | Défaillance de l'alimentation électrique.           |

Les événements liés aux changements de l'état de redondance de l'alimentation qui enregistrent des entrées dans le journal SEL sont la perte de redondance et le rétablissement de la redondance pour une enceinte configurée avec la stratégie d'alimentation **Redondance de l'alimentation de réseau** ou **Alertes de redondance uniquement**. Le tableau suivant répertorie les entrées SEL liées aux modifications de la redondance d'alimentation.

| <b>Événement de stratégie d'alimentation</b> | <b>Entrée du journal d'événements système (SEL)</b>                                      |
|----------------------------------------------|------------------------------------------------------------------------------------------|
| Perte de la redondance                       | Power supply redundancy is lost. (Perte de la redondance du bloc d'alimentation.)        |
| Regain de la redondance                      | The power supplies are not redundant. (Les blocs d'alimentation ne sont pas redondants.) |

## Configuration du bilan d'alimentation et de la redondance

Vous pouvez configurer le bilan d'alimentation, la redondance et l'alimentation dynamique de l'ensemble du châssis (châssis, serveurs, 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

## Économie d'énergie et bilan de puissance

Si la consommation d'énergie 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 avec l'interface Web CMC

 **REMARQUE** : Vous devez disposer du privilège **Administrateur de configuration du châssis** pour pouvoir exécuter les tâches de gestion de l'alimentation.

Pour configurer le bilan de puissance :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** → **Alimentation** → **Configuration**.
2. Dans la page **Configuration du bilan/de la redondance**, sélectionnez certaines ou toutes les propriétés suivantes en fonction des besoins. Pour plus d'informations sur les champs, voir l'*Aide en ligne*.
  - **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 **Administrateur 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 *<valeur>* est 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 *<valeur>* est 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 énergétique maximale, entrez :  

```
racadm config -g cfgChassisPower -o cfgChassisMaxPowerConservationMode 1
```
  - Pour rétablir le fonctionnement normal, entrez :  

```
racadm config -g cfgChassisPower -o cfgChassisMaxPowerConservationMode 0
```
  - Pour activer la fonctionnalité de journalisation de l'alimentation distante, entrez la commande suivante :  

```
racadm config -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingEnabled 1
```
  - Pour spécifier l'intervalle de journalisation de votre choix, entrez la commande suivante :  

```
racadm config -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingInterval n
```

 où *n* correspond à 1 à 1 440 minutes.
  - Pour déterminer si la fonction de journalisation de l'alimentation distante est activée, entrez la commande suivante :  

```
racadm getconfig -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingEnabled
```
  - Pour déterminer l'intervalle de journalisation à distance de l'alimentation, entrez la commande suivante :  


```
racadm getconfig -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingInterval
```
- La fonction de journalisation à distance de l'alimentation dépend des hôtes syslog distants déjà configurés. Vous devez activer la journalisation sur un ou plusieurs hôtes syslog distants. Autrement, la consommation électrique n'est pas journalisée. Vous pouvez effectuer l'opération dans l'interface utilisateur graphique Web ou dans l'interface de ligne de commande (CLI) RACADM. Pour plus d'informations, voir les instructions de configuration des hôtes syslog distants.
- 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**, **getpbinf** et **cfgChassisPower** du *Dell Chassis Management Controller for PowerEdge FX2/FX2s RACADM Command Line Reference Guide* (Guide de référence de la ligne de commande RACADM de 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 pouvoir exécuter les tâches de gestion de l'alimentation.

## Exécution d'opérations de contrôle de l'alimentation sur le module IOM à l'aide de l'interface Web CMC

Pour exécuter des opérations de contrôle de l'alimentation sur le module d'E/S :

1. Dans le volet de gauche, cliquez sur **Présentation du châssis** → **Présentation du module d'E/S** → **Alimentation**.
2. Sur la page **Contrôle de l'alimentation**, pour le module IOM, dans le menu déroulant, sélectionnez l'opération à exécuter (cycle d'alimentation).
3. Cliquez sur **Appliquer**.

## Exécution d'opérations de contrôle de l'alimentation sur le module IOM à l'aide de RACADM

Pour exécuter des opérations de contrôle de l'alimentation sur le module IOM à l'aide de RACADM, ouvrez une console texte série/Telnet/SSH sur le contrôleur CMC, connectez-vous et entrez :

```
racadm chassisaction -m switch <action>
```


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

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) sur le site [dell.com/support/manuals](http://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.


## Affichage des logements PCIe

Les châssis PowerEdge FX2/FX2s contiennent (en option) huit logements PCIe, où chaque logement PCIe est attribué à un traîneau. Par défaut, tous les emplacements PCIe sont adressés. Les logements PCIe ne peuvent pas être réattribués ou non affectés aux serveurs.


| Logement PCIe   | Adressage du 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                            |

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

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

 **REMARQUE** : La fonction de surveillance sans agent n'est pas disponible pour le contrôleur PERC PCIe et les cartes réseau se trouvant dans les logements PCIe du châssis. La surveillance sans agent est la solution de gestion des serveurs Dell de 12e génération. Elle s'effectue complètement hors bande et ne dépend d'aucun agent du système d'exploitation. L'utilisation de cette solution vous permet de surveiller les systèmes de stockage reliés aux périphériques réseau du serveur (PERC, les disques durs, les enceintes, etc.) à l'aide de l'iDRAC, sans procéder à l'installation d'un agent sur le système géré ou sur la station de gestion. Pour en savoir plus sur la surveillance sans agent, voir le livre blanc *Agent-free inventory and monitoring for storage and network devices in Dell PowerEdge 12G Servers* (Inventaire et surveillance sans agent des périphériques de stockage et de réseau sur les serveurs Dell PowerEdge de 12e génération) du Dell TechCenter.


## Affichage des propriétés des logements PCIe à l'aide de l'interface Web CMC

- Pour afficher les informations relatives aux huit logements PCIe, dans le volet de gauche, cliquez sur **Présentation du châssis** → **Présentation de PCIe**. Cliquez sur le  pour afficher toutes les propriétés du logement approprié.

- Pour afficher les informations d'un logement PCIe, cliquez sur **Présentation du châssis** → **Logement PCIe <numéro>** → **Propriétés** → **Condition**.

## Affichage des propriétés des logements PCIe à l'aide de l'interface 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](http://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 chariot 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
```

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

## 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

## 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 en savoir plus sur `racdump`, 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).

| Sous-système                                     | Commande RACADM |
|--------------------------------------------------|-----------------|
| Informations générales sur le système/RAC        | getsysinfo      |
| Informations sur les sessions                    | getssninfo      |
| Informations du capteur                          | getsensorinfo   |
| Informations du commutateur (module d'E/S)       | getioinfo       |
| Informations de la carte mezzanine (carte fille) | getdcinfo       |
| Informations de tous les modules                 | getmodinfo      |
| Informations du bilan de puissance               | getpbinfo       |
| Informations 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 (base d'information de gestion) SNMP

Le fichier MIB SNMP CMC définit les types de châssis, les événements et les indicateurs. Le contrôleur CMC permet de télécharger le fichier MIB en utilisant 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 de gauche, cliquez sur **Présentation du châssis** → **Réseau** → **Services** → **SNMP**.
2. Dans la section **Configuration SNMP**, cliquez sur **Enregistrer** pour télécharger le fichier **MIB** CMC vers le système local.

Pour plus d'informations sur le fichier **MIB** SNMP, voir le document *Dell OpenManage Server Administrator SNMP Reference Guide* (Guide de référence SNMP de Dell OpenManage Server Administrator) sur le site [dell.com/support/manuals](http://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 de temps du réseau (NTP)

Après la configuration du CMC pour qu'il synchronise son horloge avec un serveur de temps distant sur le réseau, il peut s'écouler 2 à 3 minutes avant que la date et l'heure ne soient modifiées. Si aucun changement ne s'est produit après ce délai, il existe peut-être un problème que vous devez corriger. Le CMC ne peut pas synchroniser son horloge dans les circonstances suivantes :

- Problème des paramètres Serveur NTP 1, Serveur NTP 2 et 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 NTP, consultez les informations du journal de trace CMC. Ce journal contient un message d'erreur pour les échecs NTP. Si le contrôleur CMC ne peut se synchroniser avec aucun des serveurs NTP distants configurés, l'horloge du contrôleur CMC est synchronisée avec l'horloge du système local et le journal de trace contient 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 gettractime -n
```


Si l'astérisque (\*) n'apparaît pas pour l'un des serveurs configurés, ses paramètres sont peut-être incorrects. La sortie de cette commande contient des statistiques NTP détaillées très utiles pour la résolution des problèmes.

Si vous tentez de configurer un serveur NTP Windows, il peut être judicieux d'augmenter la valeur du paramètre `MaxDist` pour `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 Utilisation de la console de diagnostic.

## Interprétation des couleurs des LED et séquences de clignotement

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

- Une LED orange clignotant sur un module indique une panne de ce module.
- Les voyants bleus clignotant peuvent être configurés par l'utilisateur et utilisés à des fins d'identification. Pour plus d'informations sur la configuration, voir [CMC\\_Stmp\\_Configuration des voyants pour l'identification des composants du châssis](#).

**Tableau 17. Couleur des LED et séquences de clignotement**

| Composant              | Couleur de la LED, séquence de clignotement | Condition                                           |
|------------------------|---------------------------------------------|-----------------------------------------------------|
| CMC                    |                                             | Sous tension                                        |
|                        |                                             | Micrologiciel en cours de téléversement             |
|                        |                                             | Hors tension                                        |
|                        | Bleu, continu                               | Actif                                               |
|                        | Bleu, clignotant                            | Identificateur d'un module activé par l'utilisateur |
| Serveur                | Orange, continu                             | Inutilisé                                           |
|                        | Orange, clignotant                          | Panne                                               |
|                        |                                             | Sous tension                                        |
|                        |                                             | Micrologiciel en cours de téléversement             |
|                        |                                             | Hors tension                                        |
| Module d'E/S (courant) | 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                     |

| Composant                | Couleur de la LED, séquence de clignotement | Condition                                                            |
|--------------------------|---------------------------------------------|----------------------------------------------------------------------|
| 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                                                         |
| Fan (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                                                            |
| le bloc d'alimentation   | (Ovale) Vert, continu                       | Alimentation en courant alternatif OK                                |
|                          | (Ovale) Vert, clignotant                    | Inutilisé                                                            |
|                          | (Ovale) Vert, foncé                         | Alimentation en courant alternatif défailante                        |
|                          | 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 défailante                           |
| PCI                      | Bleu, foncé                                 | Sous tension                                                         |
|                          | Bleu, clignotant                            | L'identification PCI est en cours.                                   |
|                          | Orange, clignotant                          | 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 :

| 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>

## 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

### 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 sslcsrigen [-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](http://www.dell.com/openmanagemanuals).