Micrologiciel Dell Chassis Management Controller Guide d'utilisation Version 4.3

Remarques, précautions et avertissements

REMARQUE : Une REMARQUE indique des informations importantes qui peuvent vous aider à mieux utiliser l'ordinateur.

PRÉCAUTION : Une PRÉCAUTION indique un risque de dommage matériel ou de perte de données et vous indique comment éviter le problème.

AVERTISSEMENT : Un AVERTISSEMENT indique un risque d'endommagement du matériel, de blessure corporelle ou de mort.

2012 - 12

Rev. A00

Table des matières

1

Présentation

Dell Chassis Management Controller (CMC) est une solution matérielle et logicielle de gestion des systèmes conçue pour gérer plusieurs châssis à lames Dell. Il s'agit d'un module enfichable à chaud installé à l'arrière du châssis Dell PowerEdge M1000e. Le CMC possède son propre microprocesseur et sa propre mémoire, et est alimenté par le châssis modulaire où il est installé.

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

- Affichage de l'inventaire
- Exécution de tâches de configuration et de surveillance
- Allumage ou extinction de lames à distance
- Activation d'alertes pour les événements des serveurs et composants du châssis à lames

Vous pouvez configurer le châssis M1000e à l'aide d'un seul CMC ou de modules CMC redondants. Dans les configurations avec CMC redondants, si le CMC principal perd la communication avec le châssis M1000e ou le réseau de gestion, le CMC de secours se charge de la gestion du châssis.

Le CMC offre plusieurs fonctions de gestion des systèmes conçues pour les serveurs lames. Ses fonctions principales sont la gestion de l'alimentation et de la température.

- Gestion automatique des températures et de la consommation au niveau du châssis et en temps réel.
  - CMC surveille les besoins en alimentation du système et prend en charge l'utilisation (facultative) du mode DPSE (Dynamic Power Supply Engagement - Enclenchement dynamique des blocs d'alimentation). Ainsi, le CMC peut activer les blocs d'alimentation ou les mettre en veille en fonction de la charge de travail et des besoins de redondance, pour une consommation électrique mieux contrôlée.
  - CMC donne des informations en temps réel sur la consommation, avec une consignation des limites haute et basse accompagnée d'un horodatage.
  - CMC prend en charge la définition d'un seuil d'alimentation (facultatif) qui permet de générer une alerte ou de déclencher certaines actions visant à maintenir la consommation en dessous d'un niveau donné : basculement des modules serveurs dans un mode de consommation réduite et/ou désactivation de la mise sous tension de nouveaux serveurs lames, etc.
  - CMC surveille et contrôle automatiquement le fonctionnement des ventilateurs en se basant sur la mesure en temps réel des températures ambiantes et internes.
  - CMC comporte des fonctions complètes d'inventaire et de consignation des erreurs ou des états.
- CMC permet de centraliser la configuration des paramètres suivants :
  - Paramètres réseau et de sécurité du châssis M1000e
  - Redondance de l'alimentation et définition de seuils
  - Paramètres réseau des commutateurs d'E/S et du module iDRAC
  - Définition du premier périphérique d'amorçage sur les serveurs lames
  - CMC vérifie la cohérence des infrastructures d'E/S entre les modules d'E/S et les serveurs lames. Si nécessaire, il désactive des composants afin de protéger le matériel du système.
  - Sécurité des accès utilisateur

Vous pouvez configurer CMC pour envoyer des alertes par courrier électronique ou des alertes d'interruption SNMP en cas d'avertissements ou d'erreurs liés à la température, aux problèmes de configuration matérielle, aux coupures de courant et aux vitesses de ventilateur.

Nouveautés de cette version

Cette version de CMC prend en charge :

- Commutateur Cisco FEX
- Commutateur FC16 - Brocade M6505
- Cartes mezzanine
  - QLogic FC16 2P QME2662
  - Emulex FC16 LPm16002B-D
- Capacité de mise à jour du micrologiciel indépendante du SE, sans agent un-à-plusieurs pour les cartes mezzanine Fibre Channel (FC) 12 G prises en charge
- Mise à jour de micrologiciel pour Dell PowerEdge M I/O Aggregator
- Enregistrement des informations de configuration du BIOS sur le disque dur et restauration des informations sur le même serveur ou un autre serveur.
- Configuration des matrices lames Dell EqualLogic PS M4110 à l'aide de RACADM
- Gestion de plusieurs châssis :
  - possibilité de sélectionner les propriétés de configuration du châssis à partir du châssis maître et de les propager aux membres du groupe
  - possibilité de synchroniser les paramètres de châssis des membres du groupe avec le châssis maître
- Affichage de l'indication que le châssis est conforme aux normes d'air frais. Le terme « Air frais » est affiché après le nom du modèle.
- Réinitialisation d'iDRAC sans avoir à redémarrer le système d'exploitation.

Principales fonctions

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

Fonctions de gestion

CMC offre les fonctionnalités de gestion suivantes :

- Environnement CMC redondant
- Enregistrement DDNS (Système de noms de domaine dynamique) pour IPv4 et IPv6
- Gestion et surveillance à distance du système à l'aide de SNMP, d'une interface Web, d'un module iKVM 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 CMC
- Mises à jour du micrologiciel pour différents composants de châssis : permettent de mettre à jour le micrologiciel du CMC, des serveurs, du module iKVM et des dispositifs d'infrastructure de module d'E/S.
- Mise à jour micrologicielle de composants de serveurs entre autres le BIOS, les contrôleurs de réseau, les contrôleurs de stockage, 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'IT Assistant.

- Alertes CMC : vous avertit des problèmes potentiels du nœud géré au moyen d'un message électronique ou d'une interruption SNMP.
- Gestion de l'alimentation à distance : offre des fonctionnalités de gestion de l'alimentation à distance, comme l'arrêt et la réinitialisation de n'importe quel composant 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 Integrated Dell Remote Access Controller (iDRAC).
- Prise en charge de la gestion WS
- 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
- L'Assistant Configuration iDRAC LCD prend en charge la configuration réseau iDRAC
- Connexion unique iDRAC
- Prise en charge du protocole NTP
- Pages de résumé du serveur, de rapports de l'alimentation et de contrôle de l'alimentation optimisées
- Basculement CMC forcé et réattribution de sièges virtuelle de serveurs
- Réinitialisation d'iDRAC sans avoir à redémarrer le système d'exploitation.
- Gestion de plusieurs châssis. Celle-ci permet à jusqu'à huit autres châssis d'être visibles depuis le châssis maître.
- Prise en charge de la configuration de réseau de stockage via RACADM : vous permet de configurer IP, de rejoindre ou créer un groupe, et de sélectionner une structure de matrices de stockage à l'aide de RACADM.
- Gestion de plusieurs châssis :
  - possibilité de sélectionner les propriétés de configuration du châssis à partir du châssis maître et de les propager aux membres du groupe
  - possibilité de synchroniser les paramètres de châssis des membres du groupe avec le châssis maître
- Prise en charge de l'enregistrement des informations de configuration du BIOS sur le disque dur et de leur restauration sur le même serveur ou un autre serveur.

Fonctionnalités de sécurité

CMC dispose des fonctionnalités de sécurité suivantes :

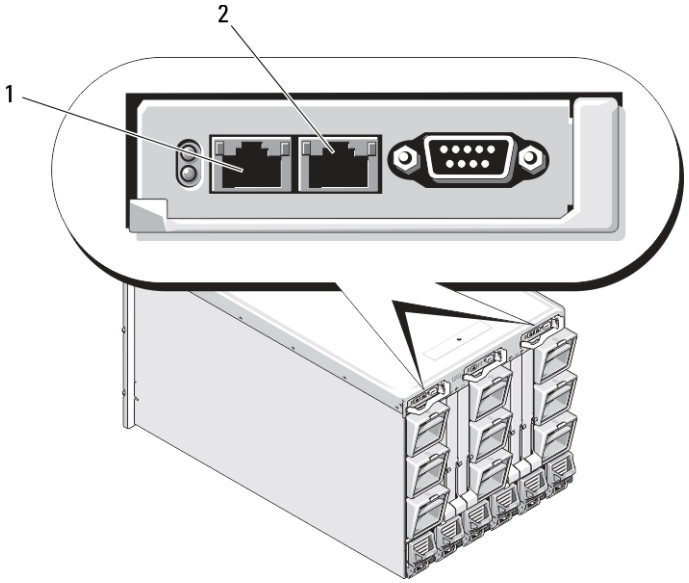
- Gestion de la sécurité au niveau des mots de passe : empêche tout accès non autorisé à un système distant.
- Authentification utilisateur centralisée via :
  - Active Directory, à l'aide d'un schéma standard ou d'un schéma étendu (facultatif).
  - Identifiants et mots de passe utilisateur stockés dans le matériel.
- Autorité basée sur le rôle qui permet à un administrateur de configurer des privilèges spécifiques pour chaque utilisateur
- Configuration des ID utilisateur et des mots de passe via l'interface Web
- L'interface Web prend en charge le cryptage SSL 128 bits et 40 bits 3.0 (pour les pays où le 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 à CMC
- Secure Shell (SSH) qui utilise une couche cryptée pour une sécurité plus élevée
- Connexion directe, authentification bifactorielle et authentification par clé publique

Présentation du châssis

La figure suivante montre la vue de face d'un CMC (en insert) et l'emplacement des logements CMC dans le châssis.



1	Port GB
2	Port STK

Informations sur les ports CMC

Les ports TCP/IP suivants sont nécessaires pour accéder à distance à CMC à travers des pare-feux. Il s'agit des ports sur lesquels CMC écoute les connexions.

Tableau 1. Ports d'écoute de serveur CMC

Numéro de port	Fonction
22*	SSH
23*	Telnet
80*	HTTP
161	Agent SNMP
443*	HTTPS

* Port configurable

Le tableau suivant répertorie les ports que CMC utilise en tant que client.

Tableau 2. Port de client CMC

Numéro de port	Fonction
25	SMTP
53	DNS
68	Adresse IP attribuée par DHCP
69	TFTP
162	Interruption SNMP
514*	Syslog distant
636	LDAPS
3 269	LDAPS pour le catalogue global (CG)

* Port configurable

Version CMC minimale

Le tableau suivant affiche la version CMC minimale requise pour prendre en charge les serveurs lames répertoriés.

Tableau 3. Version CMC minimale pour les serveurs lames

Serveurs	Version minimale de CMC
PowerEdge M600	CMC 1.0
PowerEdge M605	CMC 1.0
PowerEdge M805	CMC 1.2
PowerEdge M905	CMC 1.2
PowerEdge M610	CMC 2.0
PowerEdge M610x	CMC 3.0
PowerEdge M710	CMC 2.0
PowerEdge M710HD	CMC 3.0
PowerEdge M910	CMC 2.3
Power Edge M915	CMC 3.2
PowerEdge M420	CMC 4.1
PowerEdge M520	CMC 4.0
PowerEdge M620	CMC 4.0
PowerEdge M820	CMC 4.11
PowerEdge PSM4110	CMC 4.11

Le tableau suivant affiche la version CMC minimale requise pour prendre en charge les IOM répertoriés.

Tableau 4. Version CMC minimale pour les IOM

Commutateurs IOM	Version minimale de CMC
PowerConnect M6220	CMC 1.0
PowerConnect M6348	CMC 2.1
PowerConnect M8024	CMC 1.2
PowerConnect M8024-k	CMC 3.2
PowerConnect M8428-k	CMC 3.1
Module d'intercommunication Ethernet 10/100/1000 Mbits Dell	CMC 1.0
Module d'intercommunication FC 4 Gb/s Dell	CMC 1.0
Module SAN FC 8/4 Gb/s Dell	CMC 1.2
Module d'intercommunication Ethernet 10 Gbits Dell	CMC 2.1
Module d'intercommunication II Ethernet 10 Gbits Dell	CMC 3.0
Module d'intercommunication -K Ethernet 10 Gbits Dell	CMC 3.0
Brocade M4424	CMC 1.0
Brocade M5424	CMC 1.2
Cisco Catalyst CBS 3130X-S	CMC 1.0
Cisco Catalyst CBS 3130G	CMC 1.0
Cisco Catalyst CBS 3032	CMC 1.0
Dell Force10 MXL 10/40 GbE	CMC 4.11
Dell PowerEdge M I/O Aggregator	CMC 4.2
Commutateur Mellanox M2401G DDR Infiniband	CMC 1.0
Commutateur Mellanox M3601Q QDR Infiniband	CMC 2.0
Commutateur Mellanox M4001F/M4001Q FDR/QDR Infiniband	CMC 4.0
Commutateur Mellanox M4001T FDR10 Infiniband	CMC 4.1
Brocade M6505	CMC 4.3
Cisco Nexus B22DELL	CMC 4.3

Connexions d'accès à distance prises en charge

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

Tableau 5. Connexions d'accès à distance prises en charge

Connexion	Fonctions
Ports d'interface réseau CMC	• Port GB : interface réseau dédiée pour l'interface Web CMC. Deux ports 10/100/1 000 Mbits/s ; un pour la gestion et l'autre pour le regroupement des câbles de châssis à châssis. • STK : port Uplink pour consolation câble réseau de gestion châssis à châssis

Connexion	Fonctions
	• Ethernet 10 Mbits/100 Mbits/ 1 Mbits sur port GbE CMC • Prise en charge de DHCP • Interruptions SNMP et notifications d'événements par e-mail • Interface réseau pour le micrologiciel iDRAC et les modules d'E/S • Prise en charge de la console de commande Telnet/SSH et des commandes CLI RACADM, y compris les commandes de démarrage du système, de réinitialisation, de mise sous tension et d'arrêt
Port série	• Prise en charge de la console série et des commandes d'interface de ligne de commande (CLI) RACADM, y compris les commandes d'amorçage, de réinitialisation, d'allumage et d'arrêt 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).
Autres connexions	• Accès à la console Dell CMC via le module de commutation KVM intégré (iKVM) Avocent

Plates-formes prises en charge

Le CMC prend en charge les systèmes modulaires conçus pour la plate-forme M1000e. Pour plus d'informations sur la compatibilité avec le CMC, voir la documentation de votre périphérique.

Pour connaître les dernières plates-formes prises en charge, voir le document *Readme* (Lisez-moi) sur **dell.com/support/manuals**.

Navigateurs Web pris en charge

Pour obtenir les dernières informations sur les navigateurs Web pris en charge, voir le document *Readme* (Lisez-moi) sur **dell.com/support/manuals**.

Affichage des versions traduites de l'interface Web CMC

Pour afficher les versions traduites de l'interface Web CMC :

1. Ouvrez le **Panneau de configuration** Windows.
2. Double-cliquez sur l'icône **Options régionales**.
3. Sélectionnez les paramètres régionaux voulus dans le menu déroulant **Paramètres régionaux (emplacement)**.

Applications de console de gestion prises en charge

Le CMC prend en charge l'intégration à Dell OpenManage IT Assistant. Pour plus d'informations, voir la documentation IT Assistant, disponible sur le site Web du support Dell, à l'adresse **dell.com/support/manuals**.

Autres documents utiles

En plus de ce guide, vous pouvez accéder aux guides suivants à partir de **dell.com/support/manuals**. Sélectionnez **Choisissez à partir d'une liste de tous les produits Dell** et cliquez sur **Continuer**. Cliquez sur **Logiciel → Moniteurs → Électronique & Périphériques → Logiciel** :

- Cliquez sur **Gestion de système d'entreprise à distance** puis cliquez sur **Dell Chassis Management Controller Version 4.3** pour afficher ce qui suit :
  - L'*Aide en ligne de CMC* fournit des informations sur l'utilisation de l'interface Web.
  - Le document « *Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification* » (Spécifications techniques de la carte Secure Digital (SD) de Chassis Management Controller (CMC)) donne des informations sur la version minimale du BIOS et du micrologiciel, leur installation et leur utilisation.
  - Le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) fournit des informations sur les sous-commandes RACADM, les interfaces prises en charge, les groupes de bases de données des propriétés et les définitions d'objets.
  - Le document « *Chassis Management Controller Version 4.3 Release Notes* » (Notes de publication de Chassis Management Controller Version 4.3) fournit des mises à jour de dernière minute sur le système ou la documentation ou des informations techniques avancées destinées aux utilisateurs expérimentés ou aux techniciens.
- Cliquez sur **Gestion de système d'entreprise à distance** puis cliquez sur le numéro de version iDRAC7 requis pour afficher le manuel « *Integrated Dell Remote Access Controller 7 (iDRAC7) User's Guide* » (Guide d'utilisation d'Integrated Dell Remote Access Controller 7 (iDRAC7)), qui fournit des informations sur l'installation, la configuration et la maintenance d'iDRAC sur les systèmes gérés.
- Cliquez sur **Gestion de système d'entreprise** puis cliquez sur le nom du produit pour afficher les documents suivants :
  - 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.

Les documents suivants disponibles sur **dell.com/support/manuals** fournissent plus d'informations sur le système sur lequel CMC 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.
- Les documents *Guide d'installation du rack* et *Instructions d'installation du rack* fournis avec la solution rack décrivent l'installation du système.
- Le manuel « *Hardware Owner's Manual* » (Manuel du propriétaire du matériel) présente les caractéristiques du système et contient des informations de dépannage, ainsi que des instructions d'installation ou de remplacement des composants.
- 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 notes de mise à jour ou les fichiers « Lisez-moi » éventuellement fournis contiennent des mises à jour de dernière minute apportées au système ou à la documentation ou bien des informations techniques avancées destinées aux utilisateurs expérimentés ou aux techniciens.
- Pour plus d'informations sur les paramètres réseau des modules d'E/S (IOM), reportez-vous au document « *Dell PowerConnect M6220 Switch Important Information* » (Informations importantes sur le commutateur Dell PowerConnect M6220) et au livre blanc « *Dell PowerConnect 6220 Series Port Aggregator* » (Agrégation de ports Dell PowerConnect série 6220).
- Documentation spécifique à votre application tierce de console de gestion.

Des documents de mise à jour sont parfois inclus 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.

2

Installation et configuration de CMC

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

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

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

Avant de commencer

Préalablement à la configuration de votre environnement CMC, téléchargez la dernière version du micrologiciel CMC depuis le site Web de support de Dell à l'adresse **support.dell.com**.

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

Installation du matériel CMC

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

Liens connexes

Fonctionnement de l'environnement CMC redondant

Liste de contrôle pour la configuration du châssis

Les étapes suivantes vous 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 par câble le port du CMC étiqueté **GB** et le réseau de gestion.

   REMARQUE : Ne branchez aucun câble sur le port Ethernet du CMC étiqueté **STK**. Pour plus d'informations sur le câblage du port STK, voir « Fonctionnement de l'environnement CMC redondant ».
2. Installez les modules d'E/S dans le châssis et reliez-les.
3. Insérez les serveurs dans le châssis.
4. Connectez le châssis à la source d'alimentation.
5. Appuyez sur le bouton d'alimentation, dans l'angle inférieur gauche du châssis ou allumez le châssis depuis l'interface Web CMC après avoir terminé l'étape 7.

   REMARQUE : N'allumez pas les serveurs.
6. À l'aide du panneau LCD sur l'avant du système, fournissez à CMC une adresse IP statique ou DHCP.

7. Connectez-vous à l'adresse IP du CMC via le navigateur Web en utilisant le nom d'utilisateur (root) et le mot de passe (Calvin) par défaut.
8. Attribuez une adresse IP à chaque iDRAC dans l'interface Web CMC, puis activez l'interface LAN et IPMI.

   REMARQUE : L'interface LAN iDRAC de certains serveurs est désactivée par défaut.
9. Attribuez une adresse IP à chaque module d'E/S (IOM) dans l'interface Web CMC.
10. Connectez-vous à chaque iDRAC par l'intermédiaire du navigateur Web et fournissez la configuration finale de l'iDRAC. Le nom d'utilisateur et le mot de passe par défaut sont *root* et *calvin*.
11. Connectez-vous à chaque module d'E/S par l'intermédiaire du navigateur Web et fournissez la configuration finale du module d'E/S.
12. Mettez sous tension les serveurs et installez le système d'exploitation.

Connexion réseau CMC de base

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

Chaque CMC possède deux ports Ethernet RJ-45, libellés **GB** (port de liaison montante) et **STK** (port d'empilage ou de regroupement des câbles). Pour le câblage de base, vous connectez le port GB sur le réseau de gestion et le port STK reste inutilisé.

PRÉCAUTION : Il est possible que vous obteniez des résultats imprévisibles lorsque vous connecterez le port STK au réseau de gestion. Le câblage des ports GB et STK au même réseau (domaine de diffusion) peut provoquer une perturbation importante de la diffusion.

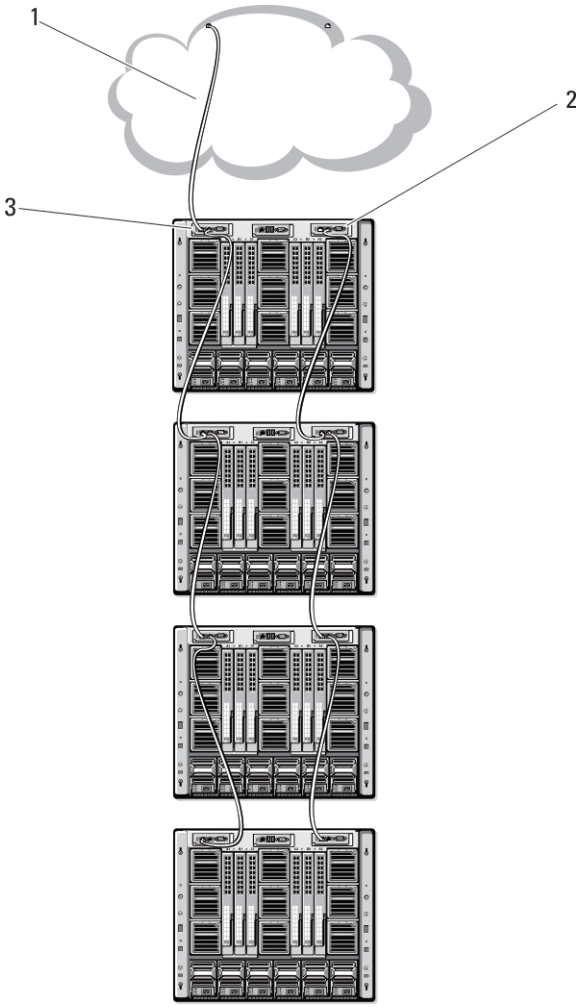
Connexions réseau CMC en chaîne

Si vous avez plusieurs châssis dans un rack, vous pouvez réduire le nombre de connexions au réseau de gestion en reliant jusqu'à quatre châssis par connexion en série. Si chacun des quatre châssis contient un module CMC redondant, le fait de les relier par connexion en série permet de réduire le nombre de connexions réseau de gestion de huit à deux. Si chaque châssis ne comporte qu'un seul module CMC, vous pouvez réduire les connexions nécessaires de quatre à une seule.

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

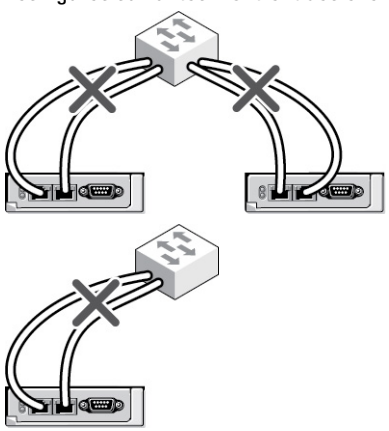
Créez des chaînes distinctes pour les contrôleurs CMC des logements CMC principal et secondaire.

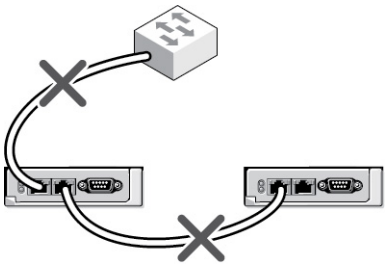
L'illustration suivante représente l'organisation des câbles de quatre châssis connectés en série, chacun comportant un module CMC actif et un module de secours.



1	Réseau de gestion
2	CMC de secours
3	CMC actif

Les figures suivantes montrent des exemples de câblage incorrect du CMC.





Pour mettre quatre châssis en chaîne :

1. Connectez le port GB du CMC actif du premier châssis sur le réseau de gestion.
2. Connectez le port GB du CMC actif du second châssis sur le port STK du CMC actif du premier châssis.
3. Si vous disposez d'un troisième châssis, connectez le port GB de son CMC actif sur le port STK du CMC actif du deuxième châssis.
4. Si vous disposez d'un quatrième châssis, connectez le port GB de son CMC actif sur le port STK du troisième châssis.
5. Si vous disposez de CMC redondants dans le châssis, connectez-les selon le même modèle.

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

   REMARQUE : Ne branchez jamais un CMC actif sur un CMC de secours.

   REMARQUE : La réinitialisation d'un CMC dont le port STK est connecté en chaîne sur un autre CMC peut perturber le réseau pour les CMC situés en aval de la chaîne. Les CMC enfants peuvent journaliser des messages signalant que la liaison réseau a été perdue, et ils peuvent basculer sur leurs CMC redondants.
6. Pour vos premiers pas avec CMC, voir « Installation de logiciel d'accès à distance sur une station de gestion ».

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

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

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

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

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

Installation de RACADM sur une station de gestion Linux

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

   REMARQUE : Sous le système d'exploitation Red Hat Enterprise Linux 5, les DVD sont montés automatiquement avec l'option de montage `–noexec mount`. Cette option ne permet pas d'exécuter des fichiers exécutables à partir du DVD. Vous devez monter le DVD-ROM manuellement, puis exécuter les fichiers exécutables.
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 sur la commande RACADM, entrez `racadm help` après avoir exécuté les commandes précédentes. Pour plus d'informations sur RACADM, voir le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de l'interface de ligne de commande RACADM pour iDRAC7 et CMC).

   REMARQUE : Lors de l'utilisation des fonctionnalités distantes de 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 <nom de fichier>`.

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

1. Ouvrez une session en tant que root sur le système sur lequel vous souhaitez désinstaller les fonctionnalités de Management Station.
2. Utilisez la commande de requête rpm pour déterminer la version installée des outils DRAC :

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

Configuration du navigateur Web

Vous pouvez configurer et gérer CMC, les serveurs et les modules installés sur le châssis par le biais d'un navigateur Web. Voir la section *Supported Browsers* (Navigateurs pris en charge) dans le document *Readme* (Lisez-moi) sur **dell.com/support/manuals**.

Le CMC et la station de gestion où vous utilisez votre navigateur doivent se trouver sur le même réseau, appelé *réseau de gestion*. Selon vos besoins en matière de sécurité, le réseau de gestion peut être un réseau isolé hautement sécurisé.

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

Certaines fonctions du navigateur peuvent interférer avec les connexions ou les performances, en particulier si le réseau de gestion n'a pas d'accès à Internet. Si votre 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.

Liens connexes

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.

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**, 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 version 3.0 :

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

Filtre anti-hameçonnage de Microsoft

Si vous activez la fonction Filtre anti-hameçonnage Microsoft dans Internet Explorer 7 sur votre système de gestion et si votre CMC n'a pas d'accès à Internet, l'accès à CMC peut être retardé de quelques secondes. Ce retard se produit lorsque vous utilisez le navigateur ou une autre interface comme le RACADM distant. Procédez comme suit pour désactiver le filtre anti-hameçonnage :

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

Récupération de la liste de révocation des certificats (CRL)

Si votre CMC ne possède aucune route vers Internet, désactivez la fonction d'extraction de liste de révocation de certificat (CRL) dans Internet Explorer. Cette fonction vérifie si un serveur, comme le serveur Web CMC, utilise un

certificat figurant sur une liste de certificats révoqués récupérée sur Internet. Si Internet est inaccessible, cette fonctionnalité peut provoquer un retard de plusieurs secondes lorsque vous accédez au CMC avec le navigateur ou avec une interface de ligne de commande (CLI) comme le RACADM distant.

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

1. Démarrez Internet Explorer.
2. Cliquez sur **Outils** → **Options Internet**, puis cliquez sur **Avancé**.
3. Faites défiler la liste jusqu'à la section Sécurité et désélectionnez la case à cocher **Vérifier la révocation des certificats de l'éditeur**, puis cliquez sur **OK**.

Téléchargement de fichiers à partir de CMC dans Internet Explorer

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

Suivez les étapes suivantes pour activer l'option **Ne pas enregistrer les pages cryptées sur le disque** :

1. Démarrez Internet Explorer.
2. Cliquez sur **Outils** → **Options Internet**, puis cliquez sur **Avancé**.
3. Faites défiler l'affichage jusqu'à la section Sécurité et cochez la case **Ne pas enregistrer les pages cryptées sur le disque**.

Autorisation des animations dans Internet Explorer

Lorsque vous transférez des fichiers vers et depuis l'interface Web, une icône de transfert de fichiers tourne pour montrer l'activité de transfert. Dans Internet Explorer, cela nécessite que vous configuriez le navigateur pour lire les animations (ce qui est le paramètre par défaut).

Pour configurer Internet Explorer pour la lecture d'animations :

1. Démarrez Internet Explorer.
2. Cliquez sur **Outils** → **Options Internet**, puis cliquez sur **Avancé**.
3. Faites défiler la liste des paramètres jusqu'à la section Multimédia, puis cochez l'option **Lire les animations dans les pages Web**.

Configuration de l'accès initial à CMC

Pour la gestion à distance de CMC, connectez CMC sur votre réseau de gestion, puis configurez les paramètres réseau CMC.

REMARQUE : Pour que vous puissiez gérer la solution M1000e, elle doit être connectée à votre réseau de gestion.

Pour plus d'informations sur la configuration des paramètres réseau CMC, voir « Configuration initiale du réseau CMC ». Cette configuration initiale définit les paramètres réseau TCP/IP qui permettent l'accès à CMC.

Le CMC et l'iDRAC de chaque serveur, ainsi que les ports de gestion de chaque module d'E/S, sont connectés à un réseau interne commun dans le châssis M1000e. Cela permet d'isoler le réseau de gestion du réseau de données serveur. Il est important de séparer ce trafic pour garantir l'accès ininterrompu à la gestion du châssis.

Le CMC est connecté au réseau de gestion. Tout accès externe au CMC et aux iDRAC se produit via le CMC. Par contre, l'accès aux serveurs gérés est effectué via des connexions réseau aux modules d'E/S (IOM). Cela permet d'isoler le réseau d'applications du réseau de gestion.

Il est recommandé d'isoler la gestion du châssis et le réseau de données. Dell ne peut pas prendre en charge un châssis mal intégré dans votre environnement et ne peut pas garantir son temps d'activité. 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 du CMC et de l'iDRAC. Ces retards provoquent un comportement imprévisible du châssis : le CMC peut par exemple indiquer que l'iDRAC est hors ligne alors que ce dernier est en ligne et en cours d'exécution. 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 CMC et les différentes interfaces réseau iDRAC peuvent être configurés pour utiliser un VLAN.

Si vous utilisez un seul châssis, connectez le CMC actif et le CMC de secours au réseau de gestion. Si vous utilisez un CMC redondant, utilisez un câble réseau différent et branchez le port **GB** du CMC sur un deuxième port du réseau de gestion.

Si vous utilisez plusieurs châssis, vous pouvez choisir entre la connexion de base (chaque CMC est branché sur le réseau de gestion) et la connexion de châssis en chaîne (les châssis sont connectés en série et un seul CMC est branché sur le réseau de gestion). Le type Connexion de base utilise plus de ports sur le réseau de gestion et fournit une meilleure redondance. Le type Connexion en chaîne utilise moins de ports sur le réseau de gestion mais crée des dépendances entre les CMC, ce qui réduit la redondance du système.

REMARQUE : Un câblage incorrect du contrôleur CMC dans une configuration redondante peut entraîner la perte de la gestion et créer des perturbations importantes de la diffusion.

Liens connexes

Connexion réseau CMC de base
Connexions réseau CMC en chaîne
Configuration du réseau CMC initial

Configuration du réseau CMC initial

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

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

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

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

- Interfaces de ligne de commande (CLI) comme la console série, Telnet, SSH ou la console CMC Dell via iKVM
- Interface RACADM distante
- Interface Web CMC

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

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

REMARQUE : L'option de configuration de CMC avec le panneau LCD est disponible uniquement jusqu'au déploiement de CMC ou jusqu'au changement de mot de passe. Si le mot de passe n'est pas modifié, vous pouvez continuer à utiliser le LCD pour reconfigurer le CMC, ce qui représente un risque potentiel pour la sécurité.

Le panneau LCD se trouve dans l'angle inférieur gauche à l'avant du châssis.

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

1. Appuyez sur le bouton d'alimentation du châssis pour l'allumer.

   L'écran LCD affiche une série d'écrans d'initialisation pendant sa mise sous tension. Lorsqu'il est prêt, l'écran **Configuration de la langue** s'affiche.

2. Sélectionnez une langue avec les boutons fléchés, appuyez sur le bouton central pour sélectionner **Accepter/Oui**, puis appuyez de nouveau sur le bouton central.

   L'écran **Enceinte** apparaît et affiche la question suivante : **Configurer l'enceinte ?**.

   - Appuyez sur le bouton central pour passer à l'écran **Paramètres réseau** de CMC. Voir étape 4.
   - Pour quitter le menu **Configurer l'enceinte**, sélectionnez l'icône NON et appuyez sur le bouton central. Voir l'étape 9.

3. Appuyez sur le bouton central pour passer à l'écran **Paramètres réseau** de CMC.
4. Sélectionnez la vitesse de votre réseau (10 Mbits/s, 100 Mbits/s, Automatique (1 Gbit/s)) avec le bouton Bas.

   Le paramètre Vitesse réseau doit correspondre à votre configuration réseau pour que le débit réseau soit efficace. Si vous choisissez une vitesse réseau inférieure à celle de votre configuration réseau, cela augmente la consommation de bande passante et ralentit les communications réseau. **Déterminez si votre réseau prend en charge les vitesses réseau ci-dessus et configurez-le en conséquence**. Si la configuration réseau ne correspond à aucune de ces valeurs, il est recommandé d'utiliser la négociation automatique (option **Automatique**). Vous pouvez également contacter le fabricant de votre équipement réseau.

   Appuyez sur le bouton central pour passer à l'écran **Paramètres réseau CMC** suivant.

5. Sélectionnez le mode duplex (semi-duplex ou duplex intégral) qui correspond à votre environnement réseau.

   REMARQUE : Les paramètres de la vitesse réseau et du mode duplex ne sont pas disponibles lorsque l'option de négociation automatique est activée ou qu'une vitesse de 1 000 Mo (1 Gbit/s) est sélectionnée.

   Si la négociation automatique est activée pour un périphérique mais pas pour l'autre, le périphérique qui utilise la négociation automatique peut déterminer la vitesse réseau de l'autre périphérique, mais pas son mode duplex ; dans ce cas, le système utilise le mode duplex par défaut, à savoir Semi-duplex, lors de la négociation automatique. Cette incohérence du mode duplex ralentit la connexion réseau.

   Appuyez sur le bouton central pour passer à l'écran **Paramètres réseau CMC** suivant.

6. Sélectionnez le protocole Internet (IPv4, IPv6 ou les deux) à utiliser avec CMC, puis appuyez sur le bouton central pour passer à l'écran **Paramètres réseau CMC** suivant.
7. Sélectionnez le mode dans lequel CMC doit obtenir les adresses IP des cartes réseau (NIC) :

DHCP (Dynamic Host Configuration Protocol - Protocole de configuration dynamique des hôtes)	CMC récupère automatiquement la configuration IP (adresse IP, masque et passerelle) depuis un serveur DHCP de votre réseau. CMC reçoit une adresse IP unique, attribuée sur votre réseau. Si vous avez activé l'option DHCP, appuyez sur le bouton central. L'écran **Configurer iDRAC7** s'affiche. Passez à l'étape 9.
Statique	Vous devez entrer manuellement l'adresse IP, la passerelle et le masque de sous-réseau dans les écrans qui suivent. Si vous avez sélectionné l'option Statique, appuyez sur le bouton central pour passer à l'écran **Paramètres réseau CMC** suivant, puis : – Définissez l'**adresse IP statique**. Utilisez les touches Gauche ou Droite pour changer de position, puis les flèches Haut et Bas pour sélectionner un numéro pour chaque position. Lorsque vous avez fini de définir l'**adresse IP statique**, appuyez sur le bouton central pour continuer. – Définissez le masque de sous-réseau, puis appuyez sur le bouton central. – Définissez la passerelle, puis appuyez sur le bouton central. L'écran **Récapitulatif réseau** s'affiche.

L'écran **Récapitulatif réseau** répertorie l'**adresse IP statique**, le **masque de sous-réseau** et la **passerelle** que vous avez définis. Vérifiez que ces paramètres sont corrects. Pour corriger une entrée, naviguez avec le bouton Gauche, puis appuyez sur le bouton central pour revenir à l'écran de ce paramètre. Après la correction, appuyez sur le bouton central.

– Lorsque vous avez vérifié que les paramètres entrés sont corrects, appuyez sur le bouton central. L'écran **Enregistrer DNS ?** s'affiche.

REMARQUE : Si le mode DHCP (Protocole de configuration dynamique des hôtes) est sélectionné pour la configuration IP CMC, l'enregistrement DNS est alors également activé par défaut.

8. Si vous avez sélectionné **DHCP** à l'étape précédente, passez à l'étape 10.

   Pour enregistrer l'adresse IP de votre serveur DNS, appuyez sur le bouton central pour continuer. Si vous n'avez pas de DNS, appuyez sur la touche Droite. L'écran **Enregistrer DNS ?** s'affiche. Passez à l'étape 10.

   Définissez l'**adresse IP DNS**. Utilisez les touches Gauche ou Droite pour changer de position, puis les flèches Haut et Bas pour sélectionner un numéro pour chaque position. Lorsque vous avez fini de définir l'adresse IP DNS, appuyez sur le bouton central pour continuer.

9. Indiquez si vous souhaitez configurer l'iDRAC :

   – **Non** : passez à l'étape 13.
   – **Oui** : appuyez sur le bouton central pour continuer.

   Vous pouvez également configurer iDRAC depuis l'interface utilisateur CMC.

10. Sélectionnez le protocole Internet (IPv4, IPv6, ou les deux) que vous souhaitez utiliser pour les serveurs.

DHCP (Dynamic Host Configuration Protocol - Protocole de configuration dynamique des hôtes)	L'iDRAC récupère automatiquement la configuration IP (adresse IP, masque et passerelle) depuis un serveur DHCP de votre réseau. L'iDRAC reçoit une adresse IP unique, attribuée sur votre réseau. Appuyez sur le bouton central.
Statique	Vous devez entrer manuellement l'adresse IP, la passerelle et le masque de sous-réseau dans les écrans qui suivent. Si vous avez sélectionné l'option Statique, appuyez sur le bouton central pour passer à l'écran **Paramètres réseau iDRAC** suivant, puis : – Définissez l'**adresse IP statique**. Utilisez les touches Gauche ou Droite pour changer de position, puis les flèches Haut et Bas pour sélectionner un numéro pour chaque position. Cette adresse est l'adresse IP de l'iDRAC situé dans le premier logement. Les adresses IP de chacun des iDRAC suivants sont calculées par incrémentation du numéro de logement pour cette adresse IP. Lorsque vous avez fini de définir l'**adresse IP statique**, appuyez sur le bouton central pour continuer. – Définissez le masque de sous-réseau, puis appuyez sur le bouton central. – Définissez la passerelle, puis appuyez sur le bouton central.

– Choisissez l'état du canal réseau (LAN) IPMI en sélectionnant **Activer** ou **Désactiver**. Appuyez sur le bouton central pour continuer.
– Dans l'écran **Configuration iDRAC**, pour appliquer tous les paramètres réseau iDRAC aux serveurs installés, mettez en surbrillance l'icône **Accepter/Oui**, puis appuyez sur le bouton central. Pour ne pas appliquer les paramètres réseau iDRAC aux serveurs installés, mettez en surbrillance l'icône **Non**, puis appuyez sur le bouton central. Passez à l'étape c.
– Dans l'écran **Configuration iDRAC** suivant, pour appliquer tous les paramètres réseau iDRAC aux serveurs nouvellement installés, mettez en surbrillance l'icône Accepter/Oui et appuyez sur le bouton central.

Lorsqu'un nouveau serveur sera inséré dans le châssis, l'écran LCD invitera l'utilisateur à choisir de déployer automatiquement ce serveur avec les paramètres/stratégies réseau précédemment configurés. Pour ne pas appliquer les paramètres réseau iDRAC aux serveurs nouvellement installés, mettez en surbrillance l'icône **Non** et appuyez sur le bouton central. Lors de l'insertion d'un nouveau serveur dans le châssis, ses paramètres réseau iDRAC ne seront pas configurés.

11. Dans l'écran **Enceinte**, pour appliquer tous les paramètres d'enceinte, mettez en surbrillance l'icône **Accepter/Oui**, puis appuyez sur le bouton central. Pour ne pas appliquer les paramètres d'enceinte, mettez en surbrillance l'icône **Non**, puis appuyez sur le bouton central.
12. Dans l'écran **Résumé IP**, passez en revue les adresses IP fournies pour vérifier qu'elles sont correctes. Pour corriger un paramètre, utilisez la touche Gauche et appuyez sur le bouton central pour revenir à l'écran de ce paramètre. Après la correction, appuyez sur le bouton central. Si nécessaire, appuyez sur la touche Droite et appuyez sur le bouton central pour revenir à l'écran **Résumé IP**.

    Lorsque vous avez vérifié que les paramètres entrés sont corrects, appuyez sur le bouton central. L'Assistant Configuration se ferme et vous ramène à l'écran **Menu principal**.

    REMARQUE : Si vous avez sélectionné **Oui/Accepter**, l'écran **Attente** apparaît avant l'affichage de l'écran **Résumé IP**.

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

    REMARQUE : une fois la configuration réseau à l'aide de l'Assistant Configuration de l'écran LCD terminée, l'Assistant devient indisponible.

Interfaces et protocoles d'accès à CMC

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

REMARQUE : Comme Telnet n'est pas aussi sécurisé que les autres interfaces, par défaut, cette option est désactivée. Activez Telnet avec l'interface Web, SSH ou l'interface RACADM distante.

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

Tableau 6. Interfaces CMC

Interface	Description
Interface Web	Permet d'accéder à distance à CMC avec une interface utilisateur graphique (GUI). L'interface Web est intégrée au micrologiciel CMC et vous y accédez via l'interface de carte réseau (NIC) depuis un navigateur Web pris en charge exécuté sur la station de gestion. Pour obtenir la liste des navigateurs Web pris en charge, voir la section Supported Browsers (Navigateurs pris en charge) dans le document *Readme* (Lisez-moi) sur **dell.com/support/manuals**.
Interface de ligne de commande RACADM à distance	Employez cet utilitaire de ligne de commande pour gérer CMC et ses composants. Vous pouvez utiliser l'interface RACADM du micrologiciel ou l'interface distante : • L'interface distante RACADM est un utilitaire client exécuté sur une station de gestion. Elle utilise l'interface réseau hors bande pour exécuter des commandes RACADM sur le système géré et le canal HTTPs. Les options `-r` exécutent la commande RACADM sur un réseau. • Vous accédez à l'interface RACADM du micrologiciel en vous connectant à CMC avec SSH ou Telnet. Vous pouvez exécuter les

Interface	Description
	commandes RACADM du micrologiciel sans spécifier l'adresse IP, le nom d'utilisateur ni le mot de passe CMC. Après avoir accédé à l'invite RACADM vous pouvez exécuter les commandes directement, sans le préfixe racadm.
Écran LCD du châssis	Utilisez l'écran LCD du panneau avant pour réaliser les opérations suivantes : • Affichage des alertes, de l'adresse IP ou MAC CMC, et des chaînes programmables par l'utilisateur • définir DHCP ; • Configuration des paramètres d'adresse IP statique CMC Pour réinitialiser CMC sans redémarrer le serveur, appuyez sur le bouton d'identification système  et maintenez-le enfoncé pendant 16 secondes.
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 il est désactivé par défaut. Telnet transmet toutes les données, y compris les mots de passe en texte clair. Pour transmettre des données sensibles utilisez l'interface SSH
SSH	Utilisez SSH pour exécuter les commandes RACADM. Vous obtenez les mêmes fonctionnalités qu'avec la console Telnet, mais avec une couche de transport cryptée qui renforce la sécurité. Le service SSH est activé par défaut dans CMC et peut être désactivé.
WS-MAN	LC-Remote Services repose sur le protocole de gestion WS pour exécuter des tâches de gestion de systèmes un à plusieurs. Vous devez utiliser un client WS-MAN, tel que WinRM (Windows) ou le client OpenWSMAN (Linux), pour pouvoir utiliser la fonctionnalité LC-Remote Services. Vous pouvez également utiliser Power Shell et Python pour exécuter des scripts vers l'interface WS-MAN. Web Services for Management (WS-Management) est un protocole de type SOAP (Simple Object Access Protocol, protocole simple d'accès aux objets) utilisé pour la gestion des systèmes. CMC utilise WS–Management pour la transmission des informations de gestion DMTF (Distributed Management Task Force, puissance de gestion distribuée) basées sur CIM (Common Information Model, modèle d'information commun). Les informations CIM définissent la sémantique et les types d'information 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. Pour plus d'informations, consultez : • fichiers MOF et profils : **delltechcenter.com/page/DCIM.Library** • site Web DTMF : **dmtf.org/standards/profiles/** • Notes de mise à jour ou fichier « Lisez-moi » de WS-MAN. • **www.wbemsolutions.com/ws_management.html** • Spécifications DMTF WS-Management : **www.dmtf.org/standards/wbem/wsman**

Interface	Description
	Vous pouvez utiliser les interfaces de services Web en exploitant l'infrastructure client existante, comme Windows WinRM et l'interface de ligne de commande (CLI) Powershell, les utilitaires Open Source comme WSMANCLI et les environnements de programmation d'applications comme Microsoft .NET. Pour la connexion client avec Microsoft WinRM, la version minimale requise est la version 2.0. Pour plus d'informations, voir l'article Microsoft <**support.microsoft.com/kb/968929**>.

REMARQUE : Par défaut, le nom d'utilisateur est **root** et le mot de passe est **calvin**.

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

Vous pouvez également lancer CMC depuis Dell Server Administrator ou Dell OpenManage IT Assistant.

Pour accéder à l'interface CMC avec Dell Server Administrator, lancez Server Administrator sur votre station de gestion. Dans l'arborescence système (panneau de gauche de la page d'accueil Server Administrator), cliquez sur **Système** → **Châssis principal du système** → **Remote Access Controller**. Pour plus d'informations, voir le manuel « *Dell Server Administrator User's Guide* » (Guide d'utilisation de Dell Server Administrator).

Téléchargement et mise à jour du micrologiciel CMC

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

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

Définition de l'emplacement physique et du nom du châssis

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

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 l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **Configuration** → **Généralités**. La page **Paramètres généraux du châssis** s'affiche.
2. Entrez les propriétés d'emplacement et le nom du châssis. Pour plus d'informations, voir l'*Aide en ligne 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 ou l'emplacement du châssis, et la date et l'heure avec l'interface de ligne de commande (CLI), voir les sections traitant des commandes **setsysinfo** et **setchassisname**. Pour plus d'informations, voir le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC).

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

Vous pouvez définir manuellement la date et l'heure, ou bien vous pouvez 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 du CMC avec l'interface Web CMC :

1. Dans l'arborescence système, accédez à Présentation du châssis, puis cliquez sur **Configuration** → **Date/Heure**.
   La page **Date/Heure** s'affiche.
2. Pour synchroniser la date et l'heure avec un serveur de synchronisation horaire (NTP), cochez **Activer NTP** et spécifiez jusqu'à trois serveurs NTP.
3. Pour définir la date et l'heure manuellement, désélectionnez l'option **Activer NTP**, puis modifiez les champs **Date** et **Heure**, sélectionnez le **Fuseau horaire** dans le menu déroulant, puis cliquez sur **Appliquer**.

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

Pour définir la date et l'heure en utilisant l'interface de ligne de commande (CLI), voir les sections traitant des groupes de propriétés de base de données `cfgRemoteHosts` dans le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC).

Configuration des LED pour l'identification des composants du châssis

Vous pouvez définir des LED pour chaque composant (châssis, serveurs et modules d'E/S). Celles-ci clignoteront alors pour identifier le composant correspondant du châssis.

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

Configuration du clignotement des LED avec l'interface Web CMC

Pour activer le clignotement d'une LED, de plusieurs ou de toutes les LED de composant avec l'interface Web CMC :

1. Accédez à l'une des pages suivantes :
   - **Présentation du châssis** → **Dépannage** → **Identifier**.
   - **Présentation du châssis** → **Contrôleur de châssis** → **Dépannage** → **Identifier**.
   - **Présentation du châssis** → **Présentation du serveur** → **Dépannage** → **Identifier**.

     REMARQUE : Sur cette page, vous pouvez uniquement sélectionner des serveurs.
   - **Présentation du châssis** → **Présentation du module d'E/S** → **Dépannage** → **Identifier**.
     La page **Identifier** s'affiche.
2. Pour activer le clignotement d'une LED de composant, sélectionnez le composant voulu, puis cliquez sur **Clignotement**.
3. Pour désactiver le clignotement d'une LED de composant, désélectionnez le composant voulu, 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 <état du voyant>]
```

où *<module>* indique le module dont vous souhaitez configurer les LED. Options de configuration :

- `server-nx` où *n* = 1-8 et *x* = a, b, c, ou d
- `switch-n`, où *n*=1 à 6
- `cmc-active`

et *<état du voyant>* indique si la LED doit clignoter. Options de configuration :

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

Configuration des propriétés de CMC

Vous pouvez configurer les propriétés 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 de l'utilitaire RACADM.

Fonctionnement de l'environnement CMC redondant

Vous pouvez installer un CMC de secours, qui remplace le CMC actif si ce dernier échoue. Le CMC redondant peut être préinstallé ou installé ultérieurement. Il importe de câbler correctement le réseau CMC pour garantir une redondance complète ou des performances optimales.

Le basculement peut survenir dans les cas suivants :

- Exécution de la commande RACADM **cmcchangeover**. (Voir la section traitant de la commande **cmcchangeover** dans le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC)).
- Exécution de la commande RACADM racreset sur le CMC actif. (Voir la section traitant de la commande **racreset** dans le manuel « *RACADM Command Line Reference Guide for iDRAC6 and CMC* » (Guide de référence de la ligne de commande RACADM d'iDRAC6 et de CMC)).
- Réinitialisation du CMC actif depuis l'interface Web. (Voir le paragraphe portant sur l'option **Réinitialiser CMC** à la section « **Opérations de contrôle de l'alimentation** » de la rubrique « Exécution d'opérations de contrôle de l'alimentation ».)
- Retrait du câble réseau du CMC actif.
- Retrait du CMC actif du châssis.
- Lancement d'un vidage Flash du micrologiciel CMC sur le CMC actif.
- Utilisation d'un CMC actif qui n'est plus fonctionnel.

  REMARQUE : Lors d'un basculement du CMC, toutes les connexions iDRAC et toutes les sessions CMC actives sont perdues. Les utilisateurs qui ont perdu leur session doivent se reconnecter au nouveau CMC actif.

Liens connexes

À propos du CMC de secours

Mode anti-défaillance du module CMC

Processus de sélection du CMC actif

Obtention de la condition d'intégrité du contrôleur CMC redondant

À propos du CMC de secours

Le CMC de secours est identique au CMC actif et géré comme miroir de ce dernier. Vous devez installer les deux CMC, actif et de secours, avec la même version du micrologiciel. Si les micrologiciels diffèrent, le système signale une dégradation de la redondance.

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

REMARQUE : Pour plus d'informations sur l'installation d'un CMC de secours, voir le « *Hardware Owner's Manual* » (Manuel du propriétaire du matériel). Pour obtenir des instructions sur l'installation du micrologiciel CMC sur votre CMC de secours, voir la section « Mise à jour du micrologiciel ».

Mode anti-défaillance du module CMC

Comme avec la protection contre les défaillances offerte par le CMC redondant, le mode Sans échec du châssis M1000e permet de protéger les lames et les modules d'E/S des défaillances. Le mode Sans échec est activé lorsqu'aucun CMC ne contrôle le châssis. Au cours d'une période de basculement du CMC ou de perte de gestion d'un seul module CMC :

- Vous ne pouvez pas mettre sous tension des lames nouvellement installées.
- Vous ne pouvez pas accéder à distance aux lames existantes.
- Les ventilateurs de refroidissement du châssis tournent à 100 % pour la protection thermique des composants.
- Jusqu'à la restauration de la gestion du CMC, la performance des lames est réduite afin de limiter la consommation d'énergie.

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

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

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

Processus de sélection du CMC actif

Il n'existe aucune différence entre les deux logements de CMC : le logement ne détermine pas l'ordre de priorité. C'est plutôt le CMC installé ou amorcé en premier qui devient CMC actif. Si vous activez l'alimentation CA après avoir installé

deux CMC, le CMC installé dans le logement CMC numéro 1 (à gauche) assume normalement le rôle de CMC actif. La LED bleue vous indique le CMC actif.

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

Obtention de la condition d'intégrité du contrôleur CMC redondant

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

3

Connexion à CMC

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

Liens connexes

Accès à l'interface Web CMC
Connexion à CMC comme utilisateur local, utilisateur Active Directory User ou utilisateur LDAP
Connexion à CMC avec une carte à puce
Connexion à CMC par connexion directe
Connexion à CMC avec la console série, Telnet ou SSH
Accès à CMC avec RACADM
Connexion à CMC à l'aide de l'authentification par clé publique

Accès à l'interface Web CMC

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

REMARQUE : Si vous utilisez Microsoft Internet Explorer pour vous connecter via un proxy et que l'erreur « La page XML ne peut être affichée » s'affiche, vous devez désactiver le proxy pour continuer.

Pour accéder à l'interface Web CMC :

1. Ouvrez une fenêtre d'un navigateur Web pris en charge.
   Pour obtenir les dernières informations sur les navigateurs Web pris en charge, voir le document *Readme* (Lisez-moi) sur **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://<adresse IP CMC>`
     Si vous avez modifié le numéro de port HTTPS par défaut (port 443), entrez : `https://<adresse IP CMC>:<numéro de port>`
   - Pour accéder à CMC avec l'adresse IPv6 : `https://[<adresse IP CMC>]`
     Si vous avez modifié le numéro de port HTTPS par défaut (port 443), entrez : `https://[<adresse IP CMC>]:<numéro de port>`

     REMARQUE : Lorsque vous utilisez IPv6, vous devez mettre *<adresse IP CMC>* entre crochets ([ ]).

     <adresse IP CMC> est l'adresse IP CMC et *<numéro de port>*, le numéro du port HTTPS.

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

Liens connexes

Configuration du navigateur Web
Connexion à CMC comme utilisateur local, utilisateur Active Directory User ou utilisateur LDAP
Connexion à CMC avec une carte à puce
Connexion à CMC par connexion directe

Connexion à CMC comme utilisateur local, utilisateur Active Directory User ou utilisateur LDAP

Pour vous connecter à CMC, vous devez disposer d'un compte CMC doté du privilège d'**Ouverture de session CMC**. Le nom d'utilisateur CMC par défaut est root et le mot de passe par défaut est calvin. Le compte root est le compte d'administration par défaut livré avec 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.

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

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.

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

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

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

   REMARQUE : Ce champ est sensible à la casse.
3. (Facultatif) Sélectionnez un délai d'attente 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.
4. Cliquez sur **OK**.

   Vous êtes connecté à CMC avec les privilèges utilisateur requis.

Liens connexes

Configuration des comptes et des privilèges des utilisateurs
Accès à l'interface Web CMC

Connexion à CMC avec une carte à puce

Vous pouvez vous connecter à CMC avec une carte à puce. Les cartes à puce fournissent une authentification TFA (Two Factor Authentication - Authentification à deux facteurs) qui fournit une sécurité à deux niveaux :

- 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 NIP.

REMARQUE : Vous ne pouvez pas utiliser l'adresse IP pour vous connecter à CMC avec une carte à puce. Kerberos valide vos références par rapport au nom FQDN (Fully Qualified Domain Name - Nom de domaine entièrement 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 à CMC en tant qu'utilisateur Active Directory en utilisant une carte à puce :

1. Connectez-vous à CMC à l'aide du lien `https://<nom-CMC.nom-domaine>`.
   La page **Connexion à CMC** qui s'affiche vous invite à insérer la carte à puce.

   REMARQUE : Si vous avez changé le numéro de port HTTPS par défaut (port 80), accédez à la page Web CMC avec `<nom-CMC.nom-domaine>:<numéro de port>`, où nom-CMC est le nom d'hôte CMC de votre CMC, **nom-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 fenêtre contextuelle du code 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.

   Vous êtes connecté à CMC avec vos références Active Directory.

Liens connexes

Configuration de la connexion directe ou par carte à puce CMC pour les utilisateurs Active Directory

Connexion à CMC par connexion directe

Lorsque la fonction de connexion directe (SSO) est activée, vous pouvez vous connecter à CMC sans entrer vos références d'authentification d'utilisateur de domaine (nom d'utilisateur et mot de passe, par exemple).

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

Avant de vous connecter à CMC par connexion directe, vérifiez les points suivants :

- 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 ouvrir une session dans CMC à l'aide de la connexion directe :

1. Ouvrez une session sur le système client avec votre compte réseau.
2. Accédez à l'interface Web CMC avec : `https://<nom-CMC.nom-domaine>`
   Par exemple, **cmc-6G2WXF1.cmcad.lab**, où **cmc-6G2WXF1** est le nom du 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 avec `<nom-CMC.nom-domaine>:<numéro de port>`, où **nom-CMC** est le nom d'hôte CMC de votre CMC, **nom-domaine** est le nom du domaine et **numéro de port** est le numéro du port HTTPS.

   CMC vous connecte à l'aide des 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'avez pas ouvert de session sur le domaine Active Directory et que vous utilisez un navigateur autre qu'Internet Explorer, l'ouverture de session échoue et le navigateur affiche uniquement une page vide.

Liens connexes

Configuration de la connexion directe ou par carte à puce CMC pour les utilisateurs Active Directory

Connexion à CMC avec la console série, Telnet ou SSH

Vous pouvez vous connecter à CMC via une connexion série, Telnet ou SSH, ou encore via la console Dell CMC du module iKVM.

Une fois le logiciel d'émulation de terminal et le BIOS du nœud géré de votre station de gestion configurés, effectuez les étapes suivantes pour ouvrir une session sur CMC :

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

   Vous êtes connecté à CMC.

Liens connexes

Configuration de CMC pour utiliser des consoles de ligne de commande
Activation de l'accès à iKVM depuis la console Dell CMC

Accès à CMC avec RACADM

RACADM fournit un ensemble de commandes permettant de configurer et de gérer le CMC via une interface de type texte. RACADM est accessible via une connexion Telnet/SSH ou une connexion série. Vous utilisez pour cela la console Dell CMC sur le module iKVM ou procédez à distance avec l'interface de ligne de commande (CLI) RACADM installée sur une station de gestion.

L'interface RACADM est classée comme suit :

REMARQUE : Le RACADM distant est inclus sur le DVD Dell Systems Management Tools and Documentation, et est installé sur une station de gestion.

- RACADM distant : permet l'exécution de commandes RACADM sur une station de gestion avec l'option -r, et le nom DNS ou l'adresse IP du CMC.
- RACADM du micrologiciel : vous permet de vous connecter au CMC via Telnet, SSH, une connexion série ou le module iKVM. Avec le RACADM du micrologiciel, vous exécutez l'implémentation RACADM incluse dans le micrologiciel CMC.

Vous pouvez utiliser les commandes RACADM distantes dans des scripts pour configurer plusieurs CMC. CMC n'offre aucune prise en charge des scripts, si bien qu'il est impossible d'exécuter les scripts directement sur le CMC.

Pour plus d'informations sur RACADM, voir le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC).

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

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

Vous pouvez vous connecter à 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 l'interface distante RACADM, puisque la session prend fin après l'exécution de la commande.

Avant de vous connecter à CMC sur SSH, assurez-vous que les clés publiques ont été téléversées.

Par exemple :

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

Lorsque vous vous connectez avec le compte de service, si une phrase de passe a été configurée lors de la création de la paire de clés privée et publique, vous pouvez être invité à saisir cette phrase de passe. Si vous utilisez une phrase de passe avec les clés, il est possible d'automatiser également cette opération, aussi bien sous Windows que sous Linux. Pour les clients Windows, vous pouvez utiliser l'application Pageant. Elle s'exécute à l'arrière-plan et la saisie de la phrase de passe devient transparente. Pour les clients Linux, vous pouvez utiliser sshagent. Pour configurer et utiliser ces deux applications, voir la documentation fournie pour l'application concernée.

Liens connexes

Configuration de l'authentification par clé publique sur SSH

Sessions CMC multiples

Le tableau suivant répertorie les sessions CMC multiples qu'il est possible d'établir avec les diverses interfaces.

Tableau 7. Sessions CMC multiples

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

4

Mise à jour du micrologiciel

Vous pouvez mettre à jour le micrologiciel des éléments suivants :

- CMC (actif et de secours)
- iKVM
- IOM

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

- iDRAC : les iDRAC antérieurs à iDRAC6 doivent être mis à jour avec l'interface de restauration. Vous pouvez également mettre à jour le micrologiciel iDRAC6 avec l'interface de restauration, mais cette fonction n'est plus utilisée dans iDRAC6 et versions ultérieures.
- BIOS
- Unified Server Configurator
- Diagnostics 32 bits
- Paquet de pilotes du SE
- Contrôleurs d'interface réseau (NIC)
- Contrôleurs RAID

Liens connexes

Téléchargement du micrologiciel CMC
Affichage des versions du micrologiciel actuellement installées
Mise à jour du micrologiciel CMC
Mise à jour du micrologiciel iKVM
Mise à jour du micrologiciel iDRAC du serveur
Mise à jour du micrologiciel des composants de serveur
Restauration du micrologiciel iDRAC avec CMC
Mise à jour du micrologiciel de périphérique d'infrastructure des modules d'E/S (IOM)

Téléchargement du micrologiciel CMC

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

Le progiciel de micrologiciel CMC comprend les composants logiciels suivants :

- Code et données compilés du micrologiciel du module CMC
- Fichiers de données de l'interface Web, JPEG et d'autres interfaces utilisateur
- Fichiers de configuration par défaut

Affichage des versions du micrologiciel actuellement installées

Vous pouvez afficher les versions du micrologiciel actuellement installées 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**
- **Présentation du châssis → Présentation du module d'E/S → Mise à jour**
- **Présentation du châssis → iKVM → Mise à jour**

La page **Mise à jour du micrologiciel** affiche la version actuelle du micrologiciel pour chaque composant répertorié et vous permet de mettre à jour le micrologiciel vers la révision la plus récente.

Si le châssis renferme un serveur de génération antérieure dont l'iDRAC est en mode Restauration ou si CMC détecte que le micrologiciel iDRAC est corrompu, l'iDRAC de génération antérieure est également répertorié dans la page Mise à jour du micrologiciel.

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

Pour afficher les versions actuellement installées du micrologiciel avec RACADM, utilisez la sous-commande **getkvminfo**. Pour plus d'informations, voir le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de l'interface de ligne de commande RACADM pour iDRAC7 et CMC).

Mise à jour du micrologiciel CMC

Vous pouvez mettre à jour le micrologiciel CMC à l'aide de l'interface Web ou de RACADM. Par défaut, la mise à jour du micrologiciel conserve les paramètres CMC actuels. Pendant le processus de mise à jour, vous pouvez réinitialiser les paramètres de configuration de CMC afin de revenir aux paramètres par défaut définis en usine.

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

Si vous utilisez une session de l'interface utilisateur Web pour mettre à jour le micrologiciel des composants système, le paramètre Délai d'attente en cas d'inactivité doit être défini sur une valeur suffisamment élevée pour gérer la durée du transfert de fichiers. Dans certains cas, ce transfert peut prendre jusqu'à 30 minutes. Pour définir la valeur 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 %.

Si vous avez installé des CMC redondants dans le châssis, il est recommandé de mettre à jour les deux CMC vers la même version du micrologiciel au même moment au cours de la même opération. Si les CMC ont des micrologiciels différents et qu'un basculement se produit, les résultats peuvent être imprévisibles.

Le CMC actif est réinitialisé et devient temporairement inaccessible après le téléversement réussi du micrologiciel. S'il existe un CMC de secours, les rôles Actif et De secours sont échangés. Le CMC de secours devient CMC actif. Si vous appliquez la mise à jour uniquement au CMC actif, une fois la réinitialisation terminée, le CMC actif n'exécute pas l'image mise à jour, car seul le CMC de secours possède cette image. En général, il est vivement recommandé de maintenir des versions de micrologiciel identiques sur les deux CMC actif et de secours.

Une fois le CMC de secours mis à jour, échangez les rôles des CMC afin que le CMC nouvellement mis à jour devienne le CMC actif et que le CMC possédant la version la plus ancienne du micrologiciel devienne le CMC de secours. Voir la section traitant de la commande `cmcchangeover` dans le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC) pour

plus d'informations sur l'échange des rôles. Cela vous permet de vérifier que la mise à jour a réussi et que le nouveau micrologiciel fonctionne correctement, avant de mettre à jour le micrologiciel du deuxième CMC. Lorsque les deux CMC ont été mis à jour, vous pouvez utiliser la commande `cmcchangeover` pour restaurer les rôles précédents des CMC. Le micrologiciel CMC version 2.x met à jour à la fois le CMC principal et le CMC redondant, sans utiliser la commande `cmcchangeover`.

Pour éviter de déconnecter les autres utilisateurs au cours d'une réinitialisation, informez les utilisateurs autorisés susceptibles de se connecter au CMC et vérifiez les sessions actives dans la page Sessions. Pour ouvrir la page **Sessions**, sélectionnez **Châssis** dans l'arborescence, cliquez sur l'onglet **Réseau**, puis cliquez sur le sous-onglet **Sessions**.

Lorsque vous transférez des fichiers vers et depuis CMC, les icônes de transfert de fichiers tournent pendant le transfert. Si votre icône est animée, vérifiez que votre navigateur est configuré pour autoriser les animations. Pour obtenir des instructions, voir « Autorisation des animations dans Internet Explorer ».

Si vous avez des difficultés à télécharger des fichiers depuis CMC dans Internet Explorer, activez l'option Ne pas enregistrer les pages cryptées sur le disque. Pour obtenir des instructions, voir « Téléchargement de fichiers à partir de CMC dans Internet Explorer ».

Liens connexes

Téléchargement du micrologiciel CMC

Affichage des versions du micrologiciel actuellement installées

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

Pour mettre à jour le micrologiciel CMC avec 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**
   - **Présentation du châssis → Présentation du module d'E/S → Mise à jour**
   - **Présentation du châssis → iKVM → Mise à jour**

   La page **Mise à jour de micrologiciel** s'affiche.
2. Dans la section **Micrologiciel CMC**, cochez dans la colonne **Cibles de mise à jour** la case du ou des CMC (si vous avez installé un CMC de secours) dont vous voulez mettre à jour le micrologiciel. Cliquez ensuite sur **Appliquer la mise à jour CMC**.
3. Dans le champ **Image de micrologiciel**, entrez le chemin d'un fichier d'image de micrologiciel figurant sur la station de gestion ou sur le réseau partagé, ou cliquez sur **Parcourir** pour naviguer vers le fichier voulu. Le nom par défaut de l'image de micrologiciel CMC est `firmimg.cmc`.
4. Cliquez sur **Lancer la mise à jour du micrologiciel**, puis sur **Oui** pour continuer. 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 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.
5. Instructions supplémentaires :
   - Ne cliquez pas sur l'icône **Actualiser** et ne naviguez vers aucune autre page pendant le transfert de fichiers.
   - Pour annuler le processus, cliquez sur **Annuler le transfert de fichier et la mise à jour**. Cette option n'est disponible que pendant le transfert de fichier.
   - Le champ **État de la mise à jour** affiche l'état de mise à jour du micrologiciel.

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

6. Pour un CMC de secours, une fois la mise à jour terminée, le champ **État de la mise à jour** affiche la mention **Terminé**. Pour un CMC actif, pendant les phases finales du processus de mise à jour du micrologiciel, la session de navigateur et la connexion au CMC sont temporairement perdues lorsque le CMC actif est mis hors ligne. Vous devez vous reconnecter après quelques minutes, une fois que le CMC actif a redémarré. Après la réinitialisation du CMC, le nouveau micrologiciel s'affiche dans la page **Mise à jour du micrologiciel**.

   REMARQUE : Après la mise à jour du micrologiciel, videz le cache du navigateur Web. Pour savoir comment procéder, voir l'aide en ligne du navigateur Web.

Mise à jour du micrologiciel CMC via RACADM

Pour mettre à jour le micrologiciel CMC avec RACADM, utilisez la sous-commande fwupdate. Pour plus d'informations, voir le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de l'interface de ligne de commande RACADM pour iDRAC7 et CMC).

Mise à jour du micrologiciel iKVM

Après le chargement réussi du micrologiciel, le module iKVM est réinitialisé et devient temporairement indisponible.

Liens connexes

Téléchargement du micrologiciel CMC

Affichage des versions du micrologiciel actuellement installées

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

Pour mettre à jour le micrologiciel iKVM avec 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**
   - **Présentation du châssis → iKVM → Mise à jour**

   La page **Mise à jour de micrologiciel** s'affiche.
2. Dans la section **Micrologiciel iKVM**, cochez la case de la colonne **Cibles de mise à jour** correspondant au module **iKVM** dont vous voulez mettre à jour le micrologiciel, puis cliquez sur **Appliquer la mise à jour iKVM**.
3. Dans le champ **Image de micrologiciel**, entrez le chemin d'un fichier d'image de micrologiciel figurant sur la station de gestion ou sur le réseau partagé, ou cliquez sur **Parcourir** pour naviguer vers le fichier voulu. Le nom par défaut de l'image de micrologiciel iKVM est **iKVM.bin**.
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** 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 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.
5. Instructions supplémentaires à suivre :
   - Ne cliquez pas sur l'icône **Actualiser** et ne naviguez vers aucune autre page pendant le transfert de fichiers.
   - Pour annuler le processus, cliquez sur **Annuler le transfert de fichier et la mise à jour**. Cette option n'est disponible que pendant le transfert de fichier.
   - Le champ **État de la mise à jour** affiche l'état de mise à jour du micrologiciel.

REMARQUE : La mise à jour de l'iKVM peut prendre jusqu'à deux minutes.

À la fin de la mise à jour, le module iKVM est réinitialisé et le nouveau micrologiciel apparaît sur la page **Mise à jour du micrologiciel**.

Mise à jour du micrologiciel iKVM via RACADM

Pour mettre à jour le micrologiciel iKVM à l'aide de l'interface RACADM, utilisez la sous-commande `fwupdate`. Pour plus d'informations, voir le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de l'interface de ligne de commande RACADM pour iDRAC7 et CMC).

Mise à jour du micrologiciel de périphérique d'infrastructure des modules d'E/S (IOM)

En exécutant cette mise à jour, vous mettez à jour le micrologiciel d'un composant du périphérique IOM, mais pas celui du périphérique IOM proprement dit. Ce composant est le circuit d'interface entre le périphérique IOM et CMC. L'image de mise à jour du composant réside dans le système de fichiers CMC et le composant est affiché comme périphérique pouvant être mis à jour dans l'interface Web CMC uniquement si les versions actuelles du composant et de l'image du composant ne correspondent pas dans CMC.

Avant de mettre à jour le micrologiciel de périphérique d'infrastructure IOM, vérifiez que le micrologiciel CMC a été mis à jour.

REMARQUE :

CMC autorise la mise à jour du micrologiciel de périphérique d'infrastructure IOM (IOMINF) uniquement s'il détecte que le micrologiciel IOMINF est plus ancien que l'image contenue dans le système de fichiers CMC. Si le micrologiciel IOMINF est à jour, CMC interdit les mises à jour d'IOMINF. Les périphériques IOMINF à jour ne sont pas répertoriés comme pouvant être mis à jour.

Liens connexes

Téléchargement du micrologiciel CMC
Affichage des versions du micrologiciel actuellement installées
Mise à jour du logiciel IOM à l'aide de l'interface Web CMC

Mise à jour du micrologiciel IOM dans l'interface Web CMC

Pour mettre à jour le micrologiciel 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 **Logiciel et micrologiciel IOM** s'affiche.

   Ou alors, accédez à l'une des pages suivantes :

   - **Présentation du châssis** → **Mise à jour**
   - **Présentation du châssis** → **Contrôleur de châssis** → **Mise à jour**
   - **Présentation du châssis** → **iKVM** → **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 **Logiciel et micrologiciel IOM**, dans la section **Logiciel IOM**, 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**.

   La section **État de la mise à jour** fournit des informations sur l'état de mise à jour du micrologiciel. 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.

Une fois la mise à jour terminée, vous perdez brièvement la connexion au périphérique IOM car il est réinitialisé, et le nouveau micrologiciel apparaît dans la page **Logiciel et micrologiciel IOM**.

Mise à jour du micrologiciel IOM avec RACADM

Pour mettre à jour le micrologiciel de périphérique d'infrastructure des modules d'E/S (IOM) avec RACADM, utilisez la sous-commande fwupdate. Pour plus d'informations, voir le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de l'interface de ligne de commande RACADM pour iDRAC7 et CMC).

Mise à jour du micrologiciel iDRAC du serveur

Vous pouvez mettre à jour le micrologiciel iDRAC6 et iDRAC7.

Vous devez utiliser le micrologiciel iDRAC version 1.4 ou supérieure pour les serveurs avec iDRAC, et version 2.0 ou supérieure pour les serveurs avec iDRAC6 Enterprise. Si vous mettez à jour le micrologiciel iDRAC vers la version 3.0 ou supérieure depuis une version d'iDRAC antérieure à 2.3, il faut d'abord effectuer une mise à jour vers iDRAC version 2.3 avant la mise à jour vers la version 3.0 ou supérieure.

L'iDRAC (sur un serveur) se réinitialise et est temporairement indisponible après le téléversement réussi des mises à jour du micrologiciel.

Liens connexes

Téléchargement du micrologiciel CMC

Affichage des versions du micrologiciel actuellement installées

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

Pour mettre à jour le micrologiciel iDRAC du serveur avec 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**
   - **Présentation du châssis → iKVM → Mise à jour**

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

   Vous pouvez également mettre à jour le micrologiciel iDRAC du serveur avec l'option **Présentation du châssis → Présentation du serveur → Mise à jour**. Pour plus informations, voir « Mise à jour du micrologiciel des composants de serveur ».
2. Pour mettre à jour le micrologiciel iDRAC6, accédez à la section **Micrologiciel iDRAC6 Enterprise** ; dans la colonne **Cibles de mise à jour** cochez la case correspondant au module iKVM dont vous voulez mettre à jour le micrologiciel. Cliquez ensuite sur **Appliquer la mise à jour iDRAC6 Enterprise**, puis passez à l'étape 4.
3. Pour mettre à jour le micrologiciel iDRAC7, accédez à la section **Micrologiciel iDRAC7 Enterprise**, puis cliquez sur le lien **Mise à jour** correspondant au serveur dont vous voulez mettre à jour le micrologiciel.

   La page **Mise à jour des composants de serveur** s'affiche. Pour continuer, voir la section « Mise à jour du micrologiciel des composants de serveur ».

4. Dans le champ **Image de micrologiciel**, entrez le chemin d'un fichier d'image de micrologiciel figurant sur la station de gestion ou sur le réseau partagé, ou cliquez sur **Parcourir** pour naviguer vers le fichier voulu. Le nom par défaut de l'image de micrologiciel iDRAC est **firmimg.imc**.
5. 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** 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 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.
6. Instructions supplémentaires à suivre :
   - Ne cliquez pas sur l'icône **Actualiser** et ne naviguez vers aucune autre page pendant le transfert de fichiers.
   - Pour annuler le processus, cliquez sur **Annuler le transfert de fichier et la mise à jour**. Cette option n'est disponible que pendant le transfert de fichier.
   - Le champ **État de la mise à jour** affiche l'état de mise à jour du micrologiciel.

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

   À la fin de la mise à jour, le module iKVM est réinitialisé et le nouveau micrologiciel apparaît sur la page **Mise à jour du micrologiciel**.

Mise à jour du micrologiciel iDRAC du serveur avec RACADM

Pour mettre à jour le micrologiciel iDRAC avec RACADM, utilisez la sous-commande **fwupdate**. Pour plus d'informations, voir le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de l'interface de ligne de commande RACADM pour iDRAC7 et CMC).

Mise à jour du micrologiciel des composants de serveur

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

Les progiciels DUP (Dell Update Package - Progiciel de mise à jour Dell) vous permettent d'effectuer les mises à jour du micrologiciel avec le Lifecycle Controller. La configuration CMC par défaut impose une limite de taille maximale de DUP de 48 Mo. Le DUP du composant Pack de pilotes de système d'exploitation dépasse cette limite et vous devez le mettre à jour séparément à l'aide de la fonctionnalité de stockage étendu.

Le Lifecycle Controller prend en charge les mises à jour des modules pour les serveurs iDRAC6 et version ultérieure. Vous devez utiliser le micrologiciel iDRAC version 3.20 ou ultérieure pour mettre le micrologiciel à jour avec le Lifecycle Controller.

Avant d'utiliser la fonctionnalité de mise à jour basée sur Lifecycle Controller, les versions du micrologiciel des serveurs doivent être mises à jour.

Vous devez mettre à jour le micrologiciel CMC avant de mettre à jour les modules de micrologiciel des composants de serveur.

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

1. BIOS
2. Lifecycle Controller
3. iDRAC

Dans l'interface Web CMC, vous pouvez mettre à jour le micrologiciel des composants de serveur dans la page **Présentation du châssis → Présentation du serveur → Mise à jour → Mise à jour des composants de serveur**.

Si le serveur ne prend pas en charge le service Lifecycle Controller, la section **Inventaire des micrologiciels du composant/périphérique** affiche la mention **Pas 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 conçu à cet effet, exécuté dans le système d'exploitation du serveur. Pour les serveurs pris en charge, un progiciel de réparation ou d'installation particulier est disponible, avec l'extension de fichier .usc. Il vous 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 du composant/périphérique** affiche la mention *Impossible d'activer Lifecycle Controller*.

Liens connexes

Activation du Lifecycle Controller
Filtrage des composants pour la mise à jour des micrologiciels
Affichage de l'inventaire des micrologiciels
Opérations de tâche Lifecycle Controller
Mise à jour du micrologiciel de périphérique d'infrastructure des modules d'E/S (IOM)

Activation du Lifecycle Controller

Vous pouvez activer le service Lifecycle Controller au cours du processus d'amorçage du serveur.

- Pour les serveurs iDRAC6, dans la console d'amorçage, lorsque vous voyez le message `Appuyez sur <CTRL-E> pour ouvrir Configuration d'accès à distance dans les 5 s`, appuyez sur <CTRL-E>. Dans l'écran de configuration, activez ensuite l'option **Services système**.
- Pour les serveurs iDRAC7, dans la console d'amorçage, appuyez sur F2 pour ouvrir Configuration du système. Dans l'écran de configuration, sélectionnez **Paramètres d'iDRAC**, puis **Services système**.

  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 des informations supplémentaires sur le Lifecycle Controller, les composants du serveur, et la gestion du micrologiciel de périphériques, voir :

- « *Lifecycle Controller Remote Services User's Guide* » (Guide d'utilisation des services distants Lifecycle Controller).
- **delltechcenter.com/page/Lifecycle+Controller**.

La page **Mise à jour des composants de serveur** vous permet de mettre à jour différents composants de micrologiciel sur votre système. Pour utiliser les fonctions et options de cette page, vous devez installer les applications suivantes :

- Pour CMC : **Server Administrator**.
- Pour iDRAC : **Configurer iDRAC** et **Ouvrir une session dans 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.

Filtrage des composants pour la mise à jour des micrologiciels

Les informations de tous les composants et périphériques de tous les serveurs sont collectées simultanément. Pour gérer ce gros volume d'informations, le Lifecycle Controller offre différents mécanismes de filtrage. Ces filtres permettent de réaliser les opérations suivantes :

- 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,
- filtrer automatiquement les composants et périphériques, pour réduire la catégorie d'un composant ou périphérique selon les types ou modèles.

  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.

Exemples

Voici quelques exemples où les mécanismes de filtrage sont appliqués :

- Si vous choisissez le filtre BIOS, seul l'inventaire BIOS de tous les serveurs est affiché. Si l'ensemble de serveurs réunit un certain nombre de modèles de serveur 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 la mise à jour du micrologiciel des cartes d'interface réseau (Network Interface Controllers - NIC) 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 progiciel DUP peut être programmé pour mettre à jour plusieurs types ou modèles de périphérique dans une catégorie donnée.

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

Pour filtrer les périphériques :

1. Dans 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 **Filtre de mise à jour des composants/périphériques**, sélectionnez un ou plusieurs des éléments suivants :

   - BIOS
   - iDRAC
   - Lifecycle Controller
   - Diagnostics 32 bits
   - Pack de pilotes du système d'exploitation
   - Contrôleur d'interface réseau
   - Contrôleur RAID

   La section **Inventaire des micrologiciels** affiche uniquement les composants ou périphériques associés pour l'ensemble des serveurs présents dans le châssis. Le filtre accepte uniquement les composants ou périphériques associés au filtre, et exclut tous les autres.

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

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

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

Pour filtrer les composants en vue de la mise à jour du micrologiciel avec RACADM, utilisez la commande getversion :

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

Pour plus d'informations, voir le manuel RACADM Command Line Reference Guide for iDRAC7 and CMC (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible sur le site **dell.com/support/manuals**.

Affichage de l'inventaire des micrologiciels

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

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

Pour afficher l'inventaire des micrologiciels :

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. Les détails d'inventaire des micrologiciels s'affichent dans la section **Inventaire des micrologiciels du composant/ périphérique**. La table contient les éléments suivants

   - Les serveurs qui ne prennent pas en charge le service Lifecycle Controller sont répertoriés sous la mention **Pas pris en charge**. Vous disposez d'un lien hypertexte vers une autre page permettant de mettre directement à jour le micrologiciel, uniquement pour l'iDRAC. Cette page ne prend en charge que la mise à jour du micrologiciel iDRAC ; elle ne gère aucun autre composant ou périphérique du serveur. La mise à jour du micrologiciel iDRAC est indépendante du service Lifecycle Controller.
   - Si le serveur est affiché comme **Pas 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 l'iDRAC soit pleinement opérationnel, puis actualisez la page pour récupérer à nouveau l'inventaire des micrologiciels.
   - Si l'inventaire des composants et périphériques ne reflète pas les éléments physiquement installés sur le serveur, vous devez appeler le Lifecycle Controller pendant le processus d'amorçage du serveur. Cela permet d'actualiser les informations internes concernant les composants et les périphériques, et vous pourrez ainsi vérifier les périphériques et composants actuellement installés. Cela se produit dans les circonstances suivantes :

     * 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 opération, les utilitaires Configuration iDRAC (pour iDRAC6) et Paramètres d'iDRAC (pour iDRAC7) offrent une option accessible via la console d'amorçage :

* Pour les serveurs iDRAC6, dans la console d'amorçage, lorsque vous voyez le message `Appuyez sur <CTRL-E> pour ouvrir Configuration d'accès à distance avant 5 s`, appuyez sur `<CTRL-E>`. Dans l'écran de configuration, activez ensuite l'option **Collecte de l'inventaire système au redémarrage**.
* Pour les serveurs iDRAC7, dans la console d'amorçage, appuyez sur F2 pour ouvrir Configuration du système. Dans l'écran de configuration, sélectionnez Paramètres d'iDRAC, pour l'option Services système (USC). Dans l'écran qui s'affiche, activez l'option **Collecte de l'inventaire système au redémarrage**.

– 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 8. : informations sur les composants et périphériques

Champ	Description
Logement	Indique le logement occupé par le serveur dans le châssis. Les numéros de logement sont des ID séquentiels allant de 1 à 16 (pour les 16 logements disponibles dans le châssis), qui vous aident à identifier l'emplacement du serveur dans le châssis. Si moins de 16 serveurs occupent des logements, seuls les logements contenant un serveur sont affichés.
Nom	Affiche le nom du serveur dans chaque logement.
Modèle	Affiche le modèle du serveur.
Composant/Périphérique	Affiche la description du composant ou périphérique sur le serveur. Si la colonne est trop étroite, utilisez l'outil de pointage à la souris pour afficher la description.
Version actuelle	Affiche la version actuelle du composant ou du périphérique sur le serveur.
Version de la restauration	Affiche la version de restauration du composant ou du périphérique sur le serveur.
Condition de la tâche	Indique l'état de chaque tâche planifiée sur le serveur. L'état des tâches est mis à jour dynamiquement, en continu. Si le système détecte l'achèvement d'une tâche (état Terminé), les versions de micrologiciel des composants et périphériques du serveur correspondant sont automatiquement actualisées, au cas où il y ait eu un changement de version de micrologiciel sur ces composants/périphériques. Une icône d'informations 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	Sélectionne le composant ou périphérique pour la mise à jour du micrologiciel 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 manuel RACADM Command Line Reference Guide for iDRAC7 and CMC (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible sur le site **dell.com/support/manuals**.

Opérations de tâche Lifecycle Controller

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 pour planification. Si vous le faites, un message pop-up de confirmation s'affiche, permettant d'annuler la navigation prévue. Sinon, l'opération est interrompue. Toute interruption, particulièrement pendant une opération de mise à jour, peut provoquer l'arrêt du téléversement du fichier d'image du micrologiciel avant son achèvement correct. Une fois que vous avez soumis l'opération pour planification, veillez à accuser réception du message de confirmation signalant la réussite de la planification de l'opération.

Liens connexes

Réinstallation du micrologiciel des composants de serveur
Restauration (rollback) du micrologiciel des composants de serveur
Mise à niveau du micrologiciel des composants de serveur
Suppression de tâches planifiées de micrologiciel de composant de serveur

Réinstallation 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.

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

Pour réinstaller le micrologiciel des composants de serveur :

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. Filtrez les composants ou périphériques (facultatif).
3. Dans la colonne **Version actuelle**, cochez la case du composant ou périphérique dont vous voulez réinstaller le micrologiciel.
4. Sélectionnez l'une des options suivantes :
   - **Redémarrer maintenant** : lance un redémarrage immédiat.
   - **Au prochain redémarrage** : permet de redémarrer manuellement le serveur, ultérieurement.
5. Cliquez sur **Réinstaller**. La version du micrologiciel est réinstallée pour le composant ou périphérique sélectionné.

Restauration (rollback) du micrologiciel des composants de serveur

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

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

Pour restaurer (rollback) une version précédente du micrologiciel d'un composant de serveur :

1. Dans l'interface Web CMC, développez 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. Filtrez les composants ou périphériques (facultatif).
3. Dans la colonne **Restaurer la version**, cochez la case du composant ou périphérique dont vous voulez restaurer le micrologiciel.
4. Sélectionnez l'une des options suivantes :
   - **Redémarrer maintenant** : lance un redémarrage immédiat.
   - **Au prochain redémarrage** : permet de redémarrer manuellement le serveur, ultérieurement.
5. Cliquez sur **Restaurer**. La version du micrologiciel précédemment installée est réinstallée sur le composant ou périphérique sélectionné.

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 Lifecycle Controller pour l'opération de restauration (rollback).

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

Il est recommandé de vider la file d'attente des tâches avant de lancer la mise à jour du micrologiciel d'un composant de serveur. La liste complète des tâches du ou des serveurs est disponible dans la page Tâches du Lifecycle Controller. Cette page permet de supprimer une ou plusieurs tâches, ou de purger toutes les tâches du serveur. Consultez la section de dépannage, « Gestion des tâches Lifecycle Controller sur un système distant ».

Les mises à jour du BIOS sont propres au modèle de serveur utilisé. La logique de sélection est basée sur ce comportement. Parfois, même si vous sélectionnez une seule carte d'interface réseau (Network Interface Controller, NIC) 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 - Progiciel de mise à jour Dell). Actuellement, seuls les DUP inférieurs à 48 Mo sont pris en charge.

Si la taille de l'image de fichier de mise à jour dépasse cette valeur, l'état de la tâche indique que le téléchargement a échoué. Si vous lancez plusieurs mises à jour de composant sur un serveur, la taille combinée de tous les fichiers de mise à jour du micrologiciel peut également dépasser 48 Mo. Dans ce cas, une seule des mises à jour de composant 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. 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 dans l'interface Web CMC

Pour mettre à niveau le micrologiciel vers la version suivante :

1. Dans l'interface Web CMC, ouvrez l'arborescence système, accédez à **Présentation du serveur**, puis cliquez sur **Mise à jour → Mise à jour des composants de serveur**.

   La page **Mise à jour des composants de serveur** s'affiche.

2. Filtrez les composants ou périphériques (facultatif).

3. Dans la colonne **Mise à jour**, cochez les cases des composants ou périphériques dont vous voulez mettre à jour le micrologiciel vers la nouvelle version. Utilisez la touche de raccourci CRTL pour sélectionner le type de composant ou de périphérique à mettre à jour sur l'ensemble des serveurs applicables. En appuyant sur la touche CRTL et en la maintenant enfoncée, vous mettez tous les composants en surbrillance en jaune. Tout en maintenant la touche CRTL enfoncée, sélectionnez le composant ou périphérique voulu en cochant la case associée dans la colonne **Mise à jour**.

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

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

   REMARQUE : Vous pouvez ignorer la limite de taille de mise à jour d'un seul progiciel DUP ou de DUP combinés, si la fonction de stockage étendu est installée et activée. Pour plus d'informations sur l'activation du stockage étendu, voir « Configuration de la carte de stockage étendu CMC ».

4. 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.

5. Sélectionnez l'une des options suivantes :

   - **Redémarrer maintenant** : lance un redémarrage immédiat.
   - **Au prochain redémarrage** : permet de redémarrer manuellement le serveur, ultérieurement.

   REMARQUE : Cette étape n'est pas valide pour la mise à jour du micrologiciel du Lifecycle Controller et de Diagnostics 32 bits. Pour ces périphériques, le serveur est immédiatement redémarré.

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

Suppression de tâches planifiées de micrologiciel de composant de serveur

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

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

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

1. Dans l'interface Web CMC, ouvrez l'arborescence système, accédez à **Présentation du serveur**, puis cliquez sur **Mise à jour → Mise à jour des composants de serveur**.

   La page **Mise à jour des composants de serveur** s'affiche.
2. Filtrez les composants ou périphériques (facultatif).
3. Dans la colonne **Condition de la tâche**, si une case à cocher apparaît en regard de la condition de la tâche, cela signifie qu'une tâche Lifecycle Controller est en cours et porte actuellement l'état indiqué. Vous pouvez la sélectionner pour l'opération de suppression de tâche.
4. Cliquez sur **Suppression de tâches**. Les tâches sont supprimées pour les composants ou 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 (CLI) SM-CLP ou des progiciels de mise à jour propres au système d'exploitation, téléchargés depuis le site **support.dell.com**. Pour plus d'informations, voir le manuel « iDRAC User's Guide » (Guide d'utilisation de l'iDRAC).

Il est possible de restaurer un micrologiciel corrompu sur un serveur ancienne génération avec le nouveau processus de mise à jour du micrologiciel iDRAC. Lorsque CMC détecte un micrologiciel iDRAC corrompu, il répertorie le serveur correspondant dans la page **Mise à jour du micrologiciel**. Appliquez la procédure habituelle pour mettre à jour le micrologiciel.

5

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

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

- CMC actifs et de secours
- Tous les serveurs, ou chaque serveur séparément
- Matrices de stockage
- Tous les modules d'E/S (IOM), ou chaque IOM séparément
- Ventilateurs
- iKVM
- Blocs d'alimentation (PSU)
- Capteurs de température
- Ensemble d'écran LCD

Affichage des récapitulatifs de châssis et de ses composants

Lorsque vous vous connectez à l'interface Web CMC, la page **Intégrité du châssis** vous permet de connaître l'intégrité du châssis et de ses composants. Elle affiche une vue graphique en direct du châssis et des divers composants. Elle est mise à jour dynamiquement et les superpositions des sous-graphiques de composant, ainsi que les info-bulles texte, sont automatiquement mises à jour pour refléter l'état actuel.

Figure 1. Exemple de graphiques du châssis dans l'interface Web

Pour afficher l'intégrité du châssis, accédez à **Présentation du châssis** → **Propriétés** → **Intégrité**. Vous affichez ainsi la condition d'intégrité globale du châssis, des CMC actif et de secours, des modules de serveur, des modules d'E/S (IOM), des ventilateurs, des modules iKVM, des blocs d'alimentation (PSU), des capteurs de température et de l'ensemble LCD. Des informations détaillées sur chaque composant sont affichées lorsque vous cliquez sur le composant voulu. De plus,

les derniers événements du journal du matériel CMC s'affichent également. Pour plus d'informations, voir l'*Aide en ligne CMC*.

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

Graphiques du châssis

Le châssis est représenté par une vue de face et une vue de dos (images du haut et du bas, respectivement). Les serveurs et l'écran LCD sont affichés dans la vue de face et les autres composants apparaissent dans la vue de dos. Les composants sélectionnés sont signalés par un marquage bleu et vous contrôlez la sélection en cliquant sur l'image du composant requis. Lorsqu'un composant est présent dans le châssis, l'icône du type de ce composant s'affiche dans les graphiques, à la position (logement) où ce composant est installé. Les positions vides sont affichées sur fond gris sombre. L'icône du composant indique visuellement son état. Les autres composants portent des icônes qui représentent visuellement chaque composant physique. Les icônes de serveur et de module IOM couvrent plusieurs logements si vous avez installé un composant double hauteur. En pointant la souris sur un composant, vous affichez une info-bulle qui fournit des informations supplémentaires sur ce composant.

Tableau 9. : États des icônes de serveur

Icône	Description
	Le serveur est allumé et fonctionne normalement.
	Le serveur est éteint.
	Le serveur signale une erreur non critique.
	Le serveur signale une erreur critique.

Icône	Description
	Aucun serveur présent.

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 que les décrivent les journaux du matériel. Vous y trouvez également des données de performances qui varient au fil du temps.
- Propriétés : indique les propriétés de composant qui ne varient pas avec le temps, ou seulement 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.

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. Développez la section Serveurs de l'arborescence Système. Tous les serveurs (1 à 16) s'affichent dans la liste Serveurs étendue. Le nom d'un logement sans serveur est grisé.
2. En pointant avec la souris sur le nom de logement ou le numéro de logement d'un serveur, vous affichez une info-bulle contenant le nom de modèle et le numéro de service (s'il existe) du serveur.

Affichage du résumé du châssis

Vous pouvez afficher le résumé des composants installés dans le châssis.

Pour afficher les informations récapitulatives sur le châssis, accédez à l'interface Web CMC, puis cliquez sur **Présentation du châssis → Propriétés → Résumé**.

La page **Résumé du châssis** s'affiche. Pour plus d'informations, voir l'*Aide en ligne CMC*.

Affichage des informations et de la condition du contrôleur de châssis

Pour afficher les informations sur le contrôleur de châssis et sa condition, accédez à l'interface Web CMC, puis cliquez sur **Présentation du châssis → Contrôleur de châssis → Propriétés → Condition**.

La page **Condition du contrôleur de châssis** s'affiche. Pour plus d'informations, voir l'*Aide en ligne CMC*.

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 :

1. Accédez à **Présentation du châssis → Propriétés → Intégrité**.
   La page *Intégrité du châssis* affiche une vue d'ensemble graphique de tous les serveurs installés dans le châssis. La condition d'intégrité du serveur est indiquée par superposition d'une couche sur le sous-graphique de serveur. Pour plus d'informations, voir l'**Aide en ligne CMC**.
2. Accédez à **Présentation du châssis → Présentation du serveur → Propriétés → Condition**.
   La page **État des serveurs** fournit une vue d'ensemble des serveurs du châssis. Pour plus d'informations, voir l'*Aide en ligne CMC*.

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

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

1. Accédez à **Présentation du châssis → Propriétés → Intégrité**.
   La page **Intégrité du châssis** affiche une présentation graphique de tous les serveurs installés dans le châssis. L'état d'intégrité du serveur est indiqué par superposition d'une couche sur le sous-graphique de serveur. Déplacez la souris pour pointer sur chaque sous-graphique de serveur. Le texte ou l'info-bulle qui correspond fournit des informations supplémentaires sur ce serveur. Cliquez sur le sous-graphique de serveur pour afficher, à droite, les informations IOM. Pour plus d'informations, voir l'*Aide en ligne CMC*.
2. Accédez à **Présentation du châssis** et développez l'entrée **Présentation du serveur** dans l'arborescence système. Tous les serveurs (1 à 16) s'affichent dans la liste étendue. Cliquez sur le serveur (logement) à afficher.
   La page **Condition du serveur** (à ne pas confondre avec la page **Condition des serveurs**) indique l'état d'intégrité du serveur dans le châssis et permet de lancer l'interface Web iDRAC, micrologiciel utilisé pour gérer le serveur. Pour plus d'informations, voir l'*Aide en ligne CMC*.

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

Affichage de la condition de la matrice de stockage

Pour afficher l'état d'intégrité des serveurs de stockage, effectuez l'une des opérations suivantes :

1. Accédez à **Présentation du châssis → Propriétés → Intégrité**.
   La page **Intégrité du châssis** affiche une présentation graphique de tous les serveurs installés dans le châssis. L'état d'intégrité du serveur est indiqué par superposition d'une couche sur le sous-graphique de serveur. Déplacez la souris pour pointer sur chaque sous-graphique de serveur. Le texte ou l'info-bulle qui correspond

fournit des informations supplémentaires sur ce serveur. Cliquez sur le sous-graphique de serveur pour afficher, à droite, les informations IOM. Pour plus d'informations, voir l'*aide en ligne CMC*.

2. Accédez à **Présentation du châssis** et développez l'entrée **Présentation du serveur** dans l'arborescence système. Tous les logements (1 à 16) s'affichent dans la liste étendue. Cliquez sur le logement où est installée la matrice de stockage.

   La page Condition de la matrice de stockage indique l'état d'intégrité et les propriétés de la matrice concernée. Pour plus d'informations, voir l'*aide en ligne CMC*.

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

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

1. Accédez à **Présentation du châssis** → **Propriétés** → **Intégrité**.

   La page **Intégrité du châssis** s'affiche. La partie inférieure des **graphiques de châssis** affiche la vue de dos du châssis et indique l'état d'intégrité des modules IOM. Cet état d'intégrité est indiqué par superposition d'une couche sur le sous-graphique de module d'E/S (IOM). Déplacez la souris pour pointer sur chaque sous-graphique IOM. Le texte correspondant fournit des informations supplémentaires sur ce module. Cliquez sur le sous-graphique de module IOM pour afficher, à droite, les informations IOM.

2. Accédez à **Présentation du châssis** → **Présentation du module d'E/S** → **Propriétés** → **Condition**.

   La page **État du module d'E/S** affiche une vue d'ensemble de tous les modules IOM associés au châssis. Pour plus d'informations, voir l'*Aide en ligne CMC*.

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

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

1. Accédez à **Présentation du châssis** → **Propriétés** → **Intégrité**.

   La page **Intégrité du châssis** s'affiche. La partie inférieure des graphiques de châssis affiche la vue de dos du châssis et indique la condition d'intégrité des modules IOM. Cette condition est indiquée par superposition d'une couche sur le sous-graphique de module d'E/S (IOM). Déplacez la souris pour pointer sur chaque sous-graphique IOM. Le texte correspondant fournit des informations supplémentaires sur ce module. Cliquez sur le sous-graphique de module IOM pour afficher, à droite, les informations IOM.

2. Accédez à **Présentation du châssis** et développez l'entrée **Présentation du module d'E/S (IOM)** dans l'arborescence système. Tous les modules IOM (1 à 6) s'affichent dans la liste étendue. Cliquez sur l'IOM (logement) à afficher.

   La page **Condition du module d'E/S** propre au logement IOM (distincte de la page globale **Condition du module d'E/S**) s'affiche. Pour plus d'informations, voir l'*Aide en ligne CMC*.

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

CMC, qui contrôle la vitesse des ventilateurs, augmente ou réduit automatiquement la vitesse en fonction des événements à l'échelle du système. CMC génère une alerte et augmente la vitesse des ventilateurs lorsque les événements suivants se produisent :

- Le seuil de température ambiante de CMC est dépassé.

- Un ventilateur est défaillant.
- Un ventilateur est retiré du châssis.

REMARQUE : Pendant la mise à jour du micrologiciel CMC ou iDRAC sur un serveur, certaines des unités de ventilateur du châssis (ou toutes) tournent à 100 %. Ce comportement est normal.

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

1. Accédez à **Présentation du châssis → Propriétés → Intégrité**.

   La page **Intégrité du châssis** s'affiche. La partie inférieure des graphiques de châssis affiche la vue de dos du châssis et indique l'état d'intégrité du ventilateur. Cet état d'intégrité est indiqué par superposition d'une couche sur le sous-graphique de ventilateur. Déplacez la souris pour pointer sur chaque sous-graphique de ventilateur. Le texte correspondant fournit des informations supplémentaires sur le ventilateur. Cliquez sur le sous-graphique de ventilateur pour afficher, à droite, les informations de ventilateur.
2. Accédez à **Présentation du châssis → Ventilateurs → Propriétés**.

   La page **Condition des ventilateurs** indique l'état et les mesures de vitesse (en tours par minute, ou tr/mn) des ventilateurs du châssis. Il peut y avoir un ou plusieurs ventilateurs.

   REMARQUE : En cas de perte des communications entre CMC et l'unité de ventilateur, CMC ne pourra pas obtenir ni afficher la condition de l'intégrité du ventilateur.

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

Affichage des informations et de la condition d'intégrité iKVM

Le module KVM d'accès local destiné au châssis de serveur Dell M1000e est appelé Avocent Integrated KVM Switch Module, soit iKVM.

Pour afficher la condition d'intégrité des modules iKVM associés au châssis, effectuez l'une des opérations suivantes :

1. Accédez à **Présentation du châssis → Propriétés → Intégrité**.

   La page **Intégrité du châssis** s'affiche. La partie inférieure de la page de graphiques de châssis affiche la vue de dos du châssis et indique la condition d'intégrité du module iKVM. Cette condition d'intégrité est indiquée par superposition d'une couche sur le sous-graphique de module iKVM. Déplacez la souris pour pointer sur chaque sous-graphique iKVM. Le texte correspondant fournit des informations supplémentaires sur ce module. Cliquez sur le sous-graphique de module iKVM pour afficher, à droite, les informations iKVM.
2. Accédez à **Présentation du châssis → iKVM → Propriétés**.

   La page **Condition iKVM** affiche la condition et les mesures concernant le module iKVM associé au châssis. Pour plus d'informations, voir l'*Aide en ligne CMC*.

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

Pour afficher la condition d'intégrité des PSU (Power Supply Units - Blocs d'alimentation) associés au châssis, effectuez l'une des opérations suivantes :

1. Accédez à **Présentation du châssis → Propriétés → Intégrité**.

   La page **Intégrité du châssis** s'affiche. La partie inférieure de la page de graphiques de châssis affiche la vue de dos du châssis et indique la condition d'intégrité de tous les PSU. Cette condition est indiquée par superposition d'une couche sur le sous-graphique de module PSU. Déplacez la souris pour pointer sur chaque sous-graphique PSU. Le texte correspondant fournit des informations supplémentaires sur ce PSU. Cliquez sur le sous-graphique de module PSU pour afficher, à droite, les informations PSU.
2. Accédez à **Présentation du châssis → Blocs d'alimentation**.

La page **Condition des blocs d'alimentation** affiche la condition et les mesures concernant les PSU associés au châssis. Elle indique la condition d'intégrité global, la condition du système et la condition de redondance des blocs d'alimentation. Pour plus d'informations, voir l'*Aide en ligne CMC*.

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

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

Accédez à **Présentation du châssis** → **Capteurs de température**.

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

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 CMC dépasse le seuil, la vitesse des ventilateurs du châssis augmente.

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

Pour afficher la condition d'intégrité du panneau LCD :

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

   La page **Intégrité du châssis** s'affiche. La section supérieure des graphiques de châssis affiche la vue de face du châssis. La condition d'intégrité de l'écran LCD est indiquée par une superposition sur le sous-graphique LCD.
2. Pointez sur le sous-graphique LCD avec la souris. L'écran de texte ou l'info-bulle qui correspond fournit des informations supplémentaires sur l'écran LCD.
3. Cliquez sur le sous-graphique LCD pour afficher les informations LCD sur la droite. Pour plus d'informations, voir l'*Aide en ligne CMC*.

6

Configuration de CMC

CMC permet de configurer les propriétés CMC, de définir des utilisateurs et de configurer des alertes pour exécuter des tâches de gestion à distance.

Avant de commencer à configurer le CMC, vous devez configurer les paramètres réseau CMC afin de permettre la gestion à distance du CMC. Cette configuration initiale consiste à définir les paramètres de mise en réseau TCP/IP qui permettent d'accéder au CMC. Pour plus d'informations, voir « Configuration de l'accès initial à CMC ».

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

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

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

- Modifiez les paramètres réseau, si nécessaire.
- Définissez les interfaces d'accès à CMC.
- Configurez les voyants.
- Configurez des groupes de châssis, si nécessaire.
- Configurez les serveurs, et les modules IOM ou iKVM.
- Configurez les paramètres VLAN.
- Obtenez les certificats nécessaires.
- Ajoutez et configurez des utilisateurs CMC avec les privilèges voulus.
- Configurez et activez des alertes par e-mail et par interruption SNMP.
- Définissez la politique de limitation d'alimentation, si nécessaire.

Liens connexes

Connexion à CMC
Affichage et modification des paramètres réseau (LAN) CMC
Configuration des paramètres de sécurité réseau
Configuration des propriétés de marquage VLAN pour CMC
Configuration des services
Configuration des LED pour l'identification des composants du châssis
Configuration d'un groupe de châssis
Configuration du serveur
Gestion de la structure d'E/S
Configuration et utilisation d'iKVM
Obtention de certificats
Configuration des comptes et des privilèges des utilisateurs
Configuration de CMC pour envoyer des alertes
Gestion et surveillance de l'alimentation
Configuration de plusieurs CMC à l'aide de RACADM

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 vous avez deux contrôleurs CMC (actif et veille) sur le châssis, et qu'ils sont connectés au réseau, le contrôleur CMC en veille acquiert automatiquement les paramètres réseau du contrôleur CMC actif en cas de basculement.

Si IPv6 est activé lors de l'amorçage, trois sollicitations de routage sont envoyées toutes les quatre secondes. Si les commutateurs du réseau externe exécutent Spanning Tree Protocol (STP), leurs ports peuvent être bloqués pendant plus de 12 secondes, au cours desquelles les sollicitations de routage IPv6 sont envoyées. Dans ce type de 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 l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **Réseau** → **Réseau**. La page **Configuration réseau** affiche les paramètres réseau actuels.
2. Modifiez les paramètres généraux, les paramètres IPv4 et les paramètres IPv6 selon vos besoins. Pour plus d'informations, voir l'*aide en ligne CMC*.
3. Cliquez sur **Appliquer les changements** dans chaque section afin d'appliquer les paramètres.

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

Pour afficher les paramètres IPv4, utilisez les sous-commandes et objets suivants :

- `getniccfg`
- `getconfig`
- cfgCurrentLanNetworking

Pour afficher les paramètres IPv6, utilisez les sous-commandes et objets suivants :

- `getconfig`
- cfgIpv6LanNetworking

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 objets, voir le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC).

Activation de l'interface réseau CMC

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

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

REMARQUE : La NIC de CMC est activée par défaut.

Pour activer/désactiver l'adressage IPv4 de 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/désactiver les adresses 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.

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

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

```
racadm config -g cfgLanNetworking -o cfgNicUseDHCP 0 racadm config -g
cfgLanNetworking -o cfgNicIpAddress <adresse IP statique> racadm config -g
cfgLanNetworking -o cfgNicGateway <passerelle statique> racadm config -g
cfgLanNetworking -o cfgNicNetmask <masque de sous-réseau statique>
```

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 <adresse IPv6> racadm config -g
cfgIPv6LanNetworking -o cfgIPv6PrefixLength 64 racadm config -g
cfgIPv6LanNetworking -o cfgIPv6Gateway <adresse IPv6>
```

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

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

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

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

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

Pour désactiver la fonctionnalité d'utilisation du protocole DHCP pour les adresses de DNS et spécifier les adresses statiques préférées et alternatives du serveur DNS, entrez :

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

Pour désactiver la fonction de DHCP d'adresse DNS pour IPv6, et pour spécifier les adresses statiques préférée et alternative des serveurs DNS, entrez :

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

Définition des adresses IP statiques du DNS

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

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

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

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

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

Configuration des paramètres DNS (IPv4 et IPv6)

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

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

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

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

  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 fonctionnalité Négociation automatique détermine si le CMC définit automatiquement le mode duplex et la vitesse réseau en communiquant avec le routeur ou le commutateur le plus proche. La 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 <mode duplex>
```

où :

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

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

où :

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

Configuration de l'unité de transmission maximale (MTU) (IPv4 et IPv6)

La propriété MTU permet de définir la taille limite maximale de paquet pouvant être transmis via l'interface. Pour définir la valeur MTU, entrez :

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

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

REMARQUE : IPv6 nécessite une valeur MTU minimale de 1280. Si IPv6 est activé et si `cfgNetTuningMtu` est défini sur une valeur plus faible, le CMC utilise la valeur MTU 1280.

Configuration des paramètres de sécurité réseau

Vous ne pouvez configurer la sécurité réseau que pour IPv4.

Configuration des paramètres de sécurité réseau avec l'interface Web CMC

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

Pour configurer les paramètres de sécurité réseau avec l'interface Web CMC :

1. Dans l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **Réseau** → **Réseau**. La page **Configuration réseau** s'affiche.
2. Dans la section Paramètres IPv4, cliquez sur **Paramètres avancés**. La page **Sécurité réseau** s'affiche.
3. Spécifiez la plage IP et les valeurs de blocage IP. Pour plus d'informations, voir l'*aide en ligne CMC*.
4. Cliquez sur **Appliquer** pour enregistrer vos paramètres.

Configuration des paramètres de sécurité réseau CMC avec RACADM

Le filtrage IP compare l'adresse IP d'une ouverture de session entrante à la plage d'adresses IP qui est spécifiée dans les propriétés **cfgRacTuning** suivantes :

- **cfgRacTuneIpRangeAddr**
- **cfgRacTuneIpRangeMask**

La connexion à partir de l'adresse IP entrante est autorisée uniquement si les deux éléments suivants sont identiques :

- **cfgRacTuneIpRangeMask** au niveau du bit et avec une adresse IP entrante
- **cfgRacTuneIpRangeMask** au niveau du bit et avec **cfgRacTuneIpRangeAddr**

Configuration des propriétés de marquage VLAN pour CMC

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.

Configuration des propriétés de marquage VLAN pour CMC à l'aide de l'interface Web

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

1. Accédez à l'une des pages suivantes :
   - Dans l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **Réseau** → **VLAN**.
   - Dans l'arborescence système, accédez à **Présentation du châssis** → **Présentation du serveur**, puis cliquez sur **Réseau** → **VLAN**.

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

   Vous pouvez également accéder à cette page depuis le sous-onglet **Présentation du châssis** → **Serveurs** → **Configuration** → **VLAN**.

Configuration des propriétés de marquage VLAN pour CMC avec RACADM

1. Activez les fonctions VLAN du réseau de gestion du châssis externe :
   ```
   racadm config -g cfgLanNetworking -o cfgNicVLanEnable 1
   ```
2. Spécifiez le N° VLAN pour le réseau de gestion du châssis externe :
   ```
   racadm config -g cfgLanNetworking -o cfgNicVlanID <ID VLAN>
   ```

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

   Par exemple :
   ```
   racadm config -g cfgLanNetworking -o cfgNicVlanID 1
   ```
3. Spécifiez ensuite la priorité VLAN du réseau de gestion du châssis externe :
   ```
   racadm config -g cfgLanNetworking -o cfgNicVLanPriority <priorité VLAN>
   ```

   Les valeurs valides pour <priorité VLAN> sont comprises entre 0 et 7. La valeur par défaut est 0.

   Par exemple :
   ```
   racadm config -g cfgLanNetworking -o cfgNicVLanPriority 7
   ```

   Vous pouvez également spécifier l'ID du VLAN et la priorité VLAN avec une seule commande :
   ```
   racadm setniccfg -v <ID VLAN> <priorité VLAN>
   ```

   Par exemple :
   ```
   racadm setniccfg -v 1 7
   ```
4. Pour supprimer le VLAN de CMC, désactivez les fonctions VLAN du réseau de gestion du châssis externe :
   ```
   racadm config -g cfgLanNetworking -o cfgNicVLanEnable 0
   ```

   Vous pouvez également supprimer le VLAN de CMC en utilisant la commande suivante :
   ```
   racadm setniccfg -v
   ```

Configuration des services

Vous pouvez configurer et activer les services suivants dans CMC :

- Console série CMC : permet d'accéder à CMC dans la console série.
- Serveur Web : permet d'accéder à l'interface Web CMC. Si vous désactivez cette option, utilisez l'interface RACADM locale pour réactiver le serveur Web, puisque la désactivation du serveur Web désactive aussi l'interface RACADM distante.
- SSH : permet d'accéder à CMC via le RACADM micrologiciel.
- Telnet : permet d'accéder à CMC via le RACADM micrologiciel.
- RACADM : permet d'accéder à CMC avec RACADM.
- SNMP : permet à CMC d'envoyer des interruptions SNMP pour les événements.
- Journal système distant : permet à CMC de journaliser des événements sur un serveur distant.

Le CMC comprend un serveur Web configuré pour utiliser le protocole de sécurité standard SSL afin d'accepter et de 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 requêtes 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 CMC.

En cas de réinitialisation du serveur Web, attendez au moins une minute pour 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 ports 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 du privilège **Administrateur de configuration du châssis**.

Le journal système distant est une cible supplémentaire de journalisation pour CMC. Une fois que vous avez configuré le journal système distant (syslog), toute nouvelle entrée de journal générée par CMC est retransmise vers cette destination.

REMARQUE : comme le transport réseau pour les entrées de journal transférées est UDP, il n'existe aucune garantie que les entrées de journal sont délivrées, pas plus que CMC n'indique si les entrées de journal ont été correctement reçues.

Configuration des services dans l'interface Web CMC

Pour configurer les services CMC dans l'interface Web CMC :

1. Dans l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **Réseau → Services**. La page **Services** s'affiche.
2. Configurez les services suivants, si nécessaire :
   - Console série CMC
   - Serveur Web
   - SSH
   - Telnet
   - Interface RACADM distante
   - SNMP
   - Syslog distant

   Pour plus d'informations sur les champs, voir l'*aide en ligne CMC*.

3. Cliquez sur **Appliquer** pour mettre à jour l'ensemble des délais par défaut, ainsi que les délais maximaux.

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 manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC), disponible à l'adresse **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 de propriétés sont affichées sous la forme « S/O » pour une fonctionnalité non prise en charge sur le serveur.

Par exemple :

```
$ racadm getconfig -g cfgSessionManagement -m server-1 #
cfgSsnMgtWebServerMaxSessions=N/A # cfgSsnMgtWebServerActiveSessions=N/A #
cfgSsnMgtWebServerTimeout=N/A # cfgSsnMgtSSHMaxSessions=N/A #
cfgSsnMgtSSHActiveSessions=N/A # cfgSsnMgtSSHTimeout=N/A #
cfgSsnMgtTelnetMaxSessions=N/A # cfgSsnMgtTelnetActiveSessions=N/A #
cfgSsnMgtTelnetTimeout=N/A
```

Configuration de la carte de stockage étendu CMC

Vous pouvez activer ou réparer le support Flash amovible en option pour l'utiliser comme stockage étendu non volatile. Certaines fonctionnalités CMC ont besoin du stockage étendu non volatile pour fonctionner correctement.

Pour activer ou réparer le support Flash amovible dans l'interface Web CMC :

1. Dans l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **Contrôleur de châssis** → **Support Flash**. La page Support Flash amovible s'affiche.
2. Dans le menu déroulant, sélectionnez l'un des éléments suivants, selon vos besoins :
   - Utiliser le média flash pour stocker les données du châssis
   - Réparer le média du contrôleur actif
   - Commencer la réplication des données entre les médias
   - Arrêter la réplication des données entre les médias
   - Arrêter d'utiliser le média flash pour stocker les données du châssis

   Pour plus d'informations sur ces options, voir l'*aide en ligne CMC*.
3. Cliquez sur **Appliquer** pour appliquer l'option sélectionnée.

   Si le châssis contient deux CMC, ils doivent tous deux contenir un support Flash. Les fonctionnalités CMC qui dépendent du support Flash (à l'exception de Flexaddress) ne sont pas opérationnelles tant que vous n'avez pas installé et activé un support autorisé par Dell dans cette page.

Configuration d'un groupe de châssis

CMC vous permet de surveiller plusieurs châssis à partir d'un châssis maître unique. Lorsque vous activez un groupe de châssis, le CMC du châssis maître génère une image graphique de la condition de ce châssis maître et de tous les châssis membres du groupe de châssis.

Les fonctions des groupes de châssis sont les suivantes :

- La page **Groupe de châssis** affiche des vues de dos et de face de chaque châssis, à raison d'un ensemble pour le châssis maître et d'un ensemble pour chaque châssis membre.
- Les problèmes d'intégrité du maître et des membres d'un groupe sont signalés par des superpositions rouges ou jaunes, et par un X ou un point d'exclamation (!) sur le composant montrant les symptômes en question. Vous affichez des détails supplémentaires sous l'image en cliquant sur l'image de châssis ou sur **Détails**.
- Des liens de lancement rapide sont disponibles pour ouvrir les pages Web du châssis membre ou du serveur.
- Un inventaire de lames et d'E/S est disponible pour tout 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 un maximum de huit membres. De plus, un maître ou un membre ne peut appartenir qu'à un seul groupe. Vous ne pouvez pas rattacher à un groupe un châssis (que ce soit comme maître ou comme membre) déjà membre d'un autre groupe. Par contre, vous pouvez supprimer un châssis d'un groupe pour l'ajouter ensuite à un autre groupe.

Pour configurer un groupe de châssis avec l'interface Web CMC :

1. Connectez-vous au châssis maître à l'aide des privilèges administrateur du châssis.
2. Cliquez sur **Configuration** → **Administration des groupes**. La page **Groupe de châssis** s'affiche.
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 (GUI) bascule automatiquement vers la page **Groupe de châssis**. L'arborescence système indique le groupe par son nom de groupe, et le châssis maître et les châssis membres non remplis apparaissent dans l'arborescence système.

Liens connexes

Ajout de membres à un groupe de châssis
Retrait d'un membre du châssis maître
Dissolution d'un groupe de châssis
Désactivation d'un seul membre sur le châssis membre
Lancement de la page Web d'un châssis membre ou d'un serveur
Propagation des propriétés du châssis maître aux châssis membres

Ajout de membres à un groupe de châssis

Une fois le groupe du châssis configuré, des membres peuvent être ajoutés à celui-ci :

1. Connectez-vous au châssis maître à l'aide des privilèges d'administrateur.
2. Sélectionnez le châssis maître dans l'arborescence.
3. Cliquez sur **Configuration** → **Administration des groupes**.

4. Sous **Gestion des groupes**, saisissez l'adresse IP ou le nom DNS du membre dans le champ **Nom d'hôte/ Adresse IP**.
5. Dans le champ **Nom d'utilisateur** du châssis membre, saisissez un nom d'utilisateur doté de privilèges d'administrateur du châssis.
6. Saisissez le mot de passe correspondant dans le champ **Mot de passe**.
7. Cliquez sur **Appliquer**.
8. Répétez les étapes 4 à 8 pour ajouter un maximum de huit membres. Les noms de châssis des nouveaux membres s'affichent dans la boîte de dialogue **Membres**.

   Vous affichez l'état du nouveau membre en sélectionnant le groupe dans l'arborescence. Pour obtenir des détails, cliquez sur l'image du châssis ou sur le bouton de détails.

   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 membre et maître. Les références ne sont pas conservées sur chaque châssis, et ne sont plus jamais échangées après l'établissement de la relation de confiance.

   Pour plus d'informations sur la propagation des propriétés du châssis maître aux châssis membres, voir Propagation des propriétés du châssis maître aux châssis membres.

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 à l'aide des privilèges d'administrateur.
2. Sélectionnez le châssis maître dans l'arborescence.
3. Cliquez sur **Configuration → Administration des groupes**.
4. Dans la liste **Suppression de membres**, sélectionnez le nom du membre ou des membres 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.

Liens connexes

Désactivation d'un seul membre sur le châssis membre

Dissolution d'un groupe de châssis

Pour dissoudre un groupe de châssis depuis le châssis maître :

1. Connectez-vous au châssis maître avec des privilèges d'Administrateur.
2. Sélectionnez le châssis maître dans l'arborescence.
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 communique avec tous les membres pour leur signaler qu'ils ont été supprimés du groupe. Enfin, le châssis maître abandonne son rôle. Vous pouvez maintenant le désigner comme membre ou châssis maître d'un autre groupe.

   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.

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 à l'aide des privilèges d'administrateur de châssis.
2. Cliquez sur **Configuration → Administration des groupes**.
3. Sélectionnez **Aucun**, puis cliquez sur **Appliquer**.

Lancement de la page Web d'un châssis membre ou d'un serveur

La page de groupe du châssis maître contient des liens vers la page Web d'un châssis membre, vers la console distante d'un serveur ou vers la page Web d'un iDRAC de serveur appartenant au groupe. Vous pouvez utiliser pour la connexion au périphérique membre le même nom d'utilisateur et le même mot de passe que ceux ayant servi à la connexion au châssis maître. Si le périphérique membre comporte les mêmes références de connexion, aucune connexion supplémentaire n'est nécessaire. Sinon, l'utilisateur est redirigé vers la page de connexion au périphérique membre.

Pour naviguer vers les périphériques membres :

1. Ouvrez une session dans le 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 de châssis qui apparaît dans le panneau **Intégrité et alertes**, 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 CMC*.

Inventaire des serveurs pour un groupe CMC

La page Intégrité du groupe de châssis affiche tous les châssis membres et vous permet d'enregistrer le rapport d'inventaire des serveurs dans un fichier à l'aide de la fonction de téléchargement d'un navigateur standard. Le rapport contient des données concernant les éléments suivants :

- Tous les serveurs actuellement présents dans le groupe de châssis (y compris le maître).
- Logements vides et les logements d'extension (y compris les lames de pleine hauteur et de double largeur).

Enregistrement de l'inventaire des serveurs

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

1. Dans l'arborescence système, sélectionnez l'entrée **Groupe** voulue. La page **Intégrité du groupe de châssis** s'affiche.
2. Cliquez sur **Enregistrer le rapport d'inventaire**. La boîte de dialogue **Téléchargement de fichier** s'affiche, et vous invite à ouvrir ou à enregistrer le fichier.
3. Cliquez sur **Enregistrer**, et spécifiez le chemin et le nom du fichier de rapport d'inventaire des lames.

   REMARQUE : Pour que le rapport d'inventaire des lames soit le plus précis possible, le maître du groupe de châssis, le châssis membre du groupe de châssis et les lames des châssis associés doivent être allumés.

Données exportées

Le rapport d'inventaire des serveurs contient les données les plus récemment renvoyées par chaque membre du groupe de châssis au cours de l'opération d'interrogation normale du maître du groupe de châssis (toutes les 30 secondes).

Pour obtenir le rapport d'inventaire des serveurs le plus exact :

- Le maître du groupe de châssis et tous les châssis membres de ce groupe doivent avoir l'état **Alimentation de châssis activée**.
- Tous les serveurs du châssis associé doivent être allumés.

Les données d'inventaire des châssis et des serveurs associés n'apparaissent pas forcément dans le rapport d'inventaire si certains des châssis membres du groupe de châssis ont les caractéristiques suivantes :

- En état de **Alimentation de châssis désactivée**
- Hors tension

  REMARQUE : Si un serveur est inséré alors que le châssis est éteint, le numéro de modèle ne s'affiche nulle part dans l'interface Web tant que le châssis n'est pas rallumé.

Le tableau suivant répertorie les champs de données et la configuration requise spécifiques signalés pour chaque serveur :

Tableau 10. : Description des champs d'inventaire des lames

Champ de données	Exemple
Nom du châssis	Chef de châssis de centre de données
Adresse IP du châssis	192.168.0.1
Emplacement de logement	1
Nom du logement	SLOT-01
Nom d'hôte	Serveur Web d'entreprise **REMARQUE :** requiert un agent Server Administrator exécuté sur le serveur; autrement, le champ sera vierge.
Système d'exploitation	Windows Server 2008 **REMARQUE :** requiert un agent Server Administrator exécuté sur le serveur; autrement, le champ sera vierge.
Modèle	PowerEdgeM610
Numéro de service	1PB8VF1
Total de mémoire système	4 Go / **REMARQUE :** requiert un CMC 4.0 (ou ultérieur) sur le membre; autrement le champ sera vierge.
Nbr d'UC	2 **REMARQUE :** requiert un CMC 4.0 (ou ultérieur) sur le membre; autrement le champ sera vierge.
Infos sur l'UC	UC Intel (R) Xeon (R) E5502 à 1,87GHzn **REMARQUE :** requiert un CMC 4.0 (ou ultérieur) sur le membre; autrement le champ sera vierge.

Format des données

Le rapport d'inventaire est généré au format de fichier **.CSV** afin qu'il puisse être importé dans différents outils, comme Microsoft Excel. Le fichier **.CSV** de rapport d'inventaire peut être importé dans le modèle. Pour ce faire, sélectionnez **Données → À partir du texte** dans MS Excel. Une fois le rapport d'inventaire importé dans MS Excel, si un message s'affiche et vous invite à entrer des informations supplémentaires, sélectionnez l'option de fichier délimité par des virgules pour importer le fichier dans MS Excel.

Obtention de certificats

Le tableau suivant répertorie les types de certificats en fonction du type de connexion.

Tableau 11. : Types de connexion et de certificat

Type de connexion	Type de certificat	Mode d'obtention
Connexion directe en utilisant Active Directory	Certificat CA de confiance	Générer un fichier RSC et le faire signer par une autorité de certification
Connexion par carte à puce en tant qu'utilisateur Active Directory	• Certificat utilisateur • Certificat CA de confiance	• Certificat utilisateur : exportez le certificat utilisateur de carte à puce comme fichier codé en base 64 en utilisant le logiciel de gestion de carte fourni par le fournisseur de carte à puce. • Certificat CA de confiance : ce certificat est émis par une autorité de certification.
Connexion utilisateur Active Directory	Certificat CA de confiance	Ce certificat est émis par une autorité de certification.
Connexion d'utilisateur local	Certificat SSL	Générer un fichier RSC et le faire signer par une autorité de certification de confiance **REMARQUE :** CMC est livré avec un certificat de serveur SSL autosigné par défaut. Le serveur Web CMC et la console virtuelle utilisent ce certificat.

Liens connexes

Certificats de serveur Secure Sockets Layer (SSL)

Certificats de serveur Secure Sockets Layer (SSL)

Le CMC comprend un serveur Web configuré pour utiliser le protocole de sécurité standard SSL afin de transférer des données cryptées sur Internet. Reposant sur une technologie de cryptage par clé publique et clé privée, SSL est une technique très répandue d'authentification et de communication cryptée entre les clients et les serveurs pour empêcher les écoutes sur le réseau.

Le protocole SSL permet à un système compatible SSL d'effectuer les tâches suivantes :

- S'authentifier sur un client activé SSL
- Permettre au client de s'authentifier sur le serveur
- Permettre aux deux systèmes d'établir une connexion cryptée

Ce processus de cryptage fournit un haut niveau de protection des données. CMC utilise le cryptage SSL 128 bits, c'est-à-dire la forme de cryptage la plus sûre disponible pour les navigateurs Internet en Amérique du Nord.

Le serveur Web CMC inclut un certificat numérique autosigné Dell (ID de serveur). Pour renforcer la sécurité sur Internet, remplacez le certificat SSL du serveur Web en soumettant une requête à CMC pour qu'il génère une nouvelle RSC (requête de signature de certificat).

Requête de signature de certificat (RSC)

La RSC est une requête numérique adressée à une autorité de certification (appelée CA dans l'interface Web) en vue d'obtenir un certificat de serveur. Les certificats de serveur sécurisés garantissent l'identité d'un système distant, et permettent de s'assurer que les informations échangées avec le système distant ne peuvent pas être affichées ni modifiées par d'autres utilisateurs. Pour garantir la sécurité de votre CMC, il est fortement recommandé de générer une RSC, de la soumettre à une autorité de certification, puis de téléverser le certificat que vous envoie cette autorité de certification.

L'autorité de certification (CA) est une entité commerciale reconnue dans le monde informatique pour son très haut niveau de fiabilité concernant le balayage, l'identification et autres critères de sécurité importants. Certaines des CA les plus connues sont Thawte et VeriSign. Lorsque l'autorité de certification reçoit votre requête de signature de certificat (RSC), elle la passe en revue et examine les informations qu'elle contient. Si votre candidature répond aux normes de sécurité de l'autorité de certification, cette dernière émet un certificat qui vous identifie de manière unique pour les transactions sur les différents réseaux et sur Internet.

Une fois que l'autorité de certification (CA) a accepté votre RSC et vous a envoyé un certificat, vous devez téléverser ce dernier dans le micrologiciel CMC. Les informations de RSC stockées dans le micrologiciel CMC doivent correspondre au contenu du certificat.

REMARQUE : Pour configurer les paramètres SSL pour CMC, vous devez disposer du privilège **Administrateur de configuration du châssis**.

REMARQUE : Les certificats de serveur que vous téléversez doivent être valides (ils ne doivent pas avoir expiré) et signés par une autorité de certification.

Liens connexes

Génération d'une nouvelle demande de signature de certificat
Téléversement d'un certificat d'un serveur
Affichage du certificat de serveur

Génération d'une nouvelle demande de signature de certificat

Pour garantir la sécurité, il est fortement recommandé d'obtenir un certificat de serveur sécurisé et de le téléverser dans CMC. Les certificats de serveur sécurisés vérifient l'identité d'un système distant, et garantissent que les informations échangées avec le système distant ne peuvent pas être affichées ni modifiées par d'autres utilisateurs. Sans certificat de serveur sécurisé, le CMC est vulnérable et accessible par des utilisateurs non autorisés.

Pour obtenir un certificat de serveur sécurisé pour CMC, vous devez soumettre une RSC (requête de signature de certificat) à l'autorité de certification de votre choix. Une RSC est une requête numérique visant à obtenir un certificat de serveur sécurisé signé contenant des informations sur votre organisation et une clé d'identification unique.

Après avoir généré la requête de signature de certificat (RSC), vous êtes invité à en enregistrer une copie sur votre station de gestion ou réseau partagé ; les informations uniques qui ont servi à générer la RSC sont stockées dans CMC. Ces informations serviront ultérieurement à authentifier le certificat de serveur que vous enverra l'autorité de certification (CA). Dès réception de ce certificat de la CA, vous devez le téléverser dans CMC.

REMARQUE : Pour que CMC puisse accepter le certificat de serveur renvoyé par l'autorité de certification, les informations d'authentification contenues dans le nouveau certificat doivent correspondre aux informations stockées sur CMC lors de la génération de la RSC.

PRÉCAUTION : Lorsqu'une nouvelle RSC est générée, elle remplace toutes les requêtes précédentes du CMC. Ainsi, si vous remplacez une requête de signature de certificat (RSC) avant que l'autorité de certification ne vous ait fourni le certificat correspondant, le CMC n'accepte pas le certificat de serveur car les informations qu'il utilise pour authentifier ce certificat sont perdues. Soyez prudent, lorsque vous générez une RSC, afin de ne pas remplacer une RSC en attente.

Génération d'une nouvelle requête de signature de certificat (RSC) dans l'interface Web

Pour générer une RSC à l'aide de l'interface Web CMC :

1. Dans l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **Réseau** → **SSL**. La fenêtre **Menu principal SSL** s'affiche.
2. Sélectionnez **Générer une nouvelle requête de signature de certificat (RSC)** et cliquez sur **Suivant**. La page **Générer une requête de signature de certificat (CSR)** s'affiche.
3. Entrez une valeur pour chaque attribut de la RSC.
4. Cliquez sur **Générer**. La boîte de dialogue **Téléchargement de fichier** s'affiche.
5. Enregistrez le fichier **csr.txt** sur votre station de gestion ou réseau partagé. (Vous pouvez également ouvrir immédiatement le fichier mais l'enregistrer plus tard.) Vous devez ensuite soumettre ce fichier à une autorité de certification (CA).

Génération d'un fichier RSC à l'aide de l'interface RACADM

Pour générer un fichier RSC, utilisez les objets du groupe `cfgRacSecurityData` pour spécifier les valeurs et la commande `sslcsrgen` pour générer le fichier RSC. Pour plus d'informations, voir le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC), disponible sur le site **dell.com/support/manuals**.

Téléversement d'un certificat d'un serveur

Après avoir généré un fichier RSC, vous pouvez téléverser le certificat de serveur SSL signé vers le micrologiciel CMC. CMC se réinitialise après que le certificat a été téléversé. CMC accepte uniquement les certificats de serveur Web X509 codés en Base 64.

PRÉCAUTION : Au cours du téléversement du certificat, CMC n'est pas disponible.

Téléversement d'un certificat de serveur à l'aide de l'interface Web CMC

Pour téléverser un certificat de serveur avec l'interface Web CMC :

1. Dans l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **Réseau** → **SSL**. La fenêtre **Menu principal SSL** s'affiche.
2. Sélectionnez l'option **Téléverser un certificat de serveur d'après la RSC générée** et cliquez sur **Suivant**.
3. Cliquez sur **Choisir un fichier** et spécifiez le fichier de certificat.
4. Cliquez sur **Appliquer**. Si le certificat n'est pas valide, un message d'erreur s'affiche.

REMARQUE : La valeur **Chemin du fichier** indique le chemin relatif du fichier de certificat que vous téléversez. Vous devez saisir le chemin absolu de ce fichier, à savoir son chemin complet, son nom et son extension.

Téléversement d'un certificat de serveur à l'aide de l'interface RACADM

Pour charger le certificat de serveur SSL, utilisez la commande `sslcertupload`. Pour plus d'informations, voir le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC), disponible sur le site **dell.com/support/manuals**.

Téléversement d'une clé et d'un certificat de serveur Web

Vous pouvez téléverser une clé de serveur Web et un certificat de serveur correspondant à cette clé. Ce certificat de serveur est émis par l'autorité de certification (CA).

Le certificat de serveur Web est un élément essentiel du processus de cryptage SSL. Il s'authentifie auprès d'un client SSL et permet à ce client de s'authentifier auprès du serveur, permettant ainsi aux deux systèmes d'établir une connexion cryptée.

REMARQUE : Pour téléverser une clé et un certificat de serveur Web Server, vous devez disposer de droits d'**Administrateur de configuration du châssis**.

Téléversement d'une clé et d'un certificat de serveur Web avec RACADM

Pour téléverser une clé et un certificat de serveur Web avec l'interface Web CMC :

1. Dans l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **Réseau → SSL**. Le **Menu principal SSL** s'affiche.
2. Sélectionnez **Téléverser la clé et le certificat de serveur Web**, puis cliquez sur **Suivant**.
3. Spécifiez le fichier de clé privée et le fichier de certificat en cliquant sur **Choisir un fichier**.
4. Une fois les deux fichiers téléversés, cliquez sur **Appliquer**. Si la clé et le certificat de serveur Web ne correspondent pas, un message d'erreur s'affiche.

   REMARQUE : CMC accepte uniquement les certificats X509 codé en Base-64. Les certificats utilisant d'autres schémas de codage, comme DER, ne sont pas acceptés. Le téléversement d'un nouveau certificat remplace le certificat par défaut reçu avec votre CMC.

   CMC se réinitialise et devient temporairement indisponible après le téléversement réussi du certificat. Pour éviter de déconnecter d'autres utilisateurs pendant la réinitialisation, prévenez les utilisateurs autorisés susceptibles de se connecter à CMC et vérifiez les sessions activez dans la page **Sessions**, dans l'onglet **Réseau**.

Téléversement d'une clé et d'un certificat de serveur Web à l'aide de RACADM

Pour téléverser une clé SSL depuis le client vers l'iDRAC, entrez la commande suivante :

```
racadm sslkeyupload -t <type> -f <nom de fichier>
```

Pour plus d'informations, voir le manuel *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible sur le site **dell.com/support/manuals**.

Affichage du certificat de serveur

Vous pouvez afficher le certificat de serveur SSL actuel utilisé dans CMC.

Affichage d'un certificat de serveur à l'aide de l'interface Web

Dans l'interface Web CMC, accédez à **Présentation du châssis → Réseau → SSL**, sélectionnez **Afficher le certificat de serveur**, puis cliquez sur Suivant. La page Afficher le certificat de serveur affiche le certificat de serveur SSL actuellement utilisé. Pour plus d'informations, voir l'aide en ligne CMC.

Affichage d'un certificat de serveur à l'aide de l'interface RACADM

Pour afficher un certificat de serveur SSL, utilisez la commande `sslcertview`. Pour plus d'informations, voir le manuel *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible sur le site **dell.com/support/manuals**.

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 spécifique à l'aide de 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 CMC, vous pouvez configurer vos 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` (étape 1) demande la configuration CMC de la carte CMC active et génère le fichier **myfile.cfg**. Si nécessaire, vous pouvez renommer ce fichier ou l'enregistrer à un autre emplacement.

   Vous pouvez utiliser la commande getconfig pour effectuer les actions suivantes :

   - afficher toutes les propriétés de configuration dans un groupe (spécifié par le nom de groupe et l'index),
   - afficher toutes les propriétés de configuration pour 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.

Liens connexes

Création d'un fichier de configuration CMC

Création d'un fichier de configuration CMC

Le fichier de configuration CMC, **<nom de fichier>.cfg**, est utilisé avec la commande `racadm config -f <nom de fichier>.cfg` pour créer un fichier texte simple. Cette commande vous permet de créer un fichier de configuration (semblable à un **.ini**) et de configurer le CMC à partir de ce fichier.

Vous pouvez utiliser n'importe quel nom de fichier, et le fichier ne nécessite pas d'extension **.cfg** (même s'il est désigné par cette extension dans cette sous-section).

REMARQUE : Pour des informations supplémentaires sur la sous-commande `getconfig`, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC).

RACADM analyse le fichier **.cfg** lors de son premier chargement dans le CMC pour vérifier qu'il contient des noms de groupe et d'objet valides, et que les règles de syntaxe simples sont appliquées. Les erreurs sont signalées, avec le

numéro de ligne où elles ont été détectées et un message qui décrit le problème. Le fichier entier est analysé pour vérifier qu'il est correct et toutes les erreurs s'affichent. Les commandes d'écriture ne sont pas transmises au CMC si une erreur est détectée dans le fichier **.cfg**. Vous devez corriger toutes les erreurs pour que la configuration se produise.

Pour rechercher les erreurs avant de créer le fichier de configuration, utilisez l'option `-c` avec la sous-commande `config`. L'option `-c` ne demande à la commande `config` que de vérifier la syntaxe, sans écrire dans le CMC.

Tenez compte des consignes suivantes lorsque vous créez un fichier **.cfg** :

- Si l'analyseur rencontre un groupe indexé, c'est la valeur de l'objet ancré qui différencie les différents index.
  L'analyseur lit tous les index de ce groupe depuis le CMC. Tous les objets de ce groupe sont modifiés lors de la configuration du CMC. Si un objet modifié représente un nouvel index, cet index est créé dans le CMC pendant la configuration.
- Vous ne pouvez pas choisir les index désirés dans un fichier **.cfg**.
  Vous pouvez créer et supprimer des index. Au fil du temps, le groupe peut être fragmenté en raison des index utilisés et non utilisés. Si un index est présent, il est modifié. Si aucun index n'est présent, le système utilise le premier index disponible.

  Cette méthode permet d'être flexible dans l'ajout d'entrées d'index, car il est inutile de faire correspondre exactement les index entre tous les CMC gérés. Les nouveaux utilisateurs sont ajoutés au premier index disponible. Un fichier **.cfg** correctement analysé et exécuté sur un CMC donné risque de ne pas fonctionner correctement sur un autre, si tous les index sont complets et que vous devez ajouter un nouvel utilisateur.
- Utilisez la sous-commande `racresetcfg` pour configurer les deux CMC avec des propriétés identiques.
  Utilisez la sous-commande `racresetcfg` pour réinitialiser les valeurs par défaut d'origine du CMC, puis exécutez la commande `racadm config -f <nom du fichier>.cfg`. Vérifiez que le fichier **.cfg** inclut tous les objets, utilisateurs, index et autres paramètres nécessaires. Pour consulter la liste complète des objets et des groupes, voir le chapitre traitant des propriétés de base de données, dans le manuel « *RACADM Command Line Reference Guide for iDRAC6 and CMC* » (Guide de référence de la ligne de commande RACADM pour iDRAC6 et CMC).

  PRÉCAUTION : Utilisez la sous-commande `racresetcfg` pour réinitialiser la base de données et les paramètres d'interface réseau CM sur les valeurs par défaut d'origine, et pour supprimer tous les utilisateurs et configurations utilisateur. Bien que l'utilisateur root soit disponible, les valeurs par défaut des paramètres des autres utilisateurs sont également réinitialisées.
- Si vous entrez `racadm getconfig -f <nom de fichier>.cfg`, la commande génère un fichier **.cfg** pour la configuration CMC actuelle. Ce fichier de configuration peut être utilisé comme exemple et comme point de départ pour votre propre fichier **.cfg**.

Liens connexes

Règles d'analyse

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 <nom du fichier> .cfg`, puis à exécuter la commande `racadm config -f <nom du fichier> .cfg` sur un autre CMC, sans ajouter de caractère d'échappement.

Par exemple :

```
# # Ceci est un commentaire [cfgUserAdmin]
cfgUserAdminPageModemInitString= <Modem init # n'est pas un commentaire>
```

- 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 iDRAC6 and CMC* » (Guide de référence de l'interface de ligne de commande RACADM pour iDRAC6 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 signé 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 <nom de fichier>.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 <nom de groupe> -o <objet ancré> -i <index 1 à 16>
  <nom d'ancre unique>
  ```

- 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 <nom de groupe> -o <nom d'objet> -i <index 1 à 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 <nom de groupe> -i <index 1 à 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= <NOM_UTILISATEUR>
  ```

- Lorsque vous utilisez l'interface RACADM à distance 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 vers d'autres CMC, la propriété de clé doit être définie avant l'exécution de la commande `getconfig -f`. Sinon, vous pouvez 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 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 <monfichier>.cfg`.

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

Affichage et fermeture de sessions CMC

Vous pouvez afficher le nombre d'utilisateurs connectés à iDRAC7 et mettre fin aux sessions utilisateur.

REMARQUE : Pour mettre fin à une session, vous devez disposer du privilège d'**Administrateur de configuration du châssis**.

Affichage et fermeture de sessions CMC à l'aide de l'interface Web

Pour afficher une session ou y mettre fin avec l'interface Web :

1. Dans l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **Réseau** → **Sessions**.
   La page **Sessions** affiche l'ID de session, le nom d'utilisateur, l'adresse IP et le type de session. Pour plus d'informations sur ces propriétés, voir l'*Aide en ligne CMC*.
2. Pour mettre fin à la session, cliquez sur **Fermer** en regard de la session en question.

Affichage et fermeture des sessions CMC avec RACADM

Vous devez disposer de privilèges Administrateur pour pouvoir mettre fin aux sessions CMC avec RACADM.

Pour afficher les sessions utilisateur en cours, utilisez la commande `getssninfo`.

Pour mettre fin à une session utilisateur, utilisez la commande `closessn`.

Pour plus d'informations sur ces commandes, voir le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC), disponible sur le site **dell.com/support/manuals**.

7

Configuration du serveur

Vous pouvez réaliser les opérations suivantes pour le serveur :

- Configuration des noms de logement
- Configuration des paramètres réseau iDRAC
- Configuration des paramètres de marquage VLAN iDRAC
- Définition du premier périphérique de démarrage
- Configuration de FlexAddress pour serveur
- Configuration d'un partage de fichiers distant
- Configuration des paramètres BIOS par clonage de serveur

Configuration des noms de logement

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

- Les noms peuvent contenir un **maximum de 15** caractères ASCII non étendus (codes ASCII de 32 à 126).
- Les noms de logement doivent être uniques dans le châssis. Il ne peut pas exister deux logements portant le même nom.
- Les chaînes ne sont pas sensibles à la casse. `Serveur-1, serveur-1 et SERVEUR-1` sont des noms identiques.
- Les noms de logements ne doivent pas commencer par les chaînes de caractères suivantes :
  - `Switch- (Commutateur-)`
  - `Fan- (Ventilateur-)`
  - `PS-`
  - `KVM`
  - `DRAC-`
  - `MC-`
  - `Châssis`
  - `Housing-Left (Boîtier-Gauche)`
  - `Housing-Right (Boîtier-Droite)`
  - `Housing-Center (Boîtier-Centre)`
- Les chaînes `Serveur-1` à `Serveur-16` peuvent être utilisées, mais uniquement pour le logement indiqué. Par exemple, `Serveur-3` est un nom valide pour le logement 3 mais pas pour le logement 4. Par contre, `Serveur-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 CMC. Si vous retirez un serveur du châssis, son nom ne le suit pas.

Le paramètre de nom de logement ne s'applique pas au module iKVM en option. Les informations de nom de logement sont disponibles dans l'unité remplaçable sur site (FRU) iKVM.

La configuration du nom d'un logement dans l'interface Web CMC supplante 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 l'arborescence système, accédez à **Présentation du châssis** → **Présentation du serveur**, puis cliquez sur **Configuration** → **Noms de logement**. La page **Noms de logement** s'affiche.
2. Dans le champ **Nom du logement**, modifiez le nom affiché. Répétez l'opération pour chacun des logements à renommer.
3. Pour utiliser le nom d'hôte du serveur comme nom de logement, sélectionnez la valeur **Utiliser le nom d'hôte** pour l'option **Nom du 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 manuel « *Dell OpenManage Server Administrator User's Guide* » (Guide d'utilisation de Dell OpenManage Server Administrator).
4. Cliquez sur **Appliquer** pour enregistrer les paramètres.
5. Pour restaurer le nom de logement par défaut du serveur (**SLOT-01** à **SLOT-16**, en fonction de la position du logement du serveur concerné), cliquez sur **Restaurer la valeur par défaut**.

Configuration des paramètres réseau iDRAC

Vous pouvez définir les paramètres de configuration réseau iDRAC d'un serveur installé ou d'un serveur nouvellement inséré. L'utilisateur peut configurer un ou plusieurs périphériques iDRAC installés. Il peut également définir les paramètres de configuration réseau iDRAC par défaut et le mot de passe racine (root) des serveurs installés ultérieurement ; ces paramètres par défaut sont les paramètres QuickDeploy (Déploiement rapide) iDRAC.

Pour plus d'informations sur iDRAC, voir le manuel « *iDRAC7 User's Guide* » (Guide d'utilisation d'iDRAC7), à l'adresse **dell.com/support/manuals**.

Liens connexes

Configuration des paramètres réseau QuickDeploy (Déploiement rapide) iDRAC
Modification des paramètres réseau iDRAC de chaque iDRAC de serveur
Modification des paramètres réseau iDRAC avec RACADM

Configuration des paramètres réseau QuickDeploy (Déploiement rapide) iDRAC

Utilisez les paramètres QuickDeploy pour configurer les paramètres réseau des serveurs nouvellement insérés. Après l'activation de QuickDeploy, les paramètres QuickDeploy sont appliqués aux serveurs lors de leur installation.

Pour activer et définir les paramètres QuickDeploy (Déploiement rapide) iDRAC avec l'interface Web CMC :

1. Dans l'arborescence système, accédez à **Présentation du serveur**, puis cliquez sur **Configuration** → **iDRAC**. La page **Déployer iDRAC** s'affiche.
2. Dans la section **Paramètres QuickDeploy**, spécifiez les paramètres décrits dans le tableau suivant.

Tableau 12. : Paramètres QuickDeploy

Paramètre	Description
QuickDeploy activé	Active/désactive la fonctionnalité **QuickDeploy**, qui applique automatiquement les paramètres iDRAC configurés dans cette page aux serveurs nouvellement insérés. La configuration automatique doit être confirmée localement sur le panneau LCD.

Paramètre	Description
	REMARQUE : Cela inclut le mot de passe de l'utilisateur racine si la case **Définir le mot de passe racine d'iDRAC sur l'insertion de serveur** est cochée. Par défaut, cette option est désactivée.
Définir le mot de passe racine d'iDRAC lors de l'insertion du serveur	Spécifie si le mot de passe iDRAC racine d'un serveur doit être remplacé par la valeur fournie dans la boîte de dialogue **Mot de passe racine iDRAC** lorsque ce serveur est inséré.
Mot de passe racine d'iDRAC	Si vous sélectionnez les options **Définir le mot de passe de root iDRAC lors de l'insertion du serveur** et **QuickDeploy activé**, cette valeur de mot de passe remplace le mot de passe d'utilisateur root (racine) iDRAC d'un serveur lorsque vous insérez ce serveur dans le châssis. Ce mot de passe peut contenir de 1 à 20 caractères imprimables (espaces compris).
Confirmez le mot de passe racine d'iDRAC	Vérifie le mot de passe entré dans le champ **Mot de passe racine d'iDRAC**.
Activer le LAN pour iDRAC	Permet d'activer ou de désactiver le canal LAN iDRAC. Par défaut, cette option est désactivée.
Activer IPv4 pour iDRAC	Permet d'activer ou de désactiver IPv4 sur l'iDRAC. Par défaut, cette option est activée.
Activer IPMI sur le LAN pour iDRAC	Permet d'activer ou de désactiver la fonction IPMI sur canal LAN pour chaque iDRAC présent dans le châssis. Par défaut, cette option est désactivée.
Activer DHCP pour iDRAC	Permet d'activer ou de désactiver DHCP pour chaque iDRAC présent dans le châssis. Si vous activez cette option, les champs **Adresse IP QuickDeploy**, **Masque de sous-réseau QuickDeploy** et **Passerelle QuickDeploy** sont désactivés, et vous ne pouvez pas les modifier, puisque DHCP sert à attribuer automatiquement ces paramètres à chaque iDRAC. Par défaut, cette option est désactivée.
Première adresse IPv4 d'iDRAC (logement 1)	Spécifie l'adresse IP statique de l'iDRAC du serveur installé dans le logement 1 de l'enceinte. L'adresse IP de chacun des iDRAC suivants est incrémentée de 1 pour chaque logement, à partir de l'adresse IP statique du logement 1. Lorsque la valeur « adresse IP plus numéro de logement » est supérieure au masque de sous-réseau, un message d'erreur s'affiche. **REMARQUE :** Le masque de sous-réseau et la passerelle ne sont pas incrémentés comme l'adresse IP.

Paramètre	Description
	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 15 est `192.168.0.265`. Si le masque de sous-réseau est `255.255.255.0`, un message d'erreur vous signale `La plage d'adresses IP QuickDeploy n'est pas entièrement dans le sous-réseau QuickDeploy`, lorsque vous cliquez sur **Enregistrer les paramètres QuickDeploy** ou **Remplir automatiquement avec les paramètres QuickDeploy**.
Masque de réseau IPv4 d'iDRAC	Spécifie le masque de sous-réseau QuickDeploy assigné à tout serveur nouvellement inséré.
Passerelle IPv4 d'iDRAC	Spécifie la passerelle par défaut QuickDeploy assignée à tout iDRAC présent dans le châssis.
Activer IPv6 pour iDRAC	Active l'adressage IPv6 pour chaque contrôleur iDRAC présent dans le châssis prenant en charge IPv6.
Activer la configuration automatique IPv6 d'iDRAC	Permet à l'iDRAC d'obtenir les paramètres IPv6 (adresse et longueur de préfixe) auprès d'un serveur DHCPv6 et autorise également la configuration automatique des adresses sans état. Par défaut, cette option est activée.
Passerelle IPv6 d'iDRAC	Spécifie la passerelle IPv6 à attribuer aux iDRAC. La valeur par défaut est « :: ».
Longueur du préfixe IPv6 d'iDRAC	Spécifie la longueur de préfixe à attribuer pour les adresses IPv6 de l'iDRAC. La valeur par défaut est 64.

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 s'exécute uniquement si vous l'avez activée et si un serveur a été inséré dans le châssis. Si vous activez les options **Définir le mot de passe de root iDRAC lors de l'insertion du serveur** et **QuickDeploy activé**, l'utilisateur est invité, via l'interface LCD, à autoriser ou refuser le changement de mot de passe. Si certains paramètres de configuration réseau diffèrent des paramètres iDRAC actuels, l'utilisateur est invité à accepter ou refuser les changements.

   REMARQUE : En cas de différence dans le LAN ou dans IPMI sur LAN, l'utilisateur est invité à accepter le paramètre d'adresse IP QuickDeploy. Si cette différence porte sur le paramètre DHCP, l'utilisateur est invité à accepter le paramètre DHCP QuickDeploy.

   Pour copier les paramètres QuickDeploy vers la section **Paramètres réseau iDRAC**, cliquez sur **Remplir automatiquement avec les paramètres QuickDeploy**. Les paramètres de configuration réseau QuickDeploy sont copiés vers les champs correspondants de la table **Paramètres de configuration réseau iDRAC**.

   REMARQUE : Les modifications apportées aux champs QuickDeploy 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 de chaque iDRAC de serveur

Utilisez ce tableau pour configurer les paramètres réseau iDRAC de chaque serveur installé. Les valeurs initiales affichées pour chaque champ sont les valeurs actuelles lues depuis l'iDRAC.

Pour modifier les paramètres réseau iDRAC avec l'interface Web CMC :

1. Dans l'arborescence système, accédez à **Présentation du serveur**, puis cliquez sur **Configuration → iDRAC**. La page **Déployer iDRAC** s'affiche. La section **Paramètres réseau iDRAC** répertorie les paramètres de configuration réseau IPv4 et IPv6 iDRAC de tous les serveurs installés.
2. Modifiez les paramètres réseau iDRAC selon vos besoins pour le ou les serveurs.

   REMARQUE : Vous devez sélectionner l'option **Activer LAN** pour spécifier les paramètres IPv4 ou IPv6. Pour plus d'informations sur les champs, voir l'Aide en ligne CMC.
3. Pour déployer les paramètres vers l'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 plus d'informations sur les valeurs par défaut des propriétés et sur les plages, voir le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC).

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 le VLAN pour un serveur à l'aide de l'interface Web CMC :

1. Accédez à l'une des pages suivantes :
   - Dans l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **Réseau → VLAN**?.
   - Dans l'arborescence système, accédez à **Présentation du châssis → Présentation du serveur**, puis cliquez sur **Réseau → VLAN**?. La page **Paramètres de marquage VLAN** s'affiche.
2. Dans la section **iDRAC**, activez le VLAN pour le ou les serveurs, définissez la priorité et entrez l'ID approprié. Pour plus d'informations sur les champs, voir l'*aide en ligne CMC*.
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 <ID VLAN> <priorité VLAN>
  ```
  Les valeurs valides pour `<n>` sont comprises entre 1 et 16.

  Les valeurs valides pour `<ID VLAN>` sont comprises entre 1 et 4 000, et entre 4 021 et 4 094.

  Les valeurs valides pour `<priorité VLAN>` sont comprises entre 0 et 7. Valeur par défaut : 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 pour `<n>` sont comprises entre 1 et 16.

  Par exemple :
  ```
  racadm setniccfg -m server-1 -v
  ```

Définition du premier périphérique de démarrage

Vous pouvez préciser le premier périphérique d'amorçage CMC de chaque serveur. Il ne s'agit pas forcément du vrai premier périphérique d'amorçage du serveur, ni même d'un périphérique présent dans ce serveur. Il s'agit plutôt d'un périphérique envoyé par CMC au serveur pour que ce serveur le reconnaisse comme premier périphérique d'amorçage de CMC.

Vous pouvez définir le périphérique d'amorçage par défaut et indiquer un périphérique d'amorçage à usage unique, qui servira à amorcer une image pour effectuer des tâches telles que l'exécution de diagnostics ou la réinstallation d'un système d'exploitation.

Vous pouvez définir le premier périphérique d'amorçage pour l'amorçage suivant uniquement ou pour tous les amorçages à venir. En fonction de cette sélection, vous pouvez définir le premier périphérique de démarrage du serveur. Le système s'amorce sur le périphérique sélectionné lors du redémarrage suivant et des redémarrages ultérieurs, et ce périphérique reste le premier dans la séquence d'amorçage du BIOS jusqu'à ce que vous le changiez à nouveau dans l'interface Web CMC ou dans la séquence d'amorçage du BIOS.

REMARQUE : Le paramètre de premier périphérique d'amorçage défini dans l'interface Web CMC écrase les paramètres d'amorçage du BIOS système.

Le périphérique d'amorçage spécifié doit exister et contenir un support amorçable.

Vous pouvez définir les périphériques suivant comme premier périphérique d'amorçage.

Tableau 13. : Périphériques d'amorçage

Périphérique d'amorçage	Description
PXE	Permet de démarrer à partir d'un protocole PXE (environnement d'exécution prédémarrage) sur la carte d'interface réseau.
Disque dur	Permet de démarrer à partir du disque dur sur le serveur.
CD/DVD local	Permet de démarrer à partir d'un lecteur de CD/DVD sur le serveur.
Disquette virtuelle	Amorçage sur le lecteur de disquette virtuel. Ce lecteur de disquette (ou image de disquette) se trouve sur un autre ordinateur du réseau de gestion et est rattaché via la visionneuse de console de l'interface utilisateur graphique (GUI) iDRAC.
CD/DVD virtuel	Amorçage sur un lecteur de CD/DVD virtuel ou sur une image ISO de CD/DVD. Ce lecteur optique (ou cette image ISO) se trouve sur un autre ordinateur ou disque disponible sur le réseau de gestion, et est rattaché via la visionneuse de console de l'interface utilisateur graphique (GUI) iDRAC.
iSCSI	Permet de démarrer à partir d'un périphérique Internet SCSI (interface système pour micro-ordinateur).
Carte SD locale	Démarrer à partir de la carte locale SD(Secure Digital) : uniquement pour les serveurs prenant en charge les systèmes iDRAC6 et iDRAC7.
Disquette	Démarrer à partir d'une disquette insérée dans le lecteur local de disquette.
RFS	Démarrer à partir d'une image RFS (Remote File Share - Partage de fichiers distant). Ce fichier d'image de disquette est rattaché via la visionneuse de console de l'interface utilisateur graphique (GUI) iDRAC.

Liens connexes

Définition du premier périphérique d'amorçage pour plusieurs serveurs dans l'interface Web CMC

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

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

Définition du premier périphérique d'amorçage pour plusieurs serveurs 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 pour plusieurs serveurs avec l'interface Web CMC :

1. Dans l'arborescence système, accédez à **Présentation du serveur**, puis cliquez sur **Configuration → Périphérique de démarrage initial**. La liste des serveurs s'affiche.
2. Dans la colonne **Périphérique de démarrage initial**, sélectionnez dans le menu déroulant le périphérique d'amorçage à utiliser pour chaque 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

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

Pour définir le premier périphérique d'amorçage pour un serveur spécifique avec l'interface Web CMC :

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

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

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

Pour activer l'option d'amorçage unique pour un périphérique, utilisez l'objet `cfgServerBootOnce`.

Pour plus d'informations sur ces objets, voir le manuel « *RACADM Command Line Reference Guide for iDRAC and CMC* » (Guide de référence de la ligne de commande RACADM pour iDRAC et CMC), disponible à l'adresse **dell.com/support/manuals**.

Configuration de FlexAddress pour serveur

Pour plus d'informations sur la configuration de FlexAddress pour les serveurs, voir « Configuration de FlexAddress pour les logements de niveau serveur ».

Configuration d'un partage de fichiers distant

La fonction de partage de fichiers sur support virtuel distant associe un fichier issu d'un lecteur de partage sur le réseau à un ou plusieurs serveurs, via 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 le système local. Deux types de support sont pris en charge : les disquettes et les lecteurs de CD/DVD.

Pour effectuer une opération de partage de fichiers à distance (connexion, déconnexion ou déploiement), vous devez disposer de droits d'Administrateur de châssis ou d'Administrateur de serveur.

Pour configurer le partage de fichiers distant dans l'interface Web CMC :

1. Dans l'arborescence système, accédez à **Présentation du serveur**, puis cliquez sur **Configuration → Partage de fichiers distant**. La page **Déployer un partage de fichiers distant** s'affiche.

   Entrez le résultat de cette opération ici (facultatif).
2. Spécifiez les paramètres voulus. Pour plus d'informations, voir l'*aide en ligne CMC*.
3. Cliquez sur **Connecter** pour vous connecter au partage de fichiers distant. Pour cette connexion, vous devez indiquer le chemin, le nom d'utilisateur et le mot de passe. La réussite de l'opération vous permet d'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 : Enregistrez tous les fichiers de travail avant d'exécuter la commande `Déployer` car cette action entraîne le redémarrage du serveur.

   Cette commande implique les actions suivantes :

   - 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 était hors tension.

Configuration des paramètres BIOS par clonage de serveur

La fonction de clonage de serveur vous permet d'appliquer tous les paramètres BIOS du serveur spécifié à un ou plusieurs autres serveurs. Les paramètres BIOS pouvant être clonés sont ceux qui sont modifiables et conçus pour être répliqués d'un serveur à l'autre.

La fonction de clonage de serveur prend en charge les serveurs iDRAC6 et iDRAC7. Les serveurs RAC ancienne génération sont répertoriés, mais ils sont grisés sur la page principale et vous ne pouvez pas y utiliser cette fonction.

Pour utiliser la fonction de clonage de serveur :

- Vous devez installer la version minimale d'iDRAC requise. Les serveurs iDRAC6 doivent utiliser la version 3.2 ou supérieure, et les serveurs iDRAC7 doivent comporter la version 1.00.00.
- Le serveur doit disposer d'une génération prise en charge d'iDRAC.
- Le serveur doit être sous tension.

Les serveurs source et cible ne doivent pas forcément être de même génération. Seuls les paramètres clonables disponibles sont appliqués d'un profil de serveur aux autres serveurs.

Vous pouvez :

- Copier les paramètres du BIOS d'un serveur à un autre.
- Enregistrer le profil d'un serveur.
- Appliquer un profil à d'autres serveurs.
- Afficher les paramètres du BIOS d'un serveur ou ceux d'un profil enregistré.
- Afficher les activités dans le journal pour des tâches récentes d'un profil du BIOS.

Liens connexes

Accès à la page Profil BIOS

Ajout ou enregistrement d'un profil

Gestion des profils stockés
Application d'un profil
Affichage des paramètres BIOS
Affichage du journal de profil
Condition d'achèvement et dépannage

Accès à la page Profil BIOS

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

Pour accéder à la page Profil BIOS à l'aide de l'interface Web CMC, accédez à l'arborescence système, puis à **Présentation du châssis** → **Présentation du serveur** et cliquez sur **Configuration** → **Profils**. La page **Profils BIOS** s'affiche.

Liens connexes

Ajout ou enregistrement d'un profil
Gestion des profils stockés
Application d'un profil
Affichage des paramètres BIOS
Affichage du journal de profil
Condition d'achèvement et dépannage

Ajout ou enregistrement d'un profil

Avant de cloner les propriétés BIOS d'un serveur depuis la racine, vous devez capturer ces propriétés dans un profil stocké.

Lors de la création d'un profil stocké, vous entrez un nom et (facultatif) une description pour chaque profil. Vous pouvez enregistrer un maximum de 16 profils stockés sur le support de stockage étendu non volatile 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 ou enregistrer un profil :

1. Dans la page **Profil BIOS**, dans la section **Enregistrer et appliquer des profils**, sélectionnez le serveur à partir des paramètres duquel le profil doit être généré, puis cliquez sur **Enregistrer un profil**.

   La section **Enregistrer un profil BIOS** s'affiche.
2. 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**.

   CMC communique avec le LC pour obtenir les paramètres BIOS 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.

Liens connexes

Accès à la page Profil BIOS

Gestion des profils stockés

Vous pouvez modifier, afficher ou supprimer les profils BIOS.

Pour gérer les profils stockés sur le CMC :

1. Dans la page **Profil BIOS**, sous **Appliquer un profil**, cliquez sur **Gérer les profils**. La page **Gérer les profils BIOS** s'affiche.
2. Pour modifier un profil, cliquez sur **Modifier**.
3. Pour afficher les paramètres BIOS, cliquez sur **Afficher**.
4. Pour supprimer un profil, cliquez sur **Supprimer**.
   Pour plus d'informations, voir l'*Aide en ligne CMC*.

Application d'un profil

Lorsque des profils stockés sont disponibles dans le support non volatile du CMC, vous pouvez appliquer un profil stocké à un ou plusieurs serveurs afin de lancer une opération de clonage de serveur.

REMARQUE : Si un serveur ne prend pas en charge le Lifecycle Controller ou si le châssis est hors tension, vous ne pouvez pas appliquer de profil au serveur.

Pour appliquer un profil à un ou plusieurs serveurs :

1. Dans la page **Profil BIOS**, 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.
2. À partir du menu déroulant **Sélectionner le profil**, sélectionnez le profil souhaité.
   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 BIOS va écraser les paramètres actuels et également redémarrer les serveurs sélectionnés. Vous êtes invité à confirmer si vous souhaitez continuer l'opération.

   REMARQUE : Si l'option CSIOR est désactivée, un message d'avertissement suivant s'affiche : CSIOR n'est pas activée pour les serveurs ciblés par l'opération de clonage de lame. Vous devez d'abord activer CSIOR pour effectuer l'opération de clonage de lame.
4. Cliquez sur **OK** pour appliquer le profil au serveur sélectionné.
   Le profil sélectionné est appliqué au(x)serveur(s) et le(s) serveur(s) est(sont) redémarré(s) immédiatement. Pour plus d'informations, consultez l'*Aide en ligne CMC*.

Liens connexes

Accès à la page Profil BIOS

Importation de profil

Vous pouvez importer sur CMC un profil BIOS stocké précédemment sur un serveur.

Pour importer sur CMC un profil stocké sur un serveur :

1. Dans la page **Profil BIOS**, dans la section **Gérer les profils sur la carte SD**, cliquez sur **Importer un profil**.
   La section **Importer un profil BIOS** s'affiche.
2. Cliquez sur **Parcourir** pour accéder au profil à partir de l'emplacement souhaité, puis cliquez sur **Importer le profil**.
   Pour plus d'informations, voir l'*Aide en ligne CMC*.

Exportation de profil

Vous pouvez exporter un profil BIOS stocké enregistré sur le support CMC non volatile (carte SD) vers un chemin spécifié sur un autre serveur.

Pour exporter un profil stocké :

1. Dans la page **Profil BIOS**, dans la section **Gérer les profils sur la carte SD**, sélectionnez le profil souhaité, puis cliquez sur **Exporter le profil**.

   La boîte de dialogue **Téléchargement de fichier** qui s'affiche vous invite à ouvrir ou à enregistrer le fichier.
2. Cliquez sur **Enregistrer** ou **Ouvrir** pour exporter le profil vers l'emplacement requis.

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

Modification d'un profil

Vous pouvez modifier le nom et la description d'un profil BIOS stocké sur le support CMC non volatile (carte SD).

Pour modifier un profil stocké :

1. Dans la page **Profil BIOS**, dans la section **Gérer les profils sur la carte SD**, 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 BIOS, puis cliquez sur **Modifier le profil**.

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

Suppression d'un profil

Vous pouvez supprimer un profil BIOS stocké sur le support CMC non volatile (carte SD).

Pour supprimer un profil stocké :

1. Dans la page **Profil BIOS**, dans la section **Gérer les profils sur la carte SD**, sélectionnez le profil souhaité, puis cliquez sur **Supprimer le profil**.

   Un message d'avertissement s'affiche, indiquant que la suppression d'un profil supprime définitivement le profil sélectionné.
2. Cliquez sur **OK** pour supprimer le profil sélectionné.

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

Affichage des paramètres BIOS

Pour afficher les **paramètres BIOS** du serveur sélectionné, ouvrez la page **Profils BIOS**, accédez à la section **Enregistrer et appliquer des profils** et cliquez sur **Afficher** dans la colonne des paramètres BIOS correspondant au serveur dont vous voulez consulter les paramètres BIOS. La page **Afficher les paramètres** s'affiche.

Seuls les paramètres BIOS du serveur susceptibles d'être modifiés par l'application d'un profil (paramètres clonables) sont affichés. Ces paramètres sont répartis en groupes de la même façon que lorsque vous les affichez dans l'écran de **configuration du BIOS iDRAC**.

REMARQUE : L'application de clonage de serveur CMC récupère et affiche les paramètres BIOS et d'amorçage corrects pour le serveur spécifié uniquement si l'option **Collecte de l'inventaire système au redémarrage** (CSIOR) est activée.

Pour activer CSIOR :

- Serveurs 11e génération : après avoir redémarré le serveur, activez l'écran de configuration avec **Ctrl-E** et sélectionnez **Services système**, puis activez **CSIOR** et enregistrez les changements.
- 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 changements.

Liens connexes

Accès à la page Profil BIOS

Affichage des paramètres de profil

Pour afficher les paramètres de profil des profils BIOS stockés, allez à la page **Profils BIOS**. Dans la section **Gérer les profils sur la carte SD**, cliquez sur **Afficher** dans la colonne Paramètres de profil pour le profil BIOS dont vous souhaitez afficher les paramètres de profil. La page **Affichage des paramètres** s'affiche.

Affichage du journal de profil

Pour afficher le journal de profil, ouvrez la page **Profils BIOS** et consultez la section **Journal de profil récent**. Elle répertorie les 10 dernières entrées de journal de profil consignées directement à partir des opérations de clonage de serveur. Chaque entrée indique la gravité, la date et l'heure de l'opération de clonage de serveur soumise, ainsi que la description du message de journal de clonage. Ces entrées de 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.

Condition d'achèvement et dépannage

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

1. Dans la page **Profils BIOS**, notez l'ID de tâche (JID) de la tâche soumise, affiché dans la section **Journal de profil récent**.
2. Dans l'arborescence système, accédez à **Présentation du serveur**, puis cliquez sur **Dépannage → Tâches Lifecycle Controller**. Recherchez le même JID dans la table **Tâches**.

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

CMC offre des fonctions limitées de gestion de chaque composant de châssis, comme les serveurs. Pour la gestion complète de ces composants distincts, CMC offre un point de lancement de l'interface Web du contrôleur de gestion (iDRAC) du serveur.

Comme cette fonctionnalité utilise la connexion directe (SSO), un utilisateur peut lancer l'interface Web iDRAC sans avoir à se connecter à nouveau.

- 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 Admistrateur 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.

Liens connexes

Lancement d'iDRAC depuis la page Condition des serveurs
Lancement d'iDRAC depuis la page Condition du serveur

Lancement d'iDRAC depuis la page Condition des serveurs

Pour lancer la console de gestion iDRAC depuis la page **Condition des serveurs** :

1. Dans l'arborescence système, cliquez sur **Présentation du serveur**. La page **Condition des serveurs** s'affiche.
2. Cliquez sur **Lancer iDRAC** en regard du serveur où vous voulez lancer l'interface Web iDRAC.

Lancement d'iDRAC depuis la page Condition du serveur

Pour lancer la console de gestion d'iDRAC pour un serveur individuel :

1. Dans l'arborescence système, développez **Présentation du serveur**. Tous les serveurs (1 à 16) apparaissent dans la liste **Serveurs** développée.
2. Cliquez sur le serveur pour lequel lancer l'interface Web iDRAC. La page **Condition du serveur** s'affiche.
3. Cliquez sur **Lancer l'interface utilisateur iDRAC**. L'interface Web iDRAC s'affiche.

Lancement de la console distante à partir de l'interface Web CMC

Vous pouvez lancer une session KVM (Keyboard-Video-Mouse- Clavier-Écran-Souris) directement sur le serveur. La fonction de console distante est prise en charge uniquement lorsque toutes les conditions suivantes sont réunies :

- Le châssis est sous tension,
- Serveurs prenant en charge iDRAC6 et iDRAC7.
- L'interface de réseau local sur le serveur est activée.
- La version d'iDRAC est 2.20 ou ultérieure.
- Le système hôte dispose du JRE (Java Runtime Environment) 6 Update 16 ou ultérieur.
- Le navigateur sur le système hôte autorise les fenêtres contextuelles (le blocage de fenêtres contextuelles est désactivé).

Vous pouvez également lancer la console distante depuis l'interface Web iDRAC. Pour plus d'informations, voir le manuel « *iDRAC User's Guide* » (Guide d'utilisation d'iDRAC).

Liens connexes

Lancement de la console distante depuis la page Intégrité du châssis

Pour lancer la console distante depuis l'interface Web CMC, effectuez l'une des opérations suivantes :

1. Dans l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **Propriétés** → **Intégrité**. La page **Intégrité du châssis** s'affiche.
2. Cliquez sur le serveur spécifié dans le graphique du châssis.
3. Dans la section **Liens rapides**, cliquez sur le lien **Lancer la console distante** pour effectuer le lancement.

Lancement de la console distante depuis la page Condition du serveur

Pour lancer une console distante pour un serveur particulier :

1. Dans l'arborescence système, développez **Présentation du serveur**. Tous les serveurs (1 à 16) apparaissent dans la liste des serveurs développée.
2. Cliquez sur le serveur pour lequel lancer la console distante. La page **Condition du serveur** s'affiche.
3. Cliquez sur **Lancer la console distante**.

Lancement de la console distante depuis la page Condition des serveurs

Pour lancer une console distante de serveur à partir de la page **Condition des serveurs** :

1. Dans l'arborescence système, accédez à **Présentation du serveur**, puis cliquez sur **Propriétés** → **Condition**. La page **Condition des serveurs** s'affiche.
2. Cliquez sur **Lancer la console distante** pour le serveur voulu.

8

Configuration de CMC pour envoyer des alertes

Vous pouvez définir des alertes et des actions pour certains événements qui se produisent sur le système géré. Un événement se produit lorsque la condition d'un composant système est supérieur à la condition prédéfinie. Si un événement correspond au filtre d'événements défini et si ce filtre est configuré pour générer une alerte (par e-mail ou par interruption SNMP), cette alerte est envoyée à une ou plusieurs destinations, que vous avez configurées au préalable.

Pour configurer CMC afin qu'il envoie des alertes :

1. Activez globalement les alertes d'événement de châssis.
2. (Facultatif) Sélectionnez les événements pour lesquels des alertes doivent être générées.
3. Configurez les paramètres d'alerte par e-mail ou par interruption SNMP.

Liens connexes

Activation ou désactivation des alertes
Configuration de destinations d'alerte

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 l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **Alertes → Événements sur châssis**.

   La page **Événements sur châssis** s'affiche.
2. Dans la section **Configuration de filtres d'événements de châssis**, sélectionnez l'option **Activer les alertes d'événement de châssis** pour activer la génération d'alertes. Sinon, désélectionnez cette option.
3. Dans la section **Liste des événements de châssis**, effectuez l'une des opérations suivantes :
   - Sélectionnez chacun des événements pour lesquels des alertes doivent être générées.
   - Sélectionnez l'option **Activer l'alerte** dans l'en-tête de colonne pour générer des alertes pour tous les événements. Sinon, désélectionnez cette option.
4. Cliquez sur **Appliquer** pour enregistrer le paramètre.

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 plus d'informations, voir le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de l'interface de ligne de commande RACADM pour iDRAC7 et CMC).

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 des destinations d'alerte IPv4 et IPv6, des paramètres e-mail et des paramètres de serveur SMTP et tester ces paramètres.

Avant de configurer les paramètres d'alerte par e-mail ou par interruption SNMP, vérifiez que vous disposez du privilège **Administrateur de configuration du châssis**.

Liens connexes

Configuration de destinations d'alerte pour interruption SNMP
Définition des paramètres d'alerte par e-mail

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.

   – 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 sauter 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. Spécifiez les événements pour lesquels des alertes doivent être générées :

   ```
   racadm config -g cfgAlerting -o cfgAlertingFilterMask <valeur du masque>
   ```

   où `<valeur du masque>` est une valeur hexadécimale comprise entre 0x0 et 0xffffffff.

   Pour obtenir la valeur du masque, utilisez une calculatrice scientifique en mode hexadécimal et ajoutez les deuxièmes valeurs de chaque masque (1, 2, 4, etc.) en utilisant la touche <OR> (OU).

   Par exemple, vous souhaitez activer les alertes par interruption pour un avertissement de capteur de batterie (0x2), une panne de bloc d'alimentation (0x1000) et une panne KVM (0x80000), entrez 2 <OR> 1000 <OR> 200000, puis appuyez sur la touche <=>.

   La valeur hexadécimale qui en résulte est 208002 et la valeur du masque pour la commande RACADM est 0x208002.

Tableau 14. Masques de filtrage des interruptions d'événement

Événement	Valeur du masque de filtre
Échec signalé par le capteur de ventilateur	0x1
Avertissement du capteur de batterie	0x2
Avertissement du capteur de température	0x8
Échec signalé par le capteur de température	0x10
Redondance dégradée	0x40
Perte de la redondance	0x80
Avertissement du bloc d'alimentation	0x800
Échec du bloc d'alimentation	0x1000
Bloc d'alimentation absent	0x2000
Échec du journal du matériel	0x4000
Avertissement du journal du matériel	0x8000
Serveur absent	0x10000
Échec du serveur	0x20000
KVM absent	0x40000
Échec du KVM	0x80000
IOM absent	0x100000
Échec du IOM	0x200000
La version du micrologiciel ne convient pas	0x400000
Erreur de seuil énergétique du châssis	0x1000000
CARTE SD absente	0x2000000
Erreur de CARTE SD	0x4000000
Erreur du groupe de châssis	0x8000000

Événement	Valeur du masque de filtre
Boîtier de serveur manquant	0x10000000
Structures différentes	0x20000000

4. Activez les alertes par interruption :
   ```
   racadm config -g cfgTraps -o cfgTrapsEnable 1 -i <index>
   ```
   Où <index> est une valeur comprise entre 1 et 4. 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).
5. Spécifiez une adresse IP de destination pour la réception des alertes par interruption :
   ```
   racadm config -g cfgTraps -o cfgTrapsAlertDestIPAddr <adresse IP> -i <index>
   ```
   où <adresse IP> est une destination valide et <index> est la valeur d'index spécifiée à l'étape 4.
6. Spécifiez le nom de communauté :
   ```
   racadm config -g cfgTraps -o cfgTrapsCommunityName <nom de communauté> -i
   <index>
   ```
   où <nom de communauté> est la communauté SNMP à laquelle appartient le châssis, et <index> est la valeur d'index spécifiée aux étapes 4 et 5.

   Vous pouvez configurer jusqu'à quatre destinations pour les alertes par interruption. Pour ajouter 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**.
7. Pour tester une interruption d'événement pour une destination d'alerte :
   ```
   racadm testtrap -i <index>
   ```
   où <index> est une valeur comprise entre 1 et 4 représentant la destination d'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 d'iDRAC soit configuré pour que le serveur de messagerie puisse recevoir les alertes par e-mail d'iDRAC.

REMARQUE : Les alertes par e-mail prennent en charge les adresses iPv4 et IPv6. Le nom de domaine DNS DRAC doit être défini lorsque vous utilisez le protocole IPv6.

Si votre réseau comporte un serveur SMTP qui envoie et renouvelle l'adresse IP périodiquement, et si les adresses sont différentes, il existe une durée de temporisation où ce paramètre ne fonctionne pas, en raison d'un changement dans l'adresse IP de serveur SMTP spécifiée. Dans ce cas, utilisez le nom DNS.

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

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

1. Dans l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **Alertes → Paramètres d'alertes par e-mail**.
2. Spécifiez les paramètres de serveur d'e-mail SMTP et les adresses e-mail devant recevoir les alertes. Pour plus d'informations sur les champs, voir l'*aide en ligne CMC*.
3. Cliquez sur **Appliquer** pour enregistrer les paramètres.
4. Cliquez sur **Envoyer** dans la section **E-mail test** afin d'envoyer un e-mail de test à la destination d'alerte par e-mail spécifiée.

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

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

1. Ouvrez une console série/Telnet/SSH d'accès à CMC, puis ouvrez une session.
2. Activez la génération d'alertes :
   ```
   racadm config -g cfgAlerting -o cfgAlertingEnable 1
   ```
   REMARQUE : Chaque fonction (SNMP et e-mails d'alerte) ne peut définir qu'un seul masque de filtrage. Vous pouvez sauter l'étape 3 si vous avez déjà défini un masque de filtrage.
3. Spécifiez les événements pour lesquels des alertes doivent être générées :
   ```
   racadm config -g cfgAlerting -o cfgAlertingFilterMask <valeur du masque>
   ```
   Où `<valeur du masque>` est une valeur hexadécimale comprise entre 0x0 et 0xffffffff, exprimée avec ses caractères 0x de début. La table Masques de filtrage des interruptions d'événement indique les masques de filtrage de chaque type d'événement. Pour obtenir des instructions pour le calcul de la valeur hexadécimale du masque de filtrage à activer, passez à l'étape 3 de la procédure « Configuration de destinations d'alerte par interruption SNMP à l'aide de RACADM ».
4. Activez la génération d'alertes 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.
5. Spécifiez l'adresse e-mail de destination qui doit recevoir les alertes par e-mail :
   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertAddress <adresse e-mail> -i
   <index>
   ```
   où `<adresse e-mail>` est une adresse e-mail valide et `<index>` est la valeur d'index spécifiée à l'étape 4.
6. Spécifiez le nom de la personne qui reçoit l'alerte par e-mail :
   ```
   racadm config -g cfgEmailAlert -o cfgEmailAlertEmailName <destinataire d'e-
   mail> -i <index>
   ```
   Où `<destinataire d'e-mail>` est le nom de la personne ou du groupe qui doit recevoir l'alerte par e-mail, et `<index>` est la valeur d'index spécifiée aux étapes 4 et 5. Le nom du destinataire d'e-mail peut contenir jusqu'à 32 caractères alphanumériques, tirets, caractères de soulignement et points. Les espaces ne sont pas valides.
7. Configurez l'hôte SMTP :
   ```
   racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr hôte.domaine
   ```
   Où `hôte.domaine` est le nom FQDN (Fully Qualified Domain Name - Nom de domaine entièrement qualifié).

Vous pouvez configurer jusqu'à quatre adresses e-mail de destination devant recevoir les alertes par e-mail. Pour ajouter des adresses, répétez les étapes 2 à 6.

REMARQUE : Les commandes des étapes 2 à 6 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 : `racadm getconfig -g cfgEmailAlert — I <index>`. Si l'index est déjà configuré, des valeurs apparaissent pour les objets **cfgEmailAlertAddress** et **cfgEmailAlertEmailName**.

Pour plus d'informations, voir le manuel *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) disponible sur le site **dell.com/support/manuals**.

9

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 garantir la sécurité de ce système. Par défaut, CMC est configuré avec un compte d'administrateur local. Ce nom par défaut est *root* et le mot de passe, *calvin*. En tant qu'administrateur, vous pouvez configurer des comptes d'utilisateur pour autoriser d'autres utilisateurs à accéder à 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 d'utilisateur supplémentaires. L'utilisation d'un service d'annuaire permet de disposer d'un emplacement central pour la gestion des comptes d'utilisateur autorisés.

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.

Liens connexes

Types d'utilisateur
Configuration des utilisateurs locaux
Configuration des utilisateurs d'Active Directory
Configuration d'utilisateurs LDAP générique
Modification des paramètres du compte administrateur de l'utilisateur root

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 15. : Types d'utilisateur

Droits	Description
Ouverture de session utilisateur CMC	L'utilisateur peut se connecter à CMC et afficher toutes les données CMC, mais ne peut pas ajouter ni modifier de données, ni exécuter de commandes. 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

Droits	Description
	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.
Administrateur de configuration du châssis	L'utilisateur peut ajouter ou modifier des données qui : • Identifient le châssis, tels que le nom du châssis et son emplacement. • Sont attribuées spécifiquement au châssis, tels que le mode IP (statique ou DHCP), l'adresse IP statique, la passerelle statique et le masque de sous-réseau statique. • Fournissent des services au châssis, telles que la date et heure, la mise à jour de micrologiciel et la réinitialisation du CMC. • Sont associées au châssis, 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. Lorsque vous déplacez un serveur vers un autre châssis, il hérite du nom et de la priorité du logement qu'il occupe dans le nouveau châssis. Le nom et la priorité de logement précédents restent associés au châssis précédent. **REMARQUE :** Les utilisateurs CMC dotés du privilège **Administrateur de configuration du châssis** peuvent configurer les paramètres d'alimentation. Toutefois, ils doivent disposer du privilège **Administrateur de contrôle du châssis** pour effectuer des opérations d'alimentation du châssis (allumage, extinction ou cycle d'alimentation).
Administrateur de configuration des utilisateurs	L'utilisateur peut : • Ajouter un nouvel utilisateur. • Modifier le mot de passe d'un utilisateur. • Modifier les privilèges d'un utilisateur. • Activer ou désactiver les privilèges d'ouverture de session d'un utilisateur tout en conservant le nom et les autres privilèges de l'utilisateur dans la base de données.
Administrateur des effacements de journaux	L'utilisateur peut effacer le journal matériel et le journal CMC.
Administrateur de contrôle du châssis (contrôle de l'alimentation)	Les utilisateurs CMC dotés du privilège **Administrateur de contrôle du châssis** peuvent effectuer toutes les opérations liées à l'alimentation. Ils peuvent contrôler l'alimentation du châssis (allumage, extinction ou cycle d'alimentation). **REMARQUE :** Le privilège de **Administrateur de configuration du châssis** est nécessaire pour configurer des paramètres d'alimentation.
Administrateur de serveur	Ceci est un privilège général : les droits d'administrateur de serveur sont des droits permanents qui autorisent l'utilisateur CMC à effectuer des opérations sur n'importe quel serveur présent dans le châssis. Lorsqu'un utilisateur possédant le privilège **Administrateur de serveur** émet une action à exécuter sur un serveur, le micrologiciel CMC envoie la commande au serveur ciblé sans vérifier les privilèges de cet utilisateur sur

Droits	Description
	le serveur. Autrement dit, le privilège **Administrateur de serveur** permet de passer outre à l'absence de privilèges d'administrateur sur le serveur. Sans les droits d'**Administrateur de serveur**, un utilisateur créé sur le châssis ne peut exécuter une commande sur un serveur que lorsque les conditions suivantes sont réunies : • Le même nom d'utilisateur est utilisé sur le serveur. • Le même nom d'utilisateur doit avoir exactement le même mot de passe sur le serveur. • L'utilisateur doit avoir le droit d'exécuter la commande. Lorsqu'un utilisateur CMC sans privilège d'**Administrateur de serveur** 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. 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. 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. Administration et configuration du serveur : • Définir l'adresse IP • Définir la passerelle • Définir le masque de sous-réseau • Définir le périphérique de démarrage initial Configurer les utilisateurs : • Définir le mot de passe root d'iDRAC • Réinitialisation d'iDRAC Administration de contrôle du serveur : • Mise sous tension • Mise hors tension • Cycle d'alimentation • Arrêt normal • Redémarrage du serveur
Utilisateur d'alertes de test	L'utilisateur peut envoyer des messages d'alerte d'essai.
Administrateur de commandes de débogage	L'utilisateur peut exécuter des commandes de diagnostic système.
Administrateur de structure A	L'utilisateur peut définir et configurer le module d'E/S de la structure A, qui réside dans le logement A1 ou A2 des logements d'E/S.
Administrateur de structure B	L'utilisateur peut définir et configurer le module d'E/S de la structure B, qui réside dans le logement d'E/S B1 ou B2.

Droits	Description
Administrateur de structure C	L'utilisateur peut définir et configurer le module d'E/S de la structure C, qui réside dans le logement d'E/S C1 ou C2.

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 16. : Privilèges des groupes CMC

Groupe d'utilisateurs	Privilèges accordés
Administrateur	• Ouverture de session utilisateur CMC • Administrateur de configuration du châssis • Administrateur de configuration des utilisateurs • Administrateur des effacements de journaux • Administrateur de serveur • Utilisateur d'alertes de test • Administrateur de commandes de débogage • Administrateur de structure A • Administrateur de structure B • Administrateur de structure C
Utilisateur privilégié	• Connexion • Administrateur des effacements de journaux • Administrateur de contrôle du châssis (contrôle de l'alimentation) • Administrateur de serveur • Utilisateur d'alertes de test • Administrateur de structure A • Administrateur de structure B • Administrateur de structure C
Utilisateur invité	Connexion
Personnalisé	Sélectionnez n'importe quelle combinaison des autorisations suivantes : • Ouverture de session utilisateur CMC • Administrateur de configuration du châssis • Administrateur de configuration des utilisateurs • Administrateur des effacements de journaux • Administrateur de contrôle du châssis (contrôle de l'alimentation) • Administrateur de serveur • Utilisateur d'alertes de test • Administrateur de commandes de débogage • Administrateur de structure A • Administrateur de structure B

Groupe d'utilisateurs	Privilèges accordés
	• Administrateur de structure C
Aucun	Aucun droit attribué

Tableau 17. : 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
Administrateur de serveur	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
Administrateur de structure B	Oui	Oui	Non
Administrateur de structure C	Oui	Oui	Non

Modification des paramètres du compte administrateur de l'utilisateur root

Pour plus de sécurité, il est fortement recommandé de modifier le mot de passe par défaut du compte racine (root, Utilisateur 1). Le compte racine est le compte d'administrateur par défaut livré avec le CMC.

Pour modifier le mot de passe par défaut du compte racine (root) avec l'interface Web CMC :

1. Dans l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **Authentification utilisateur** → **Utilisateurs locaux**?. La page **Utilisateurs** s'affiche.
2. Dans la colonne **Réf. utilisateur**, cliquez sur l'ID d'utilisateur 1.

   REMARQUE : L'ID utilisateur 1 correspond au compte d'utilisateur racine (root) livré par défaut avec CMC. Vous ne pouvez pas le modifier.

   La page **Configuration de l'utilisateur** s'affiche.
3. Cochez la case **Modifier le mot de passe**.

4. Entrez le nouveau mot de passe dans les champs **Nouveau mot de passe** et **Confirmez le mot de passe**.
5. Cliquez sur **Appliquer**. Le mot de passe de l'utilisateur dont la référence est ID 1 est modifié.

Configuration des utilisateurs locaux

Vous pouvez configurer jusqu'à 16 utilisateurs locaux dans CMC avec des autorisations d'accès spécifiques. Avant de créer un utilisateur CMC local, vérifiez s'il existe déjà des utilisateurs. Vous pouvez définir le nom, le mot 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 (interface Web, RACADM ou WS-MAN).

Configuration d'utilisateurs locaux dans l'interface Web CMC

Pour ajouter et configurer des utilisateurs CMC locaux :

REMARQUE : Vous devez disposer du privilège **Configurer les utilisateurs** pour pouvoir créer un utilisateur CMC.

1. Dans l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **Authentification utilisateur** → **Utilisateurs locaux**?. La page **Utilisateurs** s'affiche.
2. Dans la colonne **Réf. utilisateur**, cliquez sur un ID. La page **Configuration utilisateur** s'affiche.

   REMARQUE : L'ID utilisateur 1 correspond au compte d'utilisateur racine (root) livré par défaut avec 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 CMC*.
4. Cliquez sur **Appliquer**. L'utilisateur est créé avec les privilèges demandés.

Configuration d'utilisateurs locaux à l'aide de RACADM

REMARQUE : Vous devez ouvrir une session en tant qu'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 si vous avez utilisé la commande racadm `racresetcfg`, le seul utilisateur actuel est `root`, dont le mot de passe est `calvin`. La sous-commande `racresetcfg` réinitialise tous les paramètres de configuration sur les valeurs par défaut d'origine. 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 indice compris entre 1 et 16 :

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

REMARQUE : Vous pouvez également taper `racadm getconfig -f <monfichier.cfg>`, et afficher ou modifier le fichier **monfichier.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 `cfgUserAdminIndex` 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 quelconque 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 CMC avec les mêmes paramètres que le CMC principal.

Ajout d'un utilisateur CMC avec RACADM

Pour ajouter un nouvel utilisateur à la configuration CMC, procédez comme suit :

1. Définissez le nom de l'utilisateur.
2. Définissez le mot de passe.
3. Définissez les privilèges de l'utilisateur. Pour plus d'informations sur les privilèges utilisateur, voir « Types d'utilisateur ».
4. Activez l'utilisateur.

Exemple :

L'exemple suivant explique comment ajouter le nouvel utilisateur « Jean » avec le mot de passe « 123456 » et le privilège Connexion sur CMC.

REMARQUE : Voir le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC) pour consulter la liste des valeurs de masque binaire valides pour des privilèges utilisateurs spécifiques. La valeur de privilège par défaut est 0, qui signifie que l'utilisateur n'a aucun privilège.

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 Jean racadm config -
g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456 racadm config -g
cfgUserAdmin -i 2 -o cfgUserAdminPrivilege 0x00000001 racadm config -g
cfgUserAdmin -i 2 -o cfgUserAdminEnable 1
```

Pour vérifier que l'utilisateur a bien été ajouté avec les privilèges corrects, utilisez les commandes suivantes :

```
racadm getconfig -g cfgUserAdmin -i 2
```

Pour plus d'informations sur les commandes RACADM, voir le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC), disponible sur le site **dell.com/support/manuals**.

Désactivation d'un utilisateur CMC

Lorsque vous utilisez RACADM, les utilisateurs doivent être désactivés manuellement et de manière individuelle. Vous ne pouvez pas supprimer des utilisateurs en utilisant un fichier de configuration.

Pour supprimer un utilisateur CMC, utilisez la commande suivante :

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i <index>"" racadm
config -g cfgUserAdmin -i 2 -o cfgUserAdminPrivilege 0x0
```

Une chaîne Null entre guillemets ("") indique à CMC qu'il doit supprimer la configuration utilisateur à l'index indiqué et restaurer les valeurs par défaut définies en usine de la configuration utilisateur.

Activation d'un utilisateur CMC avec des droits

Pour activer un utilisateur avec des droits (droit basé sur un rôle) :

1. recherchez un index d'utilisateur disponible en utilisant la commande suivante :
   ```
   racadm getconfig -g cfgUserAdmin -i <index>
   ```
2. Tapez les commandes suivantes avec les nouveaux nom d'utilisateur et mot de passe.
   ```
   racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <index> <valeur
   de masque binaire de privilège d'utilisateur>
   ```

   REMARQUE : Pour consulter la liste des valeurs de masque binaire de privilèges spécifiques, voir le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC), disponible sur le site **dell.com/support/manuals**. La valeur de privilège par défaut (0) indique que l'utilisateur n'a aucun privilège.

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 : L'utilisation d'Active Directory pour reconnaître les utilisateurs CMC est prise en charge sous les systèmes d'exploitation Microsoft Windows 2000 et Windows Server 2003. Windows 2008 prend en charge Active Directory sur IPv6 et IPv4.

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 :

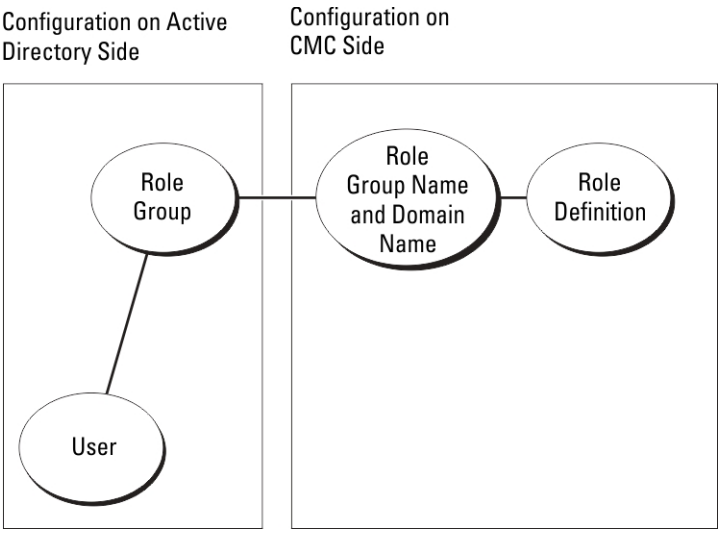
- La solution de *Schéma standard*, qui utilise uniquement les objets de groupe Active Directory par défaut Microsoft.
- La solution de *Schéma étendu*, qui inclut des objets Active Directory personnalisés fournis par Dell. Tous les objets de contrôle d'accès sont gérés dans Active Directory. Cela offre une souplesse maximale pour la configuration de l'accès des utilisateurs aux différents CMC avec divers niveaux de privilèges.

Liens connexes

Présentation d'Active Directory avec le schéma standard
Présentation d'Active Directory avec schéma étendu

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 18. : Privilèges par défaut des groupes de rôles

Groupe de rôles	Niveau de privilège par défaut	Droits accordées	Masque binaire
1	Aucun	• Ouverture de session utilisateur CMC • Administrateur de configuration du châssis • Administrateur de configuration des utilisateurs • Administrateur des effacements de journaux • Administrateur de contrôle du châssis (contrôle de l'alimentation) • Administrateur de serveur • Utilisateur d'alertes de test • Administrateur de commandes de débogage • Administrateur de structure A • Administrateur de structure B	0x00000fff

Groupe de rôles	Niveau de privilège par défaut	Droits accordées	Masque binaire
		• Administrateur de structure C	
2	Aucun	• Ouverture de session utilisateur CMC • Administrateur des effacements de journaux • Administrateur de contrôle du châssis (contrôle de l'alimentation) • Administrateur de serveur • Utilisateur d'alertes de test • Administrateur de structure A • Administrateur de structure B • Administrateur de structure C	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 CMC pour la connexion à Active Directory :

1. Sur un serveur Active Directory (contrôleur de domaine), ouvrez le **snap-in Utilisateurs et ordinateurs Active Directory**.
2. Avec l'interface Web CMC ou RACADM :
   a) Créez un groupe ou sélectionnez un groupe existant.
   b) Configurez les privilèges du rôle.
3. Ajoutez l'utilisateur Active Directory comme membre du groupe Active Directory pour qu'il puisse accéder à iDRAC6.

Configuration d'Active Directory avec le schéma standard à l'aide de l'interface Web CMC

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

1. Dans l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **Authentification utilisateur → Services d'annuaire**. La page **Services d'annuaire** s'affiche.
2. Sélectionnez **Microsoft Active Directory (Schéma standard)**. Les paramètres à configurer pour le schéma standard sont affichés dans la même page.
3. Paramétrez les options suivantes :
   - Activez Active Directory, entrez le nom du domaine racine (root) et la valeur de délai d'attente.
   - Pour que l'appel acheminé fasse une recherche dans le contrôleur de domaine et le catalogue global, sélectionnez l'option **Serveur AD de recherche à examiner (facultatif)**, puis spécifiez les détails du contrôleur de domaine et du catalogue global.
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 passerez à une autre page.
5. Dans la section **Paramètres du schéma standard**, cliquez sur une entrée **Groupe de rôles**. La page **Configurer le groupe de rôles** s'affiche.
6. Spécifiez le nom, le domaine et les privilèges d'un groupe de rôles.
7. Cliquez sur **Appliquer** pour enregistrer les paramètres de groupe de rôles, puis cliquez sur **Retour à la page Configuration**.
8. Si vous avez activé la validation de certificat, vous devez téléverser le certificat autosigné racine de la forêt de domaines vers CMC. Dans la section **Gérer les certificats**, entrez le chemin du fichier de certificat ou naviguez jusqu'à ce fichier. Cliquez sur **Téléverser** pour téléverser le fichier vers CMC.

   REMARQUE : La valeur **Chemin de fichier** indique le chemin relatif du fichier de certificat que vous téléversez. Vous devez saisir le chemin absolu de ce fichier, à savoir son chemin complet, son nom et son extension.

   Les certificats SSL des contrôleurs de domaine doivent être signés par le certificat racine signé par l'autorité de certification. Ce certificat racine doit être disponible sur la station de gestion qui accède à CMC.
9. Si vous avez activé la connexion directe (SSO), accédez à la section **Fichier keytab Kerberos**, cliquez sur **Parcourir**, spécifiez le fichier keytab, puis cliquez sur **Téléverser**. Une fois l'opération terminée, un message s'affiche, signalant la réussite ou l'échec du téléversement.
10. Cliquez sur **Appliquer**. Le serveur Web CMC redémarre automatiquement lorsque vous cliquez sur **Appliquer**.
11. Déconnectez-vous de CMC, puis reconnectez-vous pour achever la configuration d'Active Directory pour CMC.
12. Sélectionnez **Châssis** dans l'arborescence système et naviguez jusqu'à l'onglet **Réseau**. La page **Configuration réseau** s'affiche.
13. Sous **Paramètres réseau**, si vous avez activé l'option **Utiliser DHCP (pour l'adresse IP de l'interface réseau CMC)**, sélectionnez **Utiliser DHCP pour obtenir des adresses de serveur DNS**.

    Pour saisir manuellement l'adresse IP d'un serveur DNS, désélectionnez l'option **Utiliser DHCP pour obtenir des adresses de serveur DNS**, puis entrez les adresses IP des serveurs DNS primaire et secondaire.
14. Cliquez sur **Appliquer les changements**.

    La configuration du schéma standard d'Active Directory CMC est terminée.

Configuration d'Active Directory avec le schéma standard à l'aide de l'interface RACADM

Pour configurer l'annuaire Active Directory CMC avec le schéma standard en utilisant RACADM :

1. Ouvrez une console texte série/Telnet/SSH d'accès à CMC et entrez :

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1 racadm config -g
cfgActiveDirectory -o cfgADType 2 racadm config -g cfgActiveDirectory -o
cfgADRootDomain <nom FQDN racine> racadm config -g cfgStandardSchema -i
<index> -o cfgSSADRoleGroupName <nom commun du groupe de rôles> racadm
config -g cfgStandardSchema -i <index>-o cfgSSADRoleGroupDomain <nom FQDM>
racadm config -g cfgStandardSchema -i <index> -o cfgSSADRoleGroupPrivilege
<valeur de masque binaire pour des permissions utilisateur spécifiques>
```

```
racadm sslcertupload -t 0x2 -f <certificat de CA racine ADS> racadm
sslcertdownload -t 0x1 -f <certificat SSL RAC>
```

REMARQUE : Pour les valeurs de numéro de masque binaire, consultez le chapitre des propriétés de base de données dans le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC).

2. Spécifiez un serveur DNS à l'aide de l'une des options suivantes :

   – Si DHCP est activé sur le CMC et que vous voulez utiliser l'adresse DNS obtenue automatiquement par le serveur DHCP, entrez la commande suivante :

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

   – Si le protocole DHCP est désactivé sur CMC ou que vous voulez entrer manuellement l'adresse IP DNS, entrez les commandes suivantes :

   ```
   racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0 racadm
   config -g cfgLanNetworking -o cfgDNSServer1 <adresse IP du DNS
   primaire> racadm config -g cfgLanNetworking -o cfgDNSServer2 <adresse
   IP du DNS secondaire>
   ```

Présentation d'Active Directory avec schéma étendu

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

Extensions de schéma Active Directory

Les données Active Directory constituent une base de données distribuée d'*attributs* et de *classes*. Le schéma Active Directory inclut les règles qui déterminent le type de données qu'il est possible d'ajouter ou d'inclure dans la base de données. L'une des classes stockées dans la base de données est la classe Utilisateur. Les attributs de cette classe peuvent être par exemple le prénom de l'utilisateur, son nom de famille, son numéro de téléphone, etc.

Vous pouvez étendre la base de données Active Directory en ajoutant vos propres *attributs* et *classes* uniques pour répondre à des besoins spécifiques. Dell a étendu le schéma pour inclure les changements nécessaires à la prise en charge de l'authentification et de l'autorisation de la gestion à distance dans Active Directory.

Chaque *attribut* (ou *classe*) ajouté à un schéma Active Directory existant doit être défini avec un ID unique. Pour gérer les ID uniques sur l'ensemble du marché, Microsoft gère une base de données d'identificateurs d'objet Active Directory (OID) pour que, lorsque les entreprises ajoutent des extensions au schéma, ces extensions soient garanties comme uniques et n'entrent pas en conflit. Pour étendre le schéma dans l'annuaire Active Directory de Microsoft, Dell a reçu des OID uniques, des extensions de nom uniques et des ID d'attribut liés de manière unique pour les attributs et les classes ajoutés au service d'annuaire :

- Extension Dell : `dell`
- OID de base Dell : `1.2.840.113556.1.8000.1280`
- Plage d'ID de lien RAC : `12070` à `12079`

Présentation des extensions de schéma

Dell a étendu le schéma pour inclure les propriétés *Association*, *Périphériques* et *Privilège*. La propriété *Association* permet de lier les utilisateurs ou groupes possédant un ensemble de privilèges spécifiques à un ou plusieurs périphériques RAC. Ce modèle fournit à l'administrateur une souplesse optimale concernant les diverses combinaisons d'utilisateurs, de privilèges RAC et de périphériques RAC sur le réseau, sans rendre le système plus complexe.

Si vous disposez sur le réseau de deux CMC à intégrer à Active Directory pour l'authentification et l'autorisation, créez au moins un objet Association et un objet Périphérique RAC pour chaque CMC. Vous pouvez créer plusieurs objets Association, et lier chacun à autant d'utilisateurs, de groupes d'utilisateurs ou d'objets Périphérique RAC que vous le souhaitez. Les utilisateurs et les objets Périphérique RAC peuvent être membres de n'importe quel domaine dans l'entreprise.

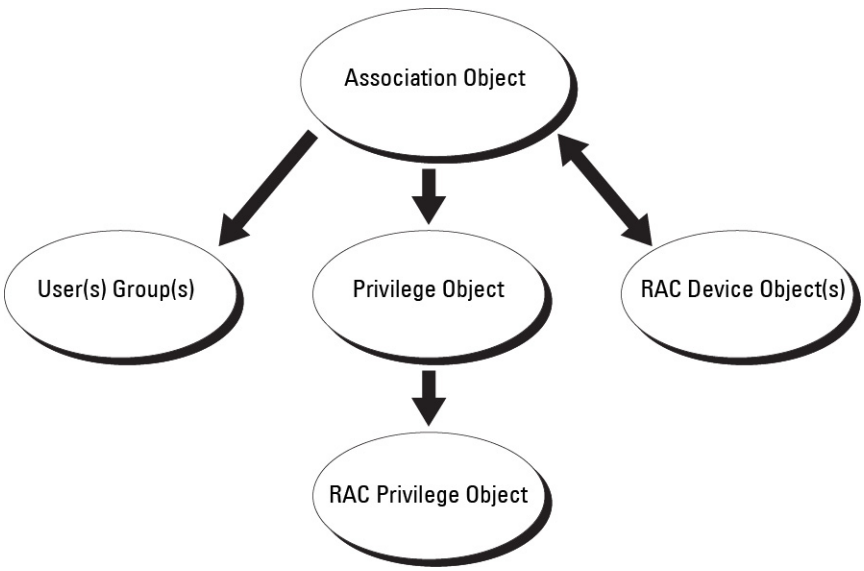
Cependant, chaque objet Association ne peut être lié (ou ne peut lier des utilisateurs, des groupes d'utilisateurs ou des objets Périphérique RAC) qu'à un seul objet Privilège. Cet exemple permet à l'administrateur de contrôler chacun des privilèges de l'utilisateur sur des CMC donnés.

L'objet Périphérique RAC est le lien que le logiciel RAC utilise pour envoyer à Active Directory des requêtes d'authentification et d'autorisation. Lorsqu'un RAC est ajouté au réseau, l'administrateur doit configurer ce RAC et son objet Périphérique avec le nom de son annuaire Active Directory, afin que les utilisateurs puissent employer l'authentification et l'autorisation Active Directory. L'administrateur doit également ajouter le RAC à au moins un objet Association pour permettre l'authentification des utilisateurs.

L'illustration suivante montre que l'objet Association fournit la connexion nécessaire à l'authentification et l'autorisation.

REMARQUE : L'objet Privilège RAC s'applique à DRAC 4, DRAC 5 et CMC.

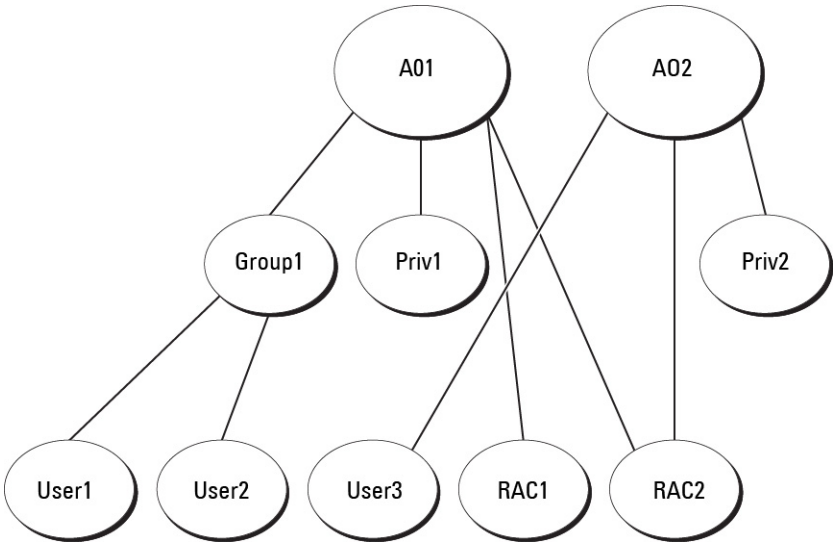
Vous pouvez créer un nombre illimité (ou aussi faible que vous le souhaitez) d'objets Association. Cependant, vous devez créer au moins un objet Association et disposer d'un objet Périphérique RAC pour chaque RAC (CMC) du réseau à intégrer à Active Directory.



L'objet Association permet de créer un nombre quelconque d'utilisateurs, de groupes et d'objets Périphérique RAC. Toutefois, l'objet Association contient un seul objet Privilège pour chaque objet Association. L'objet Association connecte les *Utilisateurs* possédant des *Privilèges* sur les RAC (CMC).

De plus, vous pouvez configurer des objets Active Directory dans un seul domaine ou dans plusieurs. Par exemple, vous disposez de deux CMC (RAC1 et RAC2) et de trois utilisateurs Active Directory existants (utilisateur1, utilisateur2 et utilisateur3). Vous souhaitez attribuer à utilisateur1 et à utilisateur2 le privilège Administrateur sur les deux CMC, et donner à utilisateur3 le privilège Connexion sur la carte RAC2. La figure suivante montre comment configurer les objets Active Directory dans ce scénario.

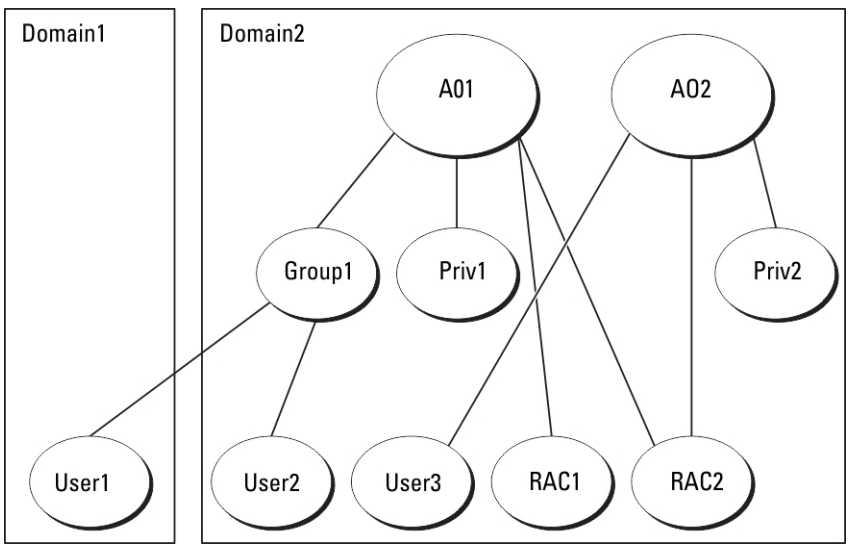
Lors de l'ajout de groupes universels de domaines distincts, créez un objet Association avec une étendue universelle. Les objets Association par défaut créés par l'utilitaire Dell Schema Extender sont des groupes locaux de domaines et ils ne fonctionnent pas avec les groupes universels des autres domaines.



Pour configurer les objets pour le scénario de domaine unique :

1. Créez deux objets Association.
2. Créez deux objets Périphérique RAC, RAC1 et RAC2, pour représenter les deux CMC.
3. Créez deux objets Privilège, Priv1 et Priv2 ; Priv1 disposant de tous les privilèges (administrateur) et Priv2 disposant des privilèges d'ouverture de session.
4. Groupez Utilisateur1 et Utilisateur2 dans le Groupe1.
5. Ajoutez Groupe1 comme membre de l'objet Association 1 (A01), Priv1 comme objet Privilège dans A01, et RAC1 et RAC2 comme périphériques RAC dans A01.
6. Ajoutez Utilisateur3 comme membre de l'objet Association 2 (A02), Priv2 comme objet Privilège dans A02 et RAC2 comme périphérique RAC dans A02.

La figure suivante montre la configuration des objets Active Directory dans plusieurs domaines. Dans ce scénario, vous utilisez 2 CMC (RAC1 et RAC2) et 3 utilisateurs Active Directory existants (utilisateur1, utilisateur2 et utilisateur3). Utilisateur1 est membre de Domaine1, mais utilisateur2 et utilisateur3 se trouvent dans Domaine2. Dans ce scénario, configurez utilisateur1 et utilisateur2 avec des privilèges Administrateur sur les deux CMC, et attribuez à utilisateur3 le privilège Connexion sur la carte RAC2.



Pour configurer les objets pour le scénario de domaines multiples :

1. Assurez-vous que la fonction de forêt de domaines est en mode Natif ou Windows 2003.
2. Créez deux objets Association, nommés A01 (étendue Universel) et A02, dans n'importe quel domaine. La figure « Configuration des objets Active Directory dans plusieurs domaines » montre les objets de Domaine2.
3. Créez deux objets Périphérique RAC, RAC1 et RAC2, pour représenter les deux CMC.
4. Créez deux objets Privilège, Priv1 et Priv2 ; Priv1 disposant de tous les privilèges (administrateur) et Priv2 disposant des privilèges d'ouverture de session.
5. Placez utilisateur1 et utilisateur2 dans Groupe1. L'étendue de Groupe1 doit être Universel.
6. Ajoutez Groupe1 comme membre de l'objet Association 1 (A01), Priv1 comme objet Privilège dans A01, et RAC1 et RAC2 comme périphériques RAC dans A01.
7. Ajoutez Utilisateur3 comme membre de l'objet Association 2 (A02), Priv2 comme objet Privilège dans A02 et RAC2 comme périphérique RAC dans A02.

Configuration d''Active Directory avec le schéma étendu

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. Configurez les propriétés Active Directory de CMC avec l'interface Web ou RACADM.

Liens connexes

Extension du schéma Active Directory
Installation de l'extension Dell dans le snap-in Utilisateurs et ordinateurs Microsoft Active Directory
Ajout d'utilisateurs et de privilèges CMC à Active Directory
Configuration d'Active Directory avec le schéma étendu à l'aide de l'interface Web CMC
Configuration d'Active Directory avec le schéma étendu à l'aide de l'interface RACADM

Extension du schéma Active Directory

L'extension du schéma Active Directory ajoute une unité organisationnelle Dell, des classes et des attributs de schéma, des exemples de privilèges et des objets Association au schéma Active Directory. Avant d'étendre le schéma, vérifiez que vous disposez des privilèges d'administration de schéma dans le rôle de propriétaire FSMO (Flexible Single Master Operation) du contrôleur de domaine principal dans la forêt de domaines.

Vous pouvez étendre votre schéma en utilisant l'une des méthodes suivantes :

- utilitaire Dell Schema Extender ;
- fichier script LDIF.

Si vous utilisez le fichier script LDIF, l'unité organisationnelle Dell n'est pas ajoutée au schéma.

Les fichiers LDIF et Dell Schema Extender se trouvent sur votre DVD *Dell Systems Management Tools and Documentation* dans les répertoires respectifs suivants :

- **<Lecteur_DVD>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_T ools \Remote_Management_Advanced\LDIF_Files**
- **<lecteur DVD>:\SYSMGMT\ManagementStation\support\OMActiveDirector y_Tools \Remote_Management_Advanced\Schema Extender**

Pour utiliser les fichiers LDIF, consultez les instructions du fichier « Lisez-moi » qui se trouve dans le répertoire **LDIF_Files**.

Vous pouvez copier et exécuter Schema Extender ou les fichiers LDIF depuis n'importe quel emplacement.

Utilisation de Dell Schema Extender

PRÉCAUTION : Dell Schema Extender utilise le fichier SchemaExtenderOem.ini. Pour assurer le bon fonctionnement de Dell Schema Extender, ne modifiez pas le nom de ce fichier.

1. Dans l'écran **d'accueil**, cliquez sur **Suivant**.
2. Lisez l'avertissement pour bien le comprendre, puis cliquez sur **Suivant**.
3. Sélectionnez **Utiliser les références d'ouverture de session actuelles** ou saisissez un nom d'utilisateur et un mot de passe ayant des droits d'administrateur de schéma.
4. Cliquez sur **Suivant** pour exécuter Dell Schema Extender.
5. Cliquez sur **Terminer**.

   Le schéma est étendu. Pour vérifier l'extension du schéma, utilisez la console MMC et le snap-in de schéma Active Directory pour vérifier l'existence des classes et attributs. Pour plus d'informations sur les classes et attributs, voir « Classes et attributs ». Consultez la documentation Microsoft pour plus d'informations sur l'utilisation de MMC et du snap-in de schéma Active Directory.

Classes et attributs

Tableau 19. : Définitions de classe pour les classes ajoutées au schéma Active Directory

Nom de classe	Numéro d'identification d'objet (OID) attribué
delliDRACDevice	1.2.840.113556.1.8000.1280.1.7.1.1
delliDRACAssociation	1.2.840.113556.1.8000.1280.1.7.1.2
dellRAC4Privileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

Tableau 20. : Classe dellRacDevice

OID	1.2.840.113556.1.8000.1280.1.7.1.1
Description	Représente le périphérique Dell RAC. Vous devez configurer RAC en tant que delliDRACDevice dans Active Directory. Cette configuration permet à CMC d'envoyer des requêtes LDAP (Lightweight Directory Access Protocol - Protocole léger d'accès à l'annuaire) à Active Directory.
Type de classe	Classe structurelle
SuperClasses	dellProduct
Attributs	dellSchemaVersion dellRacType

Tableau 21. : Classe delliDRACAssociationObject

OID	1.2.840.113556.1.8000.1280.1.7.1.2
Description	Représente l'objet Association Dell. Cet objet fournit la connexion entre les utilisateurs et les périphériques.
Type de classe	Classe structurelle
SuperClasses	Groupe
Attributs	dellProductMembers dellPrivilegeMember

Tableau 22. : Classe dellRAC4Privileges

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Description	Définit les privilèges (droits d'autorisation) du périphérique CMC.
Type de classe	Classe auxiliaire
SuperClasses	Aucun
Attributs	dellIsLoginUser dellIsCardConfigAdmin dellIsUserConfigAdmin dellIsLogClearAdmin dellIsServerResetUser dellIsTestAlertUser dellIsDebugCommandAdmin dellPermissionMask1 dellPermissionMask2

Tableau 23. : Classe dellPrivileges

OID	1.2.840.113556.1.8000.1280.1.1.1.4
Description	Fait office de classe de conteneurs pour les privilèges Dell (droits d'autorisation).
Type de classe	Classe structurelle
SuperClasses	Utilisateur
Attributs	dellRAC4Privileges

Tableau 24. : Classe dellProduct

OID	1.2.840.113556.1.8000.1280.1.1.1.5
Description	Classe principale à partir de laquelle tous les produits Dell sont dérivés.
Type de classe	Classe structurelle
SuperClasses	Ordinateur

OID	1.2.840.113556.1.8000.1280.1.1.1.5
Attributs	dellAssociationMembers

Tableau 25. : Liste des attributs ajoutés au schéma Active Directory

OID attribué/Identifiant d'objet de syntaxe	Valeur unique
Attribut : `dellPrivilegeMember` **Description** : liste des objets `dellPrivilege` appartenant à cet attribut. **OID** : 1.2.840.113556.1.8000.1280.1.1.2.1 **Nom unique** : (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
Attribut : `dellProductMembers` **Description** : liste des objets `dellRacDevices` appartenant à ce rôle. Cet attribut est le lien vers l'avant qui correspond au lien vers l'arrière `dellAssociationMembers`. **ID de lien** : 12070 **OID** : 1.2.840.113556.1.8000.1280.1.1.2.2 **Nom unique** : (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
Attribut : `dellIsCardConfigAdmin` **Description** : VRAI si l'utilisateur possède les droits Configuration de la carte sur le périphérique. **OID** : 1.2.840.113556.1.8000.1280.1.1.2.4 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut : `dellIsLoginUser` **Description** : VRAI si l'utilisateur possède les droits Ouverture de session sur le périphérique. **OID** : 1.2.840.113556.1.8000.1280.1.1.2.3 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut : `dellIsUserConfigAdmin` **Description** : TRUE (VRAI) si l'utilisateur possède les droits d'Administrateur de configuration des utilisateurs sur le périphérique. **OID** : 1.2.840.113556.1.8000.1280.1.1.2.5 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut : `delIsLogClearAdmin` **Description** : TRUE (VRAI) si l'utilisateur possède les droits d'Administrateur d'effacement des journaux sur le périphérique. **OID** : 1.2.840.113556.1.8000.1280.1.1.2.6 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut : `dellIsServerResetUser` **Description** : TRUE (VRAI) si l'utilisateur possède les droits de Réinitialisation du serveur sur le périphérique. **OID** : 1.2.840.113556.1.8000.1280.1.1.2.7 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE

OID attribué/Identifiant d'objet de syntaxe	Valeur unique
Attribut : `dellIsTestAlertUser` **Description** : TRUE (VRAI) si l'utilisateur possède les droits d'Utilisateur et test d'alertes sur le périphérique. **OID** : 1.2.840.113556.1.8000.1280.1.1.2.10 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut : `dellIsDebugCommandAdmin` **Description** : TRUE (VRAI) si l'utilisateur possède les droits d'Administrateur de commandes de débogage sur le périphérique. **OID** : 1.2.840.113556.1.8000.1280.1.1.2.11 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
Attribut : `dellSchemaVersion` **Description** : la version actuelle du schéma est utilisée pour mettre le schéma à jour. **OID** : 1.2.840.113556.1.8000.1280.1.1.2.12 Chaîne de non-prise en compte de la casse (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
Attribut : `dellRacType` **Description** : cet attribut est le type de RAC actuel pour l'objet dellRacDevice et le lien vers l'arrière correspondant au lien vers l'avant dellAssociationObjectMembers. **OID** : 1.2.840.113556.1.8000.1280.1.1.2.13 Chaîne de non-prise en compte de la casse (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
Attribut : `dellAssociationMembers` **Description** : liste des objets dellAssociationObjectMembers appartenant à ce rôle. Cet attribut est le lien vers l'arrière vers l'attribut dellProductMembers Linked. **ID de lien** : 12071 **OID** : 1.2.840.113556.1.8000.1280.1.1.2.14 Nom distingué (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
Attribut : `dellPermissionsMask1` **OID** : 1.2.840.113556.1.8000.1280.1.6.2.1 Integer (LDAPTYPE_INTEGER)	
Attribut : `dellPermissionsMask2` **OID** : 1.2.840.113556.1.8000.1280.1.6.2.2 Integer (LDAPTYPE_INTEGER)	

Installation de l'extension Dell dans le snap-in Utilisateurs et ordinateurs Microsoft Active Directory

Lorsque vous étendez le schéma dans Active Directory, vous devez également étendre le snap-in Utilisateurs et ordinateurs Active Directory pour que l'administrateur puisse gérer les périphériques RAC (CMC), les utilisateurs et les groupes d'utilisateurs, les associations RAC et les privilèges RAC.

Lorsque vous installez le logiciel de gestion de systèmes en utilisant le DVD *Dell Systems Management Tools and Documentation*, vous pouvez étendre le snap-in en sélectionnant l'option **Snap-in Utilisateurs et ordinateurs Active Directory** pendant l'installation. Voir le manuel « *Dell OpenManage Software Quick Installation Guide* » (Guide

d'installation rapide de Dell OpenManage) pour obtenir davantage d'instructions pour l'installation du logiciel de gestion de systèmes. Pour les systèmes d'exploitation Windows 64 bits, le programme d'installation du snap-in se trouve dans : **<lecteur DVD>:\SYSMGMT\ManagementStation\support\OMActiveDirect ory_SnapIn64**

Pour des informations supplémentaires sur le snap-in Utilisateurs et ordinateurs Active Directory, consultez la documentation Microsoft.

Ajout d'utilisateurs et de privilèges CMC à Active Directory

Le snap-in d'extension Dell Utilisateurs et ordinateurs Active Directory vous permet d'ajouter des utilisateurs et privilèges CMC en créant des objets Périphérique RAC, Association et Privilège. Pour ajouter chaque objet, procédez comme suit :

- Créez un objet Périphérique RAC
- Créez un objet Privilège.
- Créez un objet Association.
- Ajoutez des objets à un objet Association.

Liens connexes

Ajout d'objets à un objet Association
Création d'un objet Périphérique RAC
Création d'un objet Privilège
Création d'un objet Association

Création d'un objet Périphérique RAC

Pour créer un objet Périphérique RAC :

1. Dans la fenêtre **Racine de la console MMC**, cliquez avec le bouton droit sur un conteneur.
2. Sélectionnez **Nouveau → Objet avancé Dell Remote Management**. La fenêtre **Nouvel objet** s'affiche.
3. Entrez un nom pour le nouvel objet. Ce nom doit être identique au nom CMC entré à l'étape « Configuration d'Active Directory avec le schéma étendu à l'aide de l'interface Web CMC ».
4. Sélectionnez **Objet Périphérique RAC**, puis cliquez sur **OK**.

Création d'un objet Privilège

Pour créer un objet Privilège :

REMARQUE : Vous devez créer un objet Privilège dans le même domaine que l'objet Association associé.

1. Dans la fenêtre **Racine de la console (MMC)**, cliquez avec le bouton droit sur un conteneur.
2. Sélectionnez **Nouveau → Objet avancé Dell Remote Management**. La fenêtre **Nouvel objet** s'affiche.
3. Entrez le nom du nouvel objet.
4. Sélectionnez **Objet Privilège**, puis cliquez sur **OK**.
5. Cliquez avec le bouton droit de la souris sur l'objet Privilège que vous avez créé et sélectionnez **Propriétés**.
6. Cliquez sur l'onglet **Privilèges RAC**, et attribuez les privilèges voulus à l'utilisateur ou au groupe. Pour plus d'informations sur les privilèges utilisateur CMC, voir « Types d'utilisateur ».

Création d'un objet Association

L'objet Association est dérivé d'un groupe et doit contenir un type de groupe. L'étendue d'association spécifie le type de groupe de sécurité de l'objet Association. Lorsque vous créez un objet Association, choisissez l'étendue d'association qui s'applique au type des objets que vous prévoyez d'ajouter. Par exemple, si vous sélectionnez Universel, les objets Association sont disponibles uniquement lorsque le domaine Active Directory fonctionne en mode natif ou supérieur.

Pour créer un objet Association :

1. Dans la fenêtre **Racine de la console (MMC)**, cliquez avec le bouton droit sur un conteneur.
2. Sélectionnez **Nouveau** → **Objet avancé Dell Remote Management**. Cela ouvre la fenêtre **Nouvel objet**.
3. Entrez le nom du nouvel objet et sélectionnez **Objet Association**.
4. Sélectionnez l'étendue de l'**objet Association**, puis cliquez sur **OK**.

Ajout d'objets à un objet Association

Vous pouvez utiliser la fenêtre **Propriétés de l'objet Association** pour associer des utilisateurs ou groupes d'utilisateurs, des objets Privilège et des périphériques ou groupes de périphériques RAC. Si vous travaillez en mode Windows 2000 ou supérieur, utilisez des groupes de type Universel pour couvrir les domaines où résident vos objets Utilisateur ou RAC.

Vous pouvez ajouter des groupes d'utilisateurs et de périphériques RAC. La procédure est identique, que vous souhaitiez créer un groupe lié à Dell ou non lié à Dell.

Liens connexes

Ajout d'utilisateurs ou de groupes d'utilisateurs
Ajout de privilèges
Ajout de périphériques RAC ou de groupes de périphériques RAC

Ajout d'utilisateurs ou de groupes d'utilisateurs

Pour ajouter des utilisateurs ou des groupes d'utilisateurs :

1. Cliquez avec le bouton droit de la souris sur **l'objet Association** et sélectionnez **Propriétés**.
2. Sélectionnez l'onglet **Utilisateurs** et cliquez sur **Ajouter**.
3. Entrez le nom de l'utilisateur ou du groupe d'utilisateurs, puis cliquez sur **OK**.

Ajout de privilèges

Pour ajouter des privilèges :

1. Sélectionnez l'onglet **Objet Privilège** et cliquez sur **Ajouter**.
2. Entrez le nom de l'objet Privilège et cliquez sur **OK**.
   Cliquez sur l'onglet **Objet Privilège** pour ajouter l'objet Privilège à l'objet Association qui définit les privilèges de l'utilisateur ou du groupe d'utilisateurs lors de l'authentification auprès d'un périphérique DRAC. Vous ne pouvez ajouter qu'un seul objet Privilège à chaque objet Association.

Ajout de périphériques RAC ou de groupes de périphériques RAC

Pour ajouter des périphériques RAC ou des groupes de périphériques RAC :

1. Sélectionnez l'onglet **Produits** et cliquez sur **Ajouter**.
2. Entrez le nom des périphériques RAC ou des groupes de périphériques RAC, puis cliquez sur **OK**.
3. Dans la fenêtre **Propriétés**, cliquez sur **Appliquer**, puis sur **OK**.
   Cliquez sur l'onglet **Produits** pour ajouter un ou plusieurs périphériques RAC à l'objet Association. Les objets associés spécifient les périphériques RAC connectés au réseau qui sont disponibles pour les utilisateurs ou groupes d'utilisateurs définis. Il est possible d'ajouter plusieurs périphériques RAC à un objet Association.

Configuration d'Active Directory avec le schéma étendu à l'aide de l'interface Web CMC

Pour configurer Active Directory avec le schéma étendu dans l'interface Web CMC :

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

1. Dans l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **Authentification utilisateur → Services d'annuaire**.
2. Sélectionnez **Microsoft Active Directory (Schéma étendu)**. Les paramètres à configurer pour le schéma étendu sont affichés dans la même page.
3. Paramétrez les options suivantes :
   - Activez Active Directory, entrez le nom du domaine racine (root) et la valeur de délai d'attente.
   - Pour que l'appel acheminé fasse une recherche dans le contrôleur de domaine et le catalogue global, sélectionnez l'option **Serveur AD de recherche à examiner (facultatif)**, puis spécifiez les détails du contrôleur de domaine et du catalogue global.

     REMARQUE : La définition de l'adresse IP 0.0.0.0 empêche CMC de rechercher un serveur.

     REMARQUE : Vous pouvez spécifier une liste de serveurs de contrôleur de domaine ou de catalogue global, séparée par des virgules. CMC vous permet de spécifier jusqu'à trois adresses IP ou noms d'hôte.

     REMARQUE : Les serveurs de contrôleur de domaine ou de catalogue global qui ne sont pas correctement configurés pour tous les domaines et applications peuvent produire des résultats inattendus au cours du fonctionnement des applications/domaines existants.
4. Cliquez sur **Appliquer** pour enregistrer les paramètres.

   REMARQUE : Vous devez appliquer les paramètres avant de continuer. Si vous ne le faites pas, ils sont perdus lorsque vous passez à une autre page.
5. Dans la section **Paramètres du schéma étendu**, entrez le nom de périphérique et le nom de domaine CMC.
6. Si vous avez activé la validation de certificat, vous devez téléverser le certificat autosigné racine de la forêt de domaines vers CMC. Dans la section **Gérer les certificats**, entrez le chemin du fichier de certificat ou naviguez jusqu'à ce fichier. Cliquez sur **Téléverser** pour téléverser le fichier vers CMC.

   REMARQUE : La valeur `Chemin du fichier` indique le chemin relatif du fichier de certificat que vous téléversez. Vous devez saisir le chemin absolu de ce fichier, à savoir son chemin complet, son nom et son extension.

   Les certificats SSL des contrôleurs de domaine doivent être signés par le certificat racine signé par l'autorité de certification. Ce certificat racine doit être disponible sur la station de gestion qui accède à CMC.

   PRÉCAUTION : La validation de certificat SSL est requise par défaut. Vous prenez des risques si vous désactivez ce certificat.
7. Si vous avez activé la connexion directe (SSO), accédez à la section Fichier keytab Kerberos, cliquez sur **Parcourir**, spécifiez le fichier keytab, puis cliquez sur **Téléverser**. Une fois l'opération terminée, un message s'affiche, signalant la réussite ou l'échec du téléversement.
8. Cliquez sur **Appliquer**. Le serveur Web CMC redémarre automatiquement lorsque vous cliquez sur **Appliquer**.
9. Connectez-vous à l'interface Web CMC.
10. Sélectionnez **Châssis** dans l'arborescence système, cliquez sur l'onglet **Réseau**, puis sur le sous-onglet **Réseau**. La page **Configuration réseau** s'affiche.
11. Si l'option **Utiliser DHCP** est activée pour l'adresse IP de l'interface réseau CMC, effectuez l'une des opérations suivantes :
    - Sélectionnez l'option **Utiliser DHCP pour obtenir des adresses de serveur DNS** afin qu'il soit possible d'obtenir automatiquement les adresses de serveur DNS depuis le serveur DHCP.
    - Configurez manuellement une adresse IP de serveur DNS en laissant la case **Utiliser DHCP pour obtenir des adresses de serveur DNS** décochée puis en tapant vos adresses IP de serveur DNS principal et d'autre serveur DNS dans les champs fournis à cet effet.
12. Cliquez sur **Appliquer les changements**. Les paramètres Active Directory du schéma étendu sont configurés.

Configuration d'Active Directory avec le schéma étendu à l'aide de l'interface RACADM

Pour configurer Active Directory avec le schéma étendu à l'aide de RACADM :

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

   ```
   racadm config -g cfgActiveDirectory -o cfgADEnable 1 racadm config -g
   cfgActiveDirectory -o cfgADType 1 racadm config -g cfgActiveDirectory -o
   cfgADRacDomain <nom de domaine CMC entièrement qualifié (FQDN)> racadm
   config -g cfgActiveDirectory -o cfgADRootDomain <nom entièrement qualifié
   du domaine racine> racadm config -g cfgActiveDirectory -o cfgADRacName <nom
   commun CMC> racadm sslcertupload -t 0x2 -f <certificat de CA racine ADS> -r
   racadm sslcertdownload -t 0x1 -f <certificat SSL CMC>
   ```

   REMARQUE : Cette commande ne peut être utilisée qu'avec le RACADM distant. Pour plus d'informations sur l'interface RACADM distante, voir le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de l'interface de ligne de commande RACADM pour iDRAC7 et CMC).

   Facultatif : pour spécifier un serveur LDAP ou de catalogue global au lieu d'utiliser les serveurs renvoyés par le serveur DNS pour rechercher un nom d'utilisateur, entrez la commande suivante pour activer l'option **Spécifier un serveur** :

   ```
   racadm config -g cfgActiveDirectory -o cfgADSpecifyServerEnable 1
   ```

   REMARQUE : Lorsque vous utilisez l'option **Spécifier un serveur**, le nom d'hôte figurant dans le certificat signé par l'autorité de certification (CA) n'est pas comparé au nom du serveur spécifié. Cela est particulièrement utile si vous êtes administrateur CMC, car cela vous permet d'entrer à la fois un nom d'hôte et une adresse IP.

   Après avoir activé l'option **Spécifier un serveur**, vous pouvez spécifier un serveur LDAP et un serveur de catalogue global à l'aide des adresses IP ou des noms FQDN (Fully Qualified Domain Name - Nom de domaine entièrement qualifié) de ces serveurs. Les noms FQDN incluent les noms d'hôte et les noms de domaine des serveurs.

   Pour spécifier un serveur LDAP, entrez :

   ```
   racadm config -g cfgActiveDirectory -o cfgADDomainController <Adresse IP du
   contrôleur de domaine AD>
   ```

   Pour spécifier un serveur de catalogue global, entrez :

   ```
   racadm config -g cfgActiveDirectory -o cfgADGlobalCatalog <Adresse IP de
   catalogue global AD>
   ```

   REMARQUE : La définition de l'adresse IP 0.0.0.0 empêche CMC de rechercher un serveur.

   REMARQUE : Vous pouvez spécifier une liste de serveurs LDAP ou de serveurs de catalogue global, séparée par des virgules. CMC vous permet de spécifier jusqu'à trois adresses IP ou noms d'hôte.

   REMARQUE : Les LDAP qui ne sont pas correctement configurés pour tous les domaines et applications peuvent produire des résultats inattendus au cours du fonctionnement des applications/domaines existants.

2. Spécifiez un serveur DNS à l'aide de l'une des options suivantes :

   - Si DHCP est activé sur le CMC et que vous voulez utiliser l'adresse DNS obtenue automatiquement par le serveur DHCP, entrez la commande suivante :

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

   - Si le protocole DHCP est désactivé sur CMC ou s'il est activé mais que vous voulez spécifier manuellement l'adresse IP DNS, entrez les commandes suivantes :

     ```
     racadm config -g cfgLanNetworking -o cfgDNSServersFromDHCP 0 racadm
     config -g cfgLanNetworking -o cfgDNSServer1 <adresse IP du DNS
     primaire> racadm config -g cfgLanNetworking -o cfgDNSServer2 <adresse
     IP du DNS secondaire>
     ```

   La configuration de la fonctionnalité de schéma étendu est terminée.

Configuration d'utilisateurs LDAP générique

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

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

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

Pour plus informations sur le niveau de privilèges des groupes de rôle et sur les paramètres par défaut de ces groupes, voir « Types d'utilisateur ».

La figure suivante illustre la configuration de CMC avec un LDAP générique.

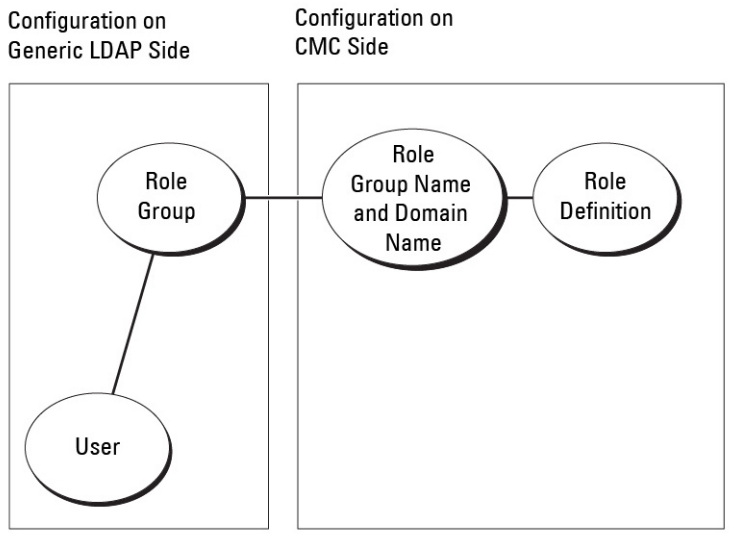


Figure 2. Configuration de CMC avec un LDAP générique

Configuration de l'annuaire LDAP générique pour accéder à CMC

L'implémentation LDAP générique de CMC utilise deux phases pour autoriser l'accès d'un utilisateur : l'authentification de cet utilisateur, puis son autorisation.

Authentification des utilisateurs LDAP

Certains serveurs d'annuaire exigent une liaison avant les recherches sur un serveur LDAP spécifique.

Pour authentifier un utilisateur :

1. (Facultatif) Connectez-vous au service d'annuaire. Par défaut, il s'agit d'une connexion anonyme.
2. Recherchez l'utilisateur sur la base de son nom de connexion. L'attribut par défaut est `uid`.

3. Si plusieurs objets sont trouvés, le processus renvoie une erreur.
4. Annulez la liaison et effectuez une liaison avec le DN et le mot de passe de l'utilisateur.
5. En cas d'échec de la liaison, la connexion échoue également.
   Si ces étapes réussissent, l'utilisateur est authentifié.

Autorisation des utilisateurs LDAP

Pour autoriser un utilisateur :

1. Recherchez le nom de domaine de chaque groupe de l'utilisateur dans les attributs `member (Membre) ou uniqueMember (Membre unique)`. L'administrateur peut configurer ce champ.
2. Pour chaque groupe dont l'utilisateur est membre, ajoutez ses privilèges.

Configuration du service d'annuaire LDAP générique à l'aide de l'interface Web de CMC

Pour configurer le service d'annuaire LDAP générique en utilisant l'interface Web :

REMARQUE : Vous devez disposer du privilège **Administrateur de configuration du châssis**.

1. Dans l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **Authentification utilisateur** → **Services d'annuaire**.
2. Sélectionnez **LDAP générique**. Les paramètres à configurer pour le schéma standard sont affichés dans la même page.
3. Paramétrez les options suivantes :

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

   - Paramètres communs
   - Serveur à utiliser avec LDAP :
     * Serveur statique : spécifiez le nom FQDN (Fully Qualified Domain Name, nom de domaine entièrement qualifié) ou l'adresse IP, et le numéro du port LDAP.
     * Serveur DNS : spécifiez le serveur DNS afin de récupérer la liste des serveurs LDAP d'après leur enregistrement SRV dans DNS.
       La requête DNS suivante est effectuée pour les enregistrements SRV :
       `_<Nom du service>._tcp.<Domaine de recherche>`
       où `<Domaine de recherche>` est le domaine racine à utiliser dans la requête et `<Nom du service>` 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 une entrée **Groupe de rôles**. La page **Configurer le groupe de rôles LDAP** s'affiche.
6. Spécifiez le nom de domaine 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 avec l'interface 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=com`

CMC peut, si vous le souhaitez, être configuré pour interroger un serveur DNS à la recherche d'enregistrements SRV. Si vous activez la propriété `cfgLDAPSRVLookupEnable`, la propriété `cfgLDAPServer` est ignorée. La requête suivante est utilisée pour trouver des 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 plus d'informations sur les objets RACADM, voir le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC), disponible sur le site **dell.com/support/manuals**.

10

Configuration de CMC pour la connexion directe (SSO) ou la connexion par carte à puce

Cette section fournit des informations sur la configuration de CMC pour la connexion par carte à puce et pour la connexion directe (SSO) des utilisateurs Active Directory.

Depuis CMC version 2.10, CMC prend en charge l'authentification Active Directory basée sur Kerberos pour la gestion des connexions directes (SSO) et par carte à puce.

La connexion SSO utilise Kerberos comme méthode d'authentification, ce qui permet aux utilisateurs connectés au domaine de se connecter automatiquement (connexion directe) aux autres applications, notamment Exchange. Pour la connexion directe, 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 autoriser les systèmes à 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, naviguez jusqu'à la page **Services** et désactivez toutes les interfaces de connexion (ou seulement 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.

Liens connexes

Configuration système requise

Prérequis pour la connexion directe ou par carte à puce

Configuration de la connexion directe ou par carte à puce CMC pour les utilisateurs Active Directory

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 bien installé les derniers Service Packs et correctifs sur le système client. Si vous utilisez Active Directory sous Windows 2008, veillez à installer SP1 avec les correctifs Hot Fix suivants :

  Windows6.0-KB951191-x86.msu pour l'utilitaire KTPASS. Sans ce correctif, l'utilitaire génère des fichiers keytab incorrects.

  Windows6.0-KB957072-x86.msu pour utiliser les transactions GSS_API et SSL pendant une liaison LDAP.
- Centre de distribution de clés Kerberos (fourni avec le logiciel du serveur Active Directory Server)
- Serveur DHCP (recommandé)

- La zone inverse du serveur DNS doit comporter une entrée pour le serveur Active Directory et pour CMC

Systèmes clients

- Pour utiliser uniquement la connexion par carte à puce, votre système client doit comporter la version redistribuable de Microsoft Visual C++ 2005. Pour plus d'informations, visitez le site **www.microsoft.com/downloads/details.aspx?FamilyID= 32BC1BEEA3F9-4C13-9C99-220B62A191EE&displaylang=en**.
- Pour la connexion directe ou par carte à puce, le système client doit faire partie du domaine Active Directory et du royaume Kerberos.

CMC

- Vous devez installer la version 2.10 ou supérieure du micrologiciel CMC.
- Chaque CMC doit posséder un compte Active Directory.
- CMC doit faire partie du domaine Active Directory et du royaume Kerberos.

Prérequis pour la connexion directe ou par carte à puce

Les prérequis de configuration de la connexion directe (SSO) ou par carte à puce sont les suivants :

- Configurez le royaume kerberos et le KDC (Key Distribution Center, centre de distribution de clés) pour Active Directory (ksetup).
- Installez une infrastructure NTP et DNS robuste pour éviter les problèmes de dérive d'horloge et de recherche inversée.
- Configurez CMC avec le groupe de rôles de schéma standard Active Directory, avec des membres autorisés.
- Pour la carte à puce, créez des utilisateurs Active Directory pour chaque CMC, configurés pour utiliser le cryptage DES Kerberos, mais pas la préauthentification.
- Configurez le navigateur pour la connexion directe (SSO) ou par carte à puce.
- Enregistrez les utilisateurs CMC auprès du centre de distribution de clés avec Ktpass (cela génère également une clé pour le téléversement dans CMC).

Liens connexes

Configuration d'Active Directory avec le schéma standard
Configuration d''Active Directory avec le schéma étendu
Configuration du navigateur pour la connexion directe (SSO)
Génération d'un fichier Keytab Kerberos
Configuration du navigateur pour la connexion par carte à puce

Génération d'un fichier Keytab Kerberos

Pour prendre en charge l'authentification de connexion directe (SSO) et par carte à puce, CMC prend en charge le réseau Windows Kerberos. L'outil ktpass (disponible chez Microsoft, sur le CD/DVD d'installation du serveur) permet de créer des liaisons SPN (Service Principal Name - Nom de principal du service) 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 adresser CMC sur 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 `nom_cmc.nom_domaine.com` doit être en minuscules pour respecter la norme RFC et la valeur `@NOM_ROYAUME` doit être en majuscules. 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 de CMC pour le schéma Active Directory

Pour plus d'informations sur la configuration de CMC pour le schéma standard Active Directory, voir « Configuration d'Active Directory avec le schéma standard ».

Pour plus d'informations sur la configuration de CMC pour le schéma étendu Active Directory, voir « Présentation d'Active Directory avec schéma étendu ».

Configuration du navigateur pour la connexion directe (SSO)

La connexion directe (SSO, Single Sign-On) est prise en charge dans Internet Explorer versions 6.0 et supérieures, et dans Firefox versions 3.0 et supérieures.

REMARQUE : Les instructions suivantes s'appliquent uniquement si CMC utilise la connexion directe avec l'authentification Kerberos.

Internet Explorer

Pour configurer Internet Explorer pour la connexion directe :

1. Dans Internet Explorer, sélectionnez **Outils** → **Options Internet**.
2. Dans l'onglet **Sécurité**, sous **Cliquez sur une zone pour afficher ou modifier les paramètres de sécurité**, sélectionnez **Intranet local**.
3. Cliquez sur **Sites**.

   La boîte de dialogue **Intranet local** s'affiche.
4. Cliquez sur **Avancé**.

   La boîte de dialogue **Paramètres avancés Intranet local** s'affiche.
5. Dans **Ajouter ce site Web à la zone**, saisissez le nom de CMC et le domaine auquel il appartient, puis cliquez sur **Ajouter**.

   REMARQUE : Vous pouvez utiliser un caractère générique (*) pour spécifier tous les périphériques ou utilisateurs du domaine.

Mozilla Firefox

1. Dans Firefox, saisissez **about:config** dans la barre d'adresse.

REMARQUE : Si le navigateur affiche l'avertissement **Ceci risque d'annuler votre garantie**, cliquez sur **Je ferai attention, promis !**.

2. Dans la zone de texte **Filtre**, entrez **negotiate**.

   Le navigateur affiche une liste des noms des préférences qui contiennent le terme negotiate uniquement.

3. Dans la liste, double-cliquez sur **network.negotiate-auth.trusted-uris**.
4. Dans la boîte de dialogue **Saisir une valeur de chaîne**, saisissez le nom de domaine CMC et cliquez sur **OK**.

Configuration du navigateur pour la connexion par carte à puce

Mozilla Firefox : CMC 2.10 ne prend pas en charge la connexion par carte à puce via le navigateur Firefox.

Internet Explorer : vérifiez que votre navigateur Internet est configuré pour télécharger les plug-ins Active-X.

Configuration de la connexion directe ou par carte à puce CMC pour les utilisateurs Active Directory

Vous pouvez utiliser l'interface Web CMC ou RACADM pour configurer la connexion directe (SSO) ou par carte à puce CMC.

Liens connexes

Prérequis pour la connexion directe ou par carte à puce

Téléversement du fichier keytab

Configuration de la connexion directe ou par carte à puce CMC pour les utilisateurs Active Directory dans l'interface Web

Pour configurer la connexion directe (SSO) ou par carte à puce Active Directory pour CMC :

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

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

   - Téléversez 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 : Toutes les interfaces hors bande de ligne de commande, y compris Secure Shell (SSH), Telnet, l'interface série et le RACADM à distance, restent inchangées si vous sélectionnez cette option.

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 <utilisateur>@<domaine>
   ```

   où `<utilisateur>` correspond à un compte utilisateur Active Directory valide.

   La réussite de cette commande indique que CMC parvient à acquérir les références Kerberos et à accéder au compte Active Directory de l'utilisateur. Si la commande échoue, résolvez l'erreur et exécutez à nouveau la commande. Pour plus d'informations, reportez-vous au manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC), disponible sur le site **dell.com/support/manuals**.

Téléversement du fichier keytab

Le fichier keytab Kerberos fournit les références de nom d'utilisateur et de mot de passe CMC à Kerberos Data Center (KDC), qui à son tour autorise l'accès à l'annuaire Active Directory. Chaque CMC du royaume Kerberos doit être enregistré auprès de l'annuaire Active Directory et disposer d'un fichier keytab unique.

Vous pouvez téléverser un fichier keytab Kerberos généré sur le serveur Active Directory associé. Pour générer le fichier keytab Kerberos à partir du serveur Active Directory, exécutez l'utilitaire **ktpass.exe**. Ce fichier keytab établit une relation de confiance entre le serveur Active Directory et CMC.

Pour téléverser le fichier keytab :

1. Dans l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **Authentification utilisateur** → **Services d'annuaire**.
2. Sélectionnez **Microsoft Active Directory (Schéma standard)**.
3. Dans la section **Fichier keytab Kerberos**, cliquez sur **Parcourir**, sélectionnez le 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 ou par carte à puce CMC pour les utilisateurs Active Directory avec 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`

11

Configuration de CMC pour utiliser des consoles de ligne de commande

Cette section fournit des informations sur les fonctionnalités 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 des systèmes via la console. Pour plus d'informations sur l'utilisation des commandes RACADM dans CMC avec la console de ligne de commande, voir le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC).

Liens connexes

Connexion à CMC avec la console série, Telnet ou SSH

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 (connect) intégrée, qui permet de se connecter à la console série des serveurs et des modules d'E/S ; également disponible sous la forme `racadm connect`.
- Modification et historique de la 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 26. : Commandes de la ligne de commande CMC

Commande	Description
`racadm`	Les commandes RACADM commencent par le mot-clé `racadm`, suivi d'une sous-commande. Pour plus d'informations, voir le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC).
`connect`	Permet de se connecter à la console série d'un serveur ou d'un module d'E/S. Pour plus d'informations, voir « Connexion aux serveurs ou aux modules d'E/S à l'aide de la commande Connect ».

Commande	Description
	REMARQUE : Vous pouvez également utiliser la commande `racadm connect`.
`exit`, `logout` et `quit`	Toutes ces commandes effectuent la même opération. Elles mettent fin à la session actuelle et vous ramènent à l'invite de connexion.

Utilisation d'une console Telnet avec CMC

Vous pouvez ouvrir simultanément jusqu'à quatre sessions Telnet avec CMC.

Si votre station de gestion exécute Windows XP ou Windows 2003, vous pouvez rencontrer un problème de caractères dans une session Telnet CMC. Cela peut donner lieu au gel de la connexion, parce que la touche Retour ne répond pas et que le message de saisie du mot de passe n'apparaît pas.

Pour corriger le problème, téléchargez le correctif Hotfix 824810 depuis le site Web du support Microsoft, à l'adresse **support.microsoft.com**. Pour plus d'informations, voir l'article de base de connaissances Microsoft Knowledge Base numéro 824810.

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 CMC prend en charge SSH version 2 avec authentification par mot de passe. Par défaut, SSH est activé sur le 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` avec **Putty.exe**. L'exécution d'`OpenSSH` à l'invite de commande Windows offre seulement des fonctionnalités limitées (certaines touches ne répondent pas et aucun graphique n'est affiché). Sous Linux, exécutez les services client SSH pour vous connecter à CMC avec n'importe quel shell.

Le système prend en charge quatre sessions SSH simultanées. Le délai d'attente de session est contrôlé par la propriété `cfgSsnMgtSshIdleTimeout`. Pour plus d'informations, voir le chapitre traitant des propriétés de base de données dans le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC), la page **Gestion des services** de l'interface Web ou la rubrique « Configuration des services ».

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. Pour plus d'informations, voir « Configuration de l'authentification par clé publique sur SSH ».

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

Pour configurer SSH, voir « Configuration des services ».

Liens connexes

Configuration des services

Schémas cryptographiques SSH pris en charge

Pour communiquer avec CMC en utilisant le protocole SSH, le système prend en charge les schémas cryptographiques répertoriés dans le tableau suivant.

Tableau 27. : Schémas cryptographiques

Type de schéma	Couleurs
Cryptographie asymétrique	Spécification de bits (aléatoire) Diffie-Hellman DSA/DSS 512-1024 par NIST
Cryptographie symétrique	• AES256-CBC • RIJNDAEL256-CBC • AES192-CBC • RIJNDAEL192-CBC • AES128-CBC • RIJNDAEL128-CBC • BLOWFISH-128-CBC • 3DES-192-CBC • ARCFOUR-128
Intégrité du message	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
Authentification	Mot de passe

Configuration de l'authentification par clé publique sur SSH

Vous pouvez configurer jusqu'à 6 clés publiques, qui seront 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 d'affichage pour connaître les clés déjà configurées, afin qu'aucune clé ne soit accidentellement écrasée ou supprimée. Le nom d'utilisateur du service correspond à un compte utilisateur spécial, qui peut être utilisé pour l'accès au 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 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 fonctionnalité ; 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. 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, n'oubliez pas que le CMC utilise uniquement les 16 premiers caractères. Le commentaire de clé publique permet au 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 des informations supplémentaires sur la commande `sshpkauth`, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC* (Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC).

Liens connexes

Génération de clés publiques pour Windows
Génération de clés publiques pour Linux
Notes de syntaxe RACADM pour CMC
Affichage des clés publiques
Ajout de clés publiques
Suppression de clés publiques

Génération de clés publiques pour 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 PuTTY Key Generator pour les clients Windows afin de créer la clé de base :

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. Cette valeur doit être comprise entre 768 et 4096.

   REMARQUE : 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 essaierez d'ouvrir une session avec ces clés, vous échouerez.
3. Cliquez sur **Générer** et déplacez la souris dans la fenêtre en suivant les instructions.

   Une fois la clé créée, vous pouvez modifier le champ Commentaire de la clé.

   Vous pouvez également entrer une phrase de phase pour sécuriser la clé. Veillez à bien enregistrer la clé privée.
4. Vous pouvez utiliser la clé publique de deux façons :
   - Enregistrer la clé publique dans un fichier à téléverser ultérieurement.
   - Copier/coller le texte de la fenêtre **Clé publique à coller** lors de l'ajout du compte à l'aide de l'option de texte.

Génération de clés publiques pour Linux

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

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

où

L'option `-t` doit être dsa ou rsa.

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

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

La valeur <`phrase de passe`> est facultative. Une fois la commande exécutée, utilisez le fichier public pour le transmettre à RACADM afin de le téléverser.

Notes de syntaxe RACADM pour CMC

Lorsque vous utilisez la commande `racadm sshpkauth`, vérifiez les points suivants :

- Pour l'option `–i`, le paramètre doit être `svcacct`. Tous les autres paramètres entrés pour `–i` échouent dans CMC. La valeur `svcacct` désigne un compte spécial destiné à l'authentification par clé publique sur SSH dans CMC.
- Pour se connecter au CMC, l'utilisateur doit être un service. Les utilisateurs d'autres catégories peuvent accéder aux clés publiques entrées avec la commande `sshpkauth`.

Affichage des clés publiques

Pour afficher les clés publiques que vous avez ajoutées au CMC, entrez :

```
racadm sshpkauth –i svcacct –k all –v
```

Pour afficher une clé à la fois, remplacez l'argument `all` par un numéro compris entre 1 et 6. Par exemple, pour afficher la clé 2, entrez :

```
racadm sshpkauth –i svcacct –k 2 –v
```

Ajout de clés publiques

Pour ajouter une clé publique à CMC à l'aide des options de téléversement de fichier `–f`, entrez :

```
racadm sshpkauth –i svcacct –k 1 –p 0xfff –f <fichier de clé publique>
```

REMARQUE : Vous pouvez uniquement utiliser l'option de téléversement de fichier avec l'interface RACADM distante. Pour plus d'informations, voir le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de l'interface de ligne de commande RACADM pour iDRAC7 et CMC).

Pour ajouter une clé publique à l'aide de l'option de téléversement de texte, entrez :

```
racadm sshpkauth –i svcacct –k 1 –p 0xfff –t "<texte de clé publique>"
```

Suppression de clés publiques

Pour supprimer une clé publique, entrez :

```
racadm sshpkauth –i svcacct –k 1 –d
```

Pour supprimer toutes les clés publiques, entrez :

```
racadm sshpkauth –i svcacct –k all –d
```

Activation de la connexion entre panneau avant et iKVM

Pour obtenir des informations et des instructions sur l'utilisation des ports de panneau avant du module iKVM, voir « Activation ou désactivation de l'accès à iKVM depuis le panneau avant ».

Configuration du logiciel d'émulation de terminal

Le CMC prend en charge une console texte série depuis une station de gestion exécutant l'un des types de logiciel d'émulation de terminal suivants :

- Linux Minicom
- HyperTerminal Private Edition (version 6.3) de Hilgraeve

Effectuez les étapes des sous-sections suivantes pour configurer votre type de logiciel de terminal.

Configuration de Linux Minicom

Minicom est un utilitaire d'accès au port série pour Linux. La procédure suivante est valide pour la configuration de Minicom version 2.0. Les autres versions de Minicom peuvent être légèrement différentes mais vous trouverez les mêmes paramètres de base. Pour configurer les autres versions de Minicom, voir la rubrique « Paramètres Minicom requis ».

Configuration de Minicom version 2.0

REMARQUE : Pour des résultats optimaux, configurez la propriété **cfgSerialConsoleColumns** afin qu'elle corresponde au nombre de colonnes. Attention, l'invite consomme deux caractères. Par exemple, pour une fenêtre de terminal à 80 colonnes :

```
racadm config -g cfgSerial -o cfgSerialConsoleColumns 80.
```

1. Si vous ne possédez pas de fichier de configuration de Minicom, passez à l'étape suivante. Si vous disposez d'un fichier de configuration de Minicom, entrez `minicom<nom du fichier de configuration de Minicom>`, puis passez à l'étape 12.
2. À l'invite de commande Linux, tapez `minicom -s`.
3. Sélectionnez **Configuration du port série** et appuyez sur <Entrée>.
4. Appuyez sur <a> et sélectionnez le périphérique série approprié (par exemple, `/dev/ttyS0`).
5. Appuyez sur <e> et définissez l'option **Bits par seconde/Parité/Bits** sur **115200 8N1**.
6. Appuyez sur <f>, puis définissez **Contrôle de flux matériel** sur **Oui** et **Contrôle de flux logiciel** sur **Non**. Pour quitter le menu **Configuration des ports série**, appuyez sur <Entrée>.
7. Sélectionnez **Modem et numérotation** et appuyez sur <Entrée>.
8. Dans le menu **Configuration du modem et de la numérotation**, appuyez sur <Ret. Arr.> pour effacer les paramètres **init**, **reset**, **connect** et **hangup** afin de les laisser vides. Appuyez ensuite sur <Entrée> pour enregistrer chaque valeur vide.
9. Lorsque tous les champs indiqués ont été effacés, appuyez sur <Entrée> pour quitter le menu **Configuration de la numérotation du modem et des paramètres**.
10. Sélectionnez **Quitter Minicom** et appuyez sur <Entrée>.
11. À l'invite du shell de commandes, entrez `minicom <nom du fichier de configuration de Minicom>`.
12. Appuyez sur <Ctrl+a>, <x>, <Entrée> pour quitter Minicom.

    Vérifiez que la fenêtre Minicom affiche l'invite de connexion. Si cette invite apparaît, votre connexion a réussi. Vous êtes prêt à ouvrir une session et à accéder à l'interface de ligne de commande (CLI) CMC.

Paramètres Minicom requis

Consultez le tableau suivant pour configurer Minicom, quelle que soit la version.

Tableau 28. : Paramètres Minicom

Description du paramètre	Paramètre requis
B/s/Par/Bits	115200 8N1
Contrôle du débit matériel	Oui
Contrôle du débit logiciel	Non
Émulation de terminal	ANSI

Description du paramètre	Paramètre requis
Paramètres de la numérotation du modem et des paramètres	Effacez les paramètres **init**, **reset**, **connect** et **hangup** pour qu'ils soient vides.

Connexion aux serveurs ou aux modules d'E/S avec la commande Connect

CMC peut établir une connexion pour rediriger la console série du serveur ou des modules d'E/S.

Pour les serveurs, vous pouvez effectuer la redirection de console série à l'aide des outils suivants :

- Ligne de commande CMC, et commande connect ou racadm connect. Pour plus d'informations, voir le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de l'interface de ligne de commande RACADM pour iDRAC7 et CMC).
- 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 CMC prend en charge la commande connect pour l'établissement d'une connexion série aux modules de serveur ou modules d'E/S (IOM). La console série du serveur contient à la fois les écrans d'amorçage et de configuration du BIOS, et la console série du système d'exploitation. Pour les modules d'E/S, la console série du commutateur est disponible.

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

REMARQUE : La commande `connect` offre 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 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>\.

Le système géré comprend jusqu'à six modules d'E/S.

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

```
connect switch-n
```

où `n` est un libellé de module d'E/S A1, A2, B1, B2, C1 et C2.

(Voir la figure 13-1 pour l'illustration du placement des modules d'E/S dans le châssis.) Lorsque vous référencez les modules d'E/S dans la commande connect, ils sont adressés sur des commutateurs, comme le montre le tableau suivant.

Tableau 29. : Adressage des modules d'E/S sur des commutateurs

Nom de modules d'E/S	Commutateur
A1	commutateur-a1 ou commutateur-1
A2	commutateur-a2 ou commutateur-2
B1	commutateur-b1 ou commutateur-3
B2	commutateur-b2 ou commutateur-4
C1	commutateur-c1 ou commutateur-5

Nom de modules d'E/S	Commutateur
C2	commutateur-c2 ou commutateur-6

REMARQUE : Il ne peut y avoir qu'une seule connexion de module d'E/S par châssis à la fois.

REMARQUE : Vous ne pouvez pas vous connecter aux fonctions d'intercommunication depuis la console série.

Pour la connexion à la console série d'un serveur géré, utilisez la commande `connect server-nx`, où `n` est un numéro de 1 à 8, et `x` est a,b, c ou d. Vous pouvez également utiliser la commande `racadm connect server-n`. Lors de la connexion à un serveur avec l'option `-b`, le système considère que la communication est binaire et le caractère d'échappement est désactivé. Si l'iDRAC n'est pas disponible, vous voyez apparaître le message d'erreur `Aucune route vers l'hôte`.

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 voir les écrans d'amorçage BIOS, vous devez activer la redirection série dans la configuration du BIOS des serveurs. De plus, vous devez définir la fenêtre de l'émulateur de terminal sur 80x25. Sinon, l'écran est brouillé.

REMARQUE : Certaines touches ne fonctionnent pas dans les écrans de configuration BIOS. Utilisez les séquences d'échappement correctes pour **CTRL+ALT+SUPPR** et les autres séquences. L'écran de redirection initial affiche les séquences d'échappement nécessaires.

Liens connexes

Configuration du BIOS du serveur géré pour la redirection de console série
Configuration de Windows pour la redirection de console série
Configuration de Linux pour la redirection de console série du serveur pendant le démarrage
Configuration de Linux pour la redirection de console série du serveur après l'amorçage

Configuration du BIOS du serveur géré pour la redirection de console série

Il est nécessaire d'établir une connexion au serveur géré avec le module iKVM (voir « Gestion de serveurs avec iKVM ») et d'établir une session de console distante depuis l'interface Web iDRAC7 (voir le manuel « *iDRAC7 User's Guide* » (Guide d'utilisation de l'iDRAC7), à l'adresse **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, série sur LAN), vous devez activer la redirection de console via COM1. Pour modifier le paramètre BIOS :

1. Démarrez le serveur géré.
2. Appuyez sur <F2> pour accéder à l'utilitaire de configuration du BIOS pendant le POST.
3. Faites défiler l'affichage jusqu'à l'entrée **Communications série** et appuyez sur <Entrée>. Dans la boîte de dialogue popup, la liste des communications série affiche les options suivantes :
   - désactivé
   - activé sans redirection de console
   - activé avec redirection de console via COM1

   Utilisez les touches fléchées pour naviguer entre ces options.
4. Assurez-vous qu'**Activé avec redirection de console via COM1** est activé.
5. Activez l'option **Redirection après démarrage** (la valeur par défaut est **Désactivé**). Cette option permet la redirection de console BIOS pour les redémarrages suivants.

6. Enregistrez les modifications et quittez.

   Le serveur 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 du client, définissez la fenêtre ou l'application qui affiche la console redirigée sur 25 lignes x 80 colonnes pour que le texte s'affiche correctement ; sinon, certains écrans de texte risquent d'être illisibles.

Modifiez le fichier **/etc/grub.conf** comme suit :

1. Localisez les sections relatives aux paramètres généraux dans le fichier et ajoutez les deux lignes suivantes :

   ```
   serial --unit=1 --speed=57600 terminal --timeout=10 serial
   ```

2. Ajoutez deux options à la ligne du noyau :

   ```
   noyau de la console=ttyS1,57600
   ```

3. Si le fichier **/etc/grub.conf** contient une instruction `splashimage`, mettez-la en commentaire pour l'exclure.

   L'exemple suivant illustre les modifications décrites dans cette procédure.

   ```
   # grub.conf generated by anaconda # # Notez qu'il est inutile d'exécuter de
   nouveau grub après modification # de ce fichier. # REMARQUE : vous n'avez
   pas de partition /boot. Ceci signifie que tous # les chemins kernel et
   initrd sont relatifs par rapport à /, ex. : # root (hd0,0) # kernel /boot/
   vmlinuz-version ro root= /dev/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/sda1 hda=ide-scsi console=ttyS0
   console=ttyS1,57600 initrd /boot/initrd-2.4.9-e.3smp.img title Red Hat
   Linux Advanced Server-up (2.4.9-e.3) root (hd0,00) kernel /boot/
   vmlinuz-2.4.9-e.3 ro root=/dev/sda1 initrd /boot/initrd-2.4.9-e.3.img
   ```

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

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

     ```
     console=ttyS1,57600
     ```

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

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

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

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

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

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

```
# # inittab Ce fichier explique comment le processus INIT # doit configurer le
système pour un certain # niveau d'exécution. # # Auteur : Miquel van
Smoorenburg # Modifié pour RHS Linux par Marc Ewing et # Donnie Barnes # #
Niveau d'exécution par défaut. Les niveaux d'exécution utilisés par RHS sont :
# 0 - halt (Ne PAS définir initdefault sur ce niveau) # 1 - Mode utilisateur
unique # 2 - Multi-utilisateur, sans NFS (Identique à 3, si vous # n'avez pas
de mise en réseau) # 3 - Mode multi-utilisateur complet # 4 - Non utilisé # 5 -
X11 # 6 - Redémarrage (Ne PAS définir initdefault sur ce niveau) # id:
3:initdefault: # Initialisation du système. si::sysinit:/etc/rc.d/rc.sysinit
l0:0:wait:/etc/rc.d/rc 0 l1:1:wait:/etc/rc.d/rc 1 l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3 l4:4:wait:/etc/rc.d/rc 4 l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6 # Éléments à exécuter à chaque niveau d'exécution.
ud::once:/sbin/update # Interruption CTRL-ALT-SUPPR ca::ctrlaltdel:/sbin/
shutdown -t3 -r now # Lorsque l'onduleur indique une panne de courant, nous
supposons qu'il reste # quelques minutes d'alimentation. Planifiez un arrêt
dans 2 minutes à partir de maintenant. # Bien entendu, on considère ici que
l'alimentation est installée, # et que l'onduleur est connecté et fonctionne
correctement. pf::powerfail:/sbin/shutdown -f -h +2 "Panne de courant ; arrêt
du système" # Si vous avez rétabli l'alimentation avant l'arrêt, annulez cet
arrêt. pr:12345:powerokwait:/sbin/shutdown -c "Alimentation restaurée ; arrêt
annulé" # Exécutez gettys avec les niveaux d'exécution standard co:
2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi 1:2345:respawn:/sbin/mingetty
tty1 2:2345:respawn:/sbin/mingetty tty2 3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4 5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6 # Exécutez xdm pour le niveau d'exécution 5
# xdm est désormais un service séparé x:5:respawn:/etc/X11/prefdm -nodaemon
```

Modifiez le fichier **/etc/securetty** comme suit :

Ajoutez une nouvelle ligne avec le nom du tty série de COM2 :

```
ttyS1
```

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

```
vc/1 vc/2 vc/3 vc/4 vc/5 vc/6 vc/7 vc/8 vc/9 vc/10 vc/11 tty1 tty2 tty3 tty4
tty5 tty6 tty7 tty8 tty9 tty10 tty11 ttyS1
```

12

Utilisation de cartes FlexAddress et FlexAdress Plus

Cette section fournit des informations sur les cartes FlexAddress et FlexAddress Plus, ainsi que sur la façon de les configurer et de les utiliser.

Liens connexes

À propos de FlexAddress
À propos de FlexAddress Plus
Comparaison entre FlexAddress et FlexAddress Plus

À propos de FlexAddress

La fonctionnalité FlexAddress est une mise à niveau facultative qui permet aux modules serveurs de remplacer les ID réseau World Wide Name et Media Access Control (WWN/MAC) d'usine par des ID WWN/MAC fournis par le châssis.

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. Avant FlexAddress, si vous aviez besoin de remplacer un module de serveur par un autre, l'ID WWN/MAC changeait, et vous deviez reconfigurer les outils Ethernet de gestion réseau et les ressources SAN afin d'identifier le nouveau module de serveur.

La fonction FlexAddress permet au module 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 réseau, ni les ressources SAN pour les adapter au nouveau module de 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.

La carte de fonction FlexAddress contient une plage d'adresses MAC. Avant d'installer FlexAddress, vous pouvez déterminer la plage d'adresses MAC figurant sur la carte de fonction FlexAddress en insérant la carte SD dans un lecteur de cartes mémoire USB et en affichant le fichier **pwwn_mac.xml**. Ce fichier XML en texte clair, stocké sur la carte SD contient la balise XML *mac_start*, qui indique la première adresse MAC hexadécimale utilisée pour cette plage d'adresses MAC uniques. La balise *mac_count* indique le nombre total d'adresses MAC allouées par la carte SD. La plage totale d'adresses MAC allouée peut être déterminée par :

```
<mac_start> + 0xCF (208 - 1) = mac_end
```

où 208 est la valeur *mac_count* et où la formule est la suivante :

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

Par exemple :

```
(starting_mac)00188BFFDCFA + 0xCF = (ending_mac)00188BFFDDC9
```

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.

À propos de FlexAddress Plus

FlexAddress Plus est une nouvelle fonction, nouveauté de la carte de fonction version 2.0. Il s'agit d'une mise à niveau de la carte de fonction FlexAddress version 1.0. FlexAddress Plus contient davantage d'adresses MAC que FlexAddress. Les deux fonctions permettent au châssis d'attribuer des adresses WWN/MAC (World Wide Name/Media Access Control - Nom universel/contrôle de l'accès aux supports) aux périphériques Fibre Channel et Ethernet. Les adresses WWN/MAC attribuées par le châssis sont uniques au niveau global et propres à un logement de serveur.

Comparaison entre FlexAddress et FlexAddress Plus

FlexAddress a 208 adresses réparties dans 16 logements de serveur, chacun étant alloué à 13 MAC.

FlexAddress Plus comporte 2 928 adresses réparties sur 16 logements de serveur, chacun recevant 183 adresses MAC.

Le tableau ci-dessous indique la quantité d'adresses MAC des deux fonctions.

	Structure A	Structure B	Structure C	Gestion iDRAC	Nbre total de MAC
Flexaddress	4	4	4	1	13
FlexAddress Plus	60	60	60	3	183

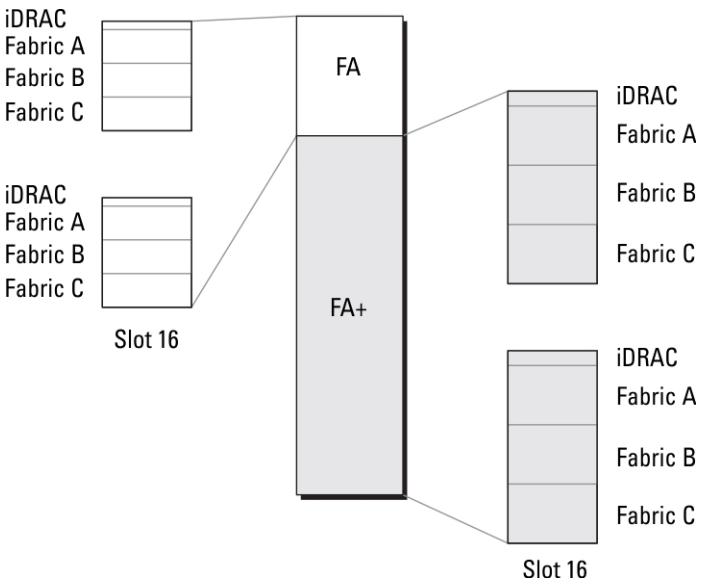


Figure 3. Fonctionnalité FlexAdress (FA) comparée à la fonctionnalité FlexPlusAddress (FA+)

Activation de FlexAddress

FlexAddress est fourni sur une carte Secure Digital (SD) que vous devez insérer dans le CMC pour activer la fonction. Pour activer la fonction FlexAddress, vous pouvez être contraint d'effectuer des mises à jour des logiciels, qui sont inutiles si vous n'utilisez pas FlexAddress. Il s'agit notamment (voir liste dans le tableau suivant) de mettre à jour le BIOS des modules serveur, le BIOS ou le micrologiciel de la carte mezzanine d'E/S et le micrologiciel CMC. Vous devez appliquer ces mises à jour avant d'activer FlexAddress. Si vous ne le faites pas, FlexAddress ne fonctionne pas comme prévu.

Composant	Version minimale requise
Carte mezzanine Ethernet : Broadcom M5708t, 5709, 5710	• Micrologiciel du code de démarrage 4.4.1 ou ultérieur • Micrologiciel de démarrage iSCSI 2.7.11 ou ultérieur • Micrologiciel PXE 4.4.3 ou ultérieur
Carte mezzanine FC : QLogic QME2472, FC8	BIOS 2.04 ou ultérieur
Carte mezzanine FC : Emulex LPe1105-M4, FC8	BIOS 3.03a3 et micrologiciel 2.72A2 ou ultérieur
BIOS du module serveur	• PowerEdge M600 – BIOS 2.02 ou version ultérieure • PowerEdge M605 – BIOS 2.03 ou version ultérieure • PowerEdge M805 • PowerEdge M905 • PowerEdge M610 • PowerEdge M710 • PowerEdge M710hd
LAN sur carte mère (LOM) de PowerEdge M600/M605	• Micrologiciel du code de démarrage 4.4.1 ou ultérieur • Micrologiciel de démarrage iSCSI 2.7.11 ou ultérieur
iDRAC	• Version 1.50 ou supérieure pour les systèmes PowerEdge xx0x • Version 2.10 ou supérieure pour les systèmes PowerEdge xx1x
CMC	Version 1.10 ou ultérieure

REMARQUE : Tout système commandé après le mois de juin 2008 intègre les versions de micrologiciel adéquates.

Pour assurer le déploiement correct de la fonction FlexAddress, mettez à jour le BIOS et le micrologiciel dans l'ordre suivant :

1. Mettez à jour le BIOS et tout le micrologiciel de la carte mezzanine.
2. Mettez à jour le BIOS du module serveur.
3. Mettez à jour le micrologiciel iDRAC sur le module de serveur.
4. Mettez à jour tout le micrologiciel CMC dans le châssis ; s'il y a des contrôleurs CMC redondants, assurez-vous que les deux soient mis à jour.
5. Insérez la carte SD dans le module passif pour un système à contrôleur CMC redondant ou dans le contrôleur CMC unique pour un système non redondant.

   REMARQUE : La fonctionnalité n'est pas activée si le micrologiciel CMC qui prend en charge FlexAddress (version 1.10 ou ultérieure) n'est pas installé.

   Voir le document *Spécifications techniques de la carte Secure Digital (SD) de Chassis Management Controller (CMC)* pour installer la carte SD.

   REMARQUE : La carte SD contient la fonction FlexAddress. Les données stockées sur la carte SD 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 empêcher le système de fonctionner correctement.

   REMARQUE : Vous ne pouvez utiliser la carte SD que dans un seul châssis. Si vous disposez de plusieurs châssis, vous devez acheter des cartes SD supplémentaires.

La fonction FlexAddress est activée automatiquement au redémarrage du CMC si vous avez inséré la carte SD de fonction ; cette activation provoque la liaison de la fonction au châssis actuel. Si vous avez installé la carte SD sur le CMC redondant, l'activation de la fonction FlexAddress se produit uniquement lorsque le CMC de secours devient actif. Pour plus d'informations sur la façon de rendre actif le CMC redondant, voir le document « *Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification* » (Spécifications techniques de la carte Secure Digital (SD) de Chassis Management Controller (CMC)).

Lorsque le CMC redémarre, vérifiez le processus d'activation. Pour plus d'informations, voir « Vérification de l'activation de FlexAddress ».

Activation de FlexAddress Plus

La fonctionnalité FlexAddress Plus est fournie sur la carte Secure Digital (SD), tout comme la fonctionnalité FlexAddress.

REMARQUE : La carte SD étiquetée FlexAddress contient uniquement FlexAddress, et la carte FlexAddress Plus contient les deux fonctions FlexAddress et FlexAddress Plus. La carte doit être insérée dans le module CMC pour que vous puissiez activer la fonction.

Certains serveurs, comme le PowerEdge M710HD, peuvent nécessiter un nombre d'adresses MAC supérieur à ce que FlexAddress peut fournir à CMC, selon leur configuration. Pour ces serveurs, la mise à niveau vers FA+ (FlexAddress Plus) permet une optimisation complète de la configuration WWN/MAC. Contactez Dell pour obtenir un support pour la fonction FlexAddress Plus.

Pour activer la fonction FlexAddress Plus, vous devez mettre à jour les logiciels suivants : BIOS du serveur, iDRAC du serveur et micrologiciel CMC. Si ces mises à jour ne sont pas effectuées, seule la fonction FlexAddress est disponible. Pour plus d'informations sur les versions minimales requises pour ces composants, voir le document « *Lisez-moi* », à l'adresse **dell.com/support/manuals**.

Vérification de l'activation de FlexAddress

Utilisez la commande de l'utilitaire RACADM suivante pour vérifier la carte de fonctionnalité SD et sa condition :

```
racadm featurecard -s
```

Tableau 30. Messages de condition renvoyés par la commande featurecard -s

Message de condition	Actions
Aucune carte de fonction insérée.	Vérifiez le CMC pour vous assurer que la carte SD a été correctement insérée. Dans une configuration avec CMC redondants, vérifiez que la carte de fonction SD a été insérée dans le CMC actif et non dans le CMC de secours.
La carte de fonction insérée est valide et contient la fonctionnalité FlexAddress suivante : la carte de fonction est liée à ce châssis.	Aucune action n'est requise.
La carte de fonction insérée est valide et contient la fonction FlexAddress suivante : la carte de fonction est liée à un autre châssis, numéro de service = ABC1234, numéro de série de la carte SD = 01122334455.	Retirez la carte SD, localisez et installez la carte SD du châssis actuel.
La carte de fonction insérée est valide et contient la fonction FlexAddress suivante : la carte de fonction n'est liée à aucun châssis.	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 `racadm`

Message de condition	Actions
	`racreset` jusqu'à ce que le module CMC dans lequel la carte de fonction est installée devienne actif.

Utilisez la commande RACADM suivante pour afficher toutes les fonctionnalités activées sur le châssis :

```
racadm feature -s
```

La commande renvoie le message de condition suivant :

```
Fonction = FlexAddress Date d'activation = 8 avril 2008 - 10:39:40 Fonction
installée depuis la carte avec le numéro de série = 01122334455
```

Si aucune fonction n'est active sur le châssis, la commande renvoie le message suivant :

```
racadm feature -s Aucune fonction active sur le châssis
```

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 :

```
ERREUR : une ou plusieurs fonctions de la carte SD sont actives sur un autre
châssis.
```

Pour plus d'informations sur les commandes **feature** et **featurecard**, voir le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC).

Désactivation de FlexAddress

La valeur FlexAddress ou la fonction peut être désactivée, et vous pouvez rétablir l'état avant 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 vous 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 CMC et le châssis doit être mis hors tension avant l'exécution de la commande de désactivation.

Si vous exécutez la commande de désactivation alors qu'aucune carte n'est pas installée ou lorsqu'une carte provenant d'un autre châssis est présente, la fonctionnalité est alors 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 :

```
la désactivation de la fonctionnalité FlexAddress sur le châssis a réussi.
```

Si le châssis n'a pas été arrêté avant l'exécution, la commande échoue et renvoie le message d'erreur suivant :

```
ERREUR : impossible de désactiver la fonction car le châssis est SOUS TENSION
```

Pour plus d'informations sur la commande, voir la section traitant de **feature** dans le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de la ligne de commande RACADM d'iDRAC7 et de CMC)).

Affichage des informations FlexAddress

Vous pouvez afficher les informations d'état de l'ensemble du châssis ou d'un serveur particulier. Les informations affichées sont les suivantes :

- Configuration des structures

- État d'activation/inactivation de FlexAddress
- Numéro et nom du logement
- Adresses attribuées par le châssis et le serveur
- Adresses en cours d'utilisation

Liens connexes

Affichage des FlexAddress pour le châssis
Affichage des informations FlexAddress pour tous les serveurs
Affichage des informations FlexAddress pour chaque serveur

Affichage des FlexAddress pour le châssis

Vous pouvez afficher les informations d'état FlexAddress pour l'ensemble du châssis. Ces informations précisent si la fonction est active et fournissent une vue d'ensemble de l'état FlexAddress de chaque serveur.

Pour afficher l'état FlexAddress du châssis avec l'interface Web CMC, accédez à **Présentation du châssis** → **Configuration** → **Généralités**.

La page **Paramètres généraux du châssis** s'affiche.

La fonction **FlexAddress** porte la valeur **Actif** ou **Inactif**. La valeur **Actif** indique que la fonction est installée sur le châssis, et la valeur **Inactif** indique que la fonction n'est ni installée, ni en cours d'utilisation sur le châssis.

Utilisez la commande RACADM suivante pour afficher l'état de FlexAddress sur l'ensemble du châssis :

```
racadm getflexaddr
```

Pour afficher l'état FlexAddress d'un logement particulier :

```
racadm getflexaddr [-i <numéro_logement>]
```

où *<numéro_logement>* est une valeur comprise entre 1 et 16.

Pour plus d'informations sur la commande **getflexaddr**, voir le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC).

Affichage des informations FlexAddress pour tous les serveurs

Pour afficher l'état FlexAddress de tous les serveurs avec l'interface Web CMC, accédez à l'arborescence système, puis cliquez sur **Présentation du serveur** → **Propriétés** → **WWN/MAC**.

La page **Résumé WWN/MAC** s'affiche. Elle indique la configuration WWN et les adresses MAC de tous les logements du châssis.

Configuration de la structure

Structure A, Structure B et Structure C affichent le type de la structure d'entrées/sorties installée. L'iDRAC affiche l'adresse MAC de gestion du serveur.

REMARQUE : Si la structure A est activée, les logements inoccupés affichent les adresses MAC attribuées par le châssis pour la structure A et MAC ou WWN pour les structures B et C s'ils sont utilisés par les logements occupés.

Adresses WWN/MAC

Affiche la configuration FlexAddress de chaque logement du châssis. Les informations affichées sont les suivantes :

- Le contrôleur de gestion d'iDRAC n'est pas une structure, mais son adresse FlexAddress est traitée en tant que telle.
- Numéro et emplacement du logement
- État d'activation/inactivation de FlexAddress
- Type de structure

- Adresses WWN/MAC en cours d'utilisation attribuées par le châssis et attribuées par le serveur

Une coche verte indique le type de l'adresse active, soit attribuée par le serveur, soit attribuée par le châssis.

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

Affichage des informations FlexAddress pour chaque serveur

Pour afficher les informations FlexAddress d'un serveur particulier avec l'interface Web CMC :

1. Dans l'arborescence système, sélectionnez **Présentation du serveur**.
   Tous les serveurs (1 à 16) s'affichent dans la liste **Serveurs** développée.
2. Cliquez sur le serveur à afficher.
   La page **Condition du serveur** s'affiche.
3. Cliquez sur l'onglet **Configuration**, puis sur le sous-onglet **FlexAddress**.
   La page **FlexAddress** s'affiche. Elle contient la configuration WWN et les adresses MAC du serveur sélectionné. Pour plus d'informations, voir l'*aide en ligne CMC*.

Configurer 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 : Dans cette section, le terme FlexAddress désigne également la version FlexAddress Plus.

Vous devez acheter et installer la mise à niveau FlexAddress pour configurer cette fonction. Si vous ne le faites pas, le texte suivant s'affiche dans l'interface Web :

```
« Fonction facultative non installée ». Voir le manuel « Dell Chassis
Management Controller Users Guide » (Guide d'utilisation de Dell Chassis
Management Controller) pour plus d'informations sur la fonction
d'administration des noms WWN et adresses MAC basée sur le châssis. Pour
acheter cette fonction, contactez Dell à l'adresse www.dell.com.
```

Si vous achetez FlexAddress avec votre châssis, la fonction est installée et active lorsque vous allumez votre système. Si vous achetez FlexAddress séparément, vous devez installer la carte de fonction SD en suivant les instructions du document « *Chassis Management Controller (CMC) Secure Digital (SD) Card Technical Specification* » (Spécifications techniques de la carte Secure Digital (SD) de Chassis Management Controller (CMC)), à l'adresse **dell.com/support/manuals**.

Vous devez éteindre le serveur avant de commencer la configuration. Vous pouvez activer ou désactiver FlexAddress séparément pour chaque structure. De plus, vous pouvez l'activer ou le désactiver pour chaque logement. Après avoir activé la fonction pour chaque structure voulue, 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 attribuée par l'usine sur le serveur.

Dans les logements sélectionnés, FlexAddress est activé pour toutes les structures activées. Par exemple, il est impossible d'activer les structures A et B, et d'activer FlexAddress dans le logement 1 de la structure A mais pas dans la structure B.

REMARQUE : Assurez-vous que les serveurs lames sont hors tension avant de changer l'adresse flex de niveau de structure (A, B, C, or DRAC).

Liens connexes

Réveil sur LAN avec FlexAddress

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

Configuration de FlexAddress pour les logements au niveau du serveur

Configuration complémentaire de FlexAddress pour Linux

Réveil sur LAN avec FlexAddress

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 pour chaque structure voulue, puis vous sélectionnez les logements à inclure dans la fonction. Vous devez activer à la fois des structures et des logements pour configurer correctement FlexAddress.

Configuration de FlexAddress pour les structures et logements au niveau du châssis avec l'interface Web CMC

Pour activer ou désactiver des structures et logements pour l'utilisation de la fonction FlexAddress avec l'interface Web CMC :

1. Dans l'arborescence système, accédez à **Présentation du serveur**, puis cliquez sur **Configuration → FlexAddress**.
   La page **Déployer FlexAddress** s'affiche.
2. Dans la section **Sélectionner les structures pour les WWN/MAC attribués par le châssis**, sélectionnez le type de structure pour lequel activer FlexAddress. Pour le désactiver, désélectionnez l'option.

   REMARQUE : Si aucune structure n'est sélectionnée, FlexAddress n'est pas activé pour les logements sélectionnés.

   La page **Sélectionner les logements pour les WWN/MAC attribués par le châssis** s'affiche.
3. Sélectionnez l'option **Activé** pour le logement où activer FlexAddress. Pour le désactiver, désélectionnez l'option.

   REMARQUE : Si un serveur est présent dans le logement, éteignez-le avant d'activer la fonction FlexAddress dans ce logement.

   REMARQUE : Si aucun logement n'est sélectionné, FlexAddress n'est pas activé pour les structures sélectionnées.
4. Cliquez sur **Appliquer** pour enregistrer les modifications.
   Pour plus d'informations, voir l'*Aide en ligne CMC*.

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

Pour activer et désactiver des structures, utilisez la commande RACADM suivante :

```
racadm setflexaddr [-f <nom_structure> <état>
```

où `<nom_structure>` = `A, B, C ou iDRAC`, et `<état>` = `0 ou 1`

(0 = désactivé et 1 = activé).

Pour activer et désactiver des logements, utilisez la commande RACADM suivante :

```
racadm setflexaddr [-i <numéro_logement> <état>
```

où `<numéro_logement>` = 1 à 16 et `<état>` = 0 ou 1

(0 = désactivé et 1 = activé).

Pour plus d'informations sur la commande **setflexaddr**, voir le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC).

Configuration de FlexAddress pour les logements au niveau du serveur

Vous pouvez activer ou désactiver la fonctionnalité FlexAddress pour des logements au niveau du serveur.

Configuration de FlexAddress pour les logements au niveau du serveur avec l'interface Web CMC

Pour activer ou désactiver un seul logement pour l'utilisation de la fonction FlexAddress avec l'interface Web CMC :

1. Dans l'arborescence système, développez l'entrée **Présentation du serveur**.
   Tous les serveurs (1 à 16) s'affichent dans la liste **Serveurs** développée.
2. Cliquez sur le serveur dont vous souhaitez afficher les informations.
   La page **Condition du serveur** s'affiche.
3. Cliquez sur l'onglet **Configuration**, puis sur le sous-onglet **FlexAddress**.
   La page **FlexAddress** s'affiche.
4. Dans le menu déroulant **FlexAddress activé**, sélectionnez **Oui** pour activer FlexAddress ou **Non** pour désactiver FlexAddress.
5. Cliquez sur **Appliquer** pour enregistrer les modifications.
   Pour plus d'informations, voir l'*Aide en ligne CMC*.

Configuration de FlexAddress pour les logements au niveau du serveur avec RACADM

Pour configurer FlexAddress pour les logements au niveau du serveur avec RACADM :

```
racadm setflexaddr [-i <numéro_logement> <état>] [-f <nom_structure> <état>]
```

où, `<numéro_logement>` = 1 à 16

`<nom_structure>` = A, B, C

`<état>` = 0 ou 1

(0 = désactivé et 1 = activé).

Configuration complémentaire de FlexAddress pour Linux

Lorsque vous passez d'un identifiant MAC attribué par le serveur à un identifiant MAC attribué par le châssis sur un système d'exploitation basée sur Linux, il peut être nécessaire d'effectuer une configuration complémentaire :

- SUSE Linux Enterprise Server 9 et 10 : vous devez exécuter YAST (Yet Another Setup Tool - Encore un autre outil de configuration) sur le système Linux pour configurer les périphériques réseau, puis redémarrer les services réseau.
- Red Hat Enterprise Linux 4 et Red Hat Enterprise Linux 5 : exécutez Kudzu, utilitaire servant à détecter et à configurer le matériel nouveau ou modifié sur le système. Kudzu affiche le menu de détection du matériel ; il détecte le changement d'adresse MAC lors du retrait du matériel et de l'ajout du nouveau matériel.

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.

Configuration de la structure

La section **Configuration de la structure** affiche le type d'Entrée/Sortie des structures A, B et C. Une coche verte indique que la structure est activée pour FlexAddress. La fonction FlexAddress sert à déployer les adresses WWN/MAC permanentes de logement et les adresses attribuées par le châssis vers divers logements et structures au sein du châssis. Cette fonction est activée sur une base par structure et par logement.

REMARQUE : Pour plus d'informations sur la fonction FlexAddress, voir CMCNoble_About Flexaddress.

Adresses WWN/MAC

La section **Adresse WWN/MAC** affiche les informations WWN/MAC attribuées à tous les serveurs, même si les logements de ces serveurs sont actuellement vides.

- **Emplacement** indique l'emplacement du logement occupé par les modules d'entrées/sorties (IOM). Les six logements sont identifiés par la combinaison du nom de groupe (A, B ou C) et du numéro de logement (1 ou 2) ; ici, les noms de logements sont A1, A2, B1, B2, C1 ou C2. iDRAC est le contrôleur de gestion intégré du serveur.
- **Structure** affiche le type de structure d'E/S.
- **Attribué par le serveur** affiche les adresses WWN/MAC attribuées par le serveur et incorporées au matériel du contrôleur.
- **Attribué par le châssis** affiche les adresses WWN/MAC attribuées par le châssis au logement spécifique concerné.

Une coche verte dans les colonnes **Attribué par le serveur** ou **Attribué par le châssis** indique le type des adresses actives. Les adresses attribuées par le châssis sont définies lors de l'activation de FlexAddress dans le châssis et représentent les adresses persistantes des logements. Lorsque vous cochez la case Attribué par le châssis, ces adresses sont utilisées même si un serveur est remplacé par un autre.

Messages des commandes

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

Tableau 31. Commandes et sortie FlexAddress

Problème	Commande	Sortie
La carte SD du contrôleur CMC actif est liée à un autre numéro de service.	`$racadm featurecard -s`	`La carte de fonction insérée est valide et contient la ou les fonction(s) suivante(s)` `FlexAddress : la carte de fonction est liée à un autre châssis, svctag = <Numéro de service>, Numéro de série de la carte SD =<Numéro de série FlexAddress valide>`
La carte SD du contrôleur CMC actif est liée au même numéro de service.	`$racadm featurecard -s`	`La carte de fonction insérée est valide et contient la ou les fonction(s) suivante(s)` `FlexAddress : la carte de fonction est liée à ce châssis`
La carte SD du contrôleur CMC actif n'est liée à aucun numéro de service.	`$racadm featurecard -s`	`La carte de fonction insérée est valide et contient la ou les fonction(s) suivante(s)` `FlexAddress : la carte de fonction n'est liée à aucun châssis`
La fonctionnalité FlexAddress n'est pas active sur le châssis pour une raison inconnue (Pas de carte SD insérée/carte SD corrompue/ fonctionnalité désactivée/carte SD liée à un autre châssis)	`$racadm setflexaddr [-f <nom_structure> <état_logement>]` `$racadm setflexaddr [-i <numéro_logement> <état_logement>]`	`ERREUR : la fonctionnalité Flexaddress n'est pas active sur le châssis`
L'utilisateur invité tente de définir FlexAddress sur des logements/des structures.	`$racadm setflexaddr [-f <nom_structure> <état_logement>]` `$racadm setflexaddr [-i <numéro_logement> <état_logement>]`	`ERREUR : privilèges utilisateur insuffisants pour effectuer cette opération`
Désactivation de la fonctionnalité FlexAddress alors que le châssis est sous tension	`$racadm feature -d -c flexaddress`	`ERREUR : impossible de désactiver la fonction car le châssis est SOUS TENSION`
L'utilisateur invité essaie de désactiver la fonctionnalité sur le châssis	`$racadm feature -d -c flexaddress`	`ERREUR : privilèges utilisateur insuffisants pour effectuer cette opération`
Modification des paramètres FlexAddress de logement/structure pendant que les modules de serveur sont sous tension.	`$racadm setflexaddr -i 1 1`	`ERREUR : impossible d'exécuter l'opération demandée car elle affecte le serveur SOUS TENSION`

CONTRAT DE LICENCE DES LOGICIELS DELL FlexAddress

Ceci est un contrat légal entre vous, l'utilisateur et Dell Products L.P. ou Dell Global B.V. (« Dell »). Cet accord couvre tous les logiciels distribués avec le produit Dell et pour lesquels il n'existe aucun contrat de licence distinct entre vous et le fabricant ou propriétaire des logiciels en question (collectivement « le logiciel »). Ce contrat ne peut donner lieu à la vente du logiciel et de toute autre propriété intellectuelle. Tous les titres et droits de propriété intellectuelle concernant le logiciel sont la propriété du fabricant ou propriétaire du logiciel. Tous les droits non expressément octroyés dans le cadre du présent contrat sont réservés au fabricant ou propriétaire du logiciel. En ouvrant le ou les emballages du logiciel, ou en brisant leur sceau de sécurité, en installant ou en téléchargeant le logiciel, ou en utilisant le logiciel préchargé ou intégré dans votre produit, vous acceptez d'être lié par les conditions du présent contrat. Si vous n'acceptez pas ces conditions, renvoyez immédiatement tous les éléments du logiciel (disques, documentation écrite et emballages), et supprimez tout le logiciel préchargé ou intégré.

Vous êtes autorisé à utiliser une seule copie du logiciel, sur un seul ordinateur à la fois. Si vous avez plusieurs licences pour le logiciel, vous pouvez utiliser simultanément autant de copies de vous avez de licences. Le terme « utiliser » désigne ici le chargement du logiciel dans la mémoire temporaire ou dans le stockage permanent de l'ordinateur. L'installation sur un serveur réseau uniquement en vue de la distribution vers d'autres ordinateurs n'est pas considérée comme une « utilisation », mais cela s'applique uniquement si vous disposez d'une licence séparée pour chacun des ordinateurs vers lesquels vous distribuez le logiciel. Vous devez vous assurer que le nombre de personnes qui utilisent le logiciel installé sur un serveur réseau ne dépasse pas celui des licences que vous possédez. Si le nombre des utilisateurs du logiciel installé sur un serveur réseau dépasse le nombre des licences, vous devez acheter des licences supplémentaires afin que le nombre des licences soit égal à celui des utilisateurs, avant d'autoriser des utilisateurs supplémentaires à utiliser le logiciel. Si vous êtes un client commercial de Dell ou une filiale Dell, vous autorisez par la présente Dell ou tout agent choisi par Dell, à effectuer un audit de votre utilisation du logiciel au cours des heures de bureau normales, vous acceptez de coopérer avec Dell pour cet audit et vous acceptez de fournir à Dell, dans les limites du raisonnable, tous les dossiers liés à votre utilisation du logiciel. L'audit se limite à la vérification de votre conformité aux conditions du présent contrat.

Le logiciel est protégé par les lois des États-Unis et les divers traités internationaux relatifs aux droits d'auteur. Vous pouvez créer une seule copie du logiciel, uniquement à des fins de sauvegarde ou d'archivage, ou le transférer vers un seul disque dur, à condition de conserver l'original uniquement pour la sauvegarde ou l'archivage. Vous ne pouvez pas louer le logiciel ni le céder en crédit-bail, ni copier les documents papier qui accompagnent le logiciel, mais vous pouvez transférer définitivement le logiciel et toute la documentation qui l'accompagne dans le cadre d'une vente ou d'un transfert du produit Dell, si vous n'en conservez aucune copie et si le destinataire accepte les conditions du présent contrat. Tout transfert doit inclure la mise à jour la plus récente et toutes les versions précédentes. Il est interdit d'effectuer l'ingénierie inverse du logiciel, de le décompiler ou de le désassembler. Si l'emballage accompagnant votre ordinateur contient des CD, ou des disques 3,5 pouces et/ou 5,25 pouces, vous ne pouvez utiliser que les disques conçus pour votre ordinateur. Vous n'avez pas le droit d'utiliser ces disques sur un autre ordinateur ou réseau, ni de les prêter, les louer, les céder en crédit-bail ou les transférer vers un autre utilisateur, sauf condition expresse du présent contrat.

GARANTIE LIMITÉE

Dell garantit que les disques du logiciel sont exempts de défaut matériel et de fabrication pour une utilisation normale pendant quatre-vingt-dix (90) jours à compter de la date où vous les recevez. Cette garantie s'applique uniquement à vous-même et n'est pas transférable. Toutes les garanties implicites sont limitées à quatre-vingt-dix (90) jours à compter de la date de réception du logiciel. Certaines juridictions n'autorisent aucune limite de durée d'une garantie implicite, si bien que cette limitation peut ne pas s'appliquer à vous. L'entière responsabilité de Dell et de ses fournisseurs, et votre seul recours, correspond (a) au remboursement du prix payé pour le logiciel ou (b) au remplacement de tout disque non conforme aux termes de la garantie, renvoyé à Dell avec un numéro d'autorisation de retour, à vos propres coûts et risques. Cette garantie limitée est nulle et non avenue si les dommages des disques résultent d'un accident, d'un abus, d'une utilisation incorrecte, d'un entretien ou d'une modification par une personne autre que Dell. Les disques de remplacement sont garantis pour la durée restante de la garantie d'origine ou pour trente (30) jours. La durée la plus longue sera appliquée.

Dell ne garantit PAS que les fonctions du logiciel répondront à vos besoins, ni que le fonctionnement du logiciel sera ininterrompu ou exempt d'erreur. Vous assumez l'entière responsabilité du choix de ce logiciel pour obtenir les résultats recherchés, ainsi que de l'utilisation et des résultats du logiciel.

DELL, EN SON PROPRE NOM ET EN CELUI DE SES FOURNISSEURS, REJETTE TOUTE AUTRE GARANTIE, EXPRESSE OU IMPLICITE, Y COMPRIS MAIS SANS S'Y LIMITER, LES GARANTIES IMPLICITES DE VALEUR MARCHANDE ET D'ADÉQUATION À UNE UTILISATION PARTICULIÈRE, POUR LE LOGICIEL ET TOUTE LA DOCUMENTATION ÉCRITE QUI L'ACCOMPAGNE. Cette garantie limitée vous donne des droits légaux spécifiques ; vous pouvez avoir d'autres droits, qui varient d'une juridiction à l'autre.

DELL OU SES FOURNISSEURS NE SAURAIENT EN AUCUN CAS ÊTRE TENUS POUR RESPONSABLE DES ÉVENTUELS DOMMAGES (Y COMPRIS, SANS S'Y LIMITER, LES DOMMAGES DE TYPE PERTE DE PROFIT, INTERRUPTION DES ACTIVITÉS, PERTE D'INFORMATIONS COMMERCIALES OU AUTRE PERTE FINANCIÈRE) DÉCOULANT DE L'UTILISATION OU DE L'IMPOSSIBILITÉ D'UTILISER LE LOGICIEL, MÊME S'ILS ONT ÉTÉ AVERTIS DE L'ÉVENTUALITÉ DE TELS DOMMAGES. Comme certaines juridictions n'autorisent pas l'exclusion ou la limitation de responsabilité pour les dommages induits ou accidentels, la limitation ci-dessus ne s'applique pas forcément à votre cas.

LOGICIEL LIBRE (Open Source)

Une partie de ce CD peut contenir des logiciels libres, que vous pouvez utiliser conformément aux termes et conditions des licences spécifiques sous lesquelles ils ont été distribués.

CE LOGICIEL OPEN SOURCE EST DISTRIBUÉ DANS L'ESPOIR QU'IL VOUS SERA UTILE, MAIS IL EST FOURNI « EN L'ÉTAT », SANS AUCUNE GARANTIE EXPRESSE OU IMPLICITE, Y COMPRIS MAIS SANS S'Y LIMITER LES GARANTIES IMPLICITES DE VALEUR MARCHANDE OU D'ADÉQUATION À UNE UTILISATION PARTICULIÈRE. DELL, LES DÉTENTEURS DES DROITS DE COPYRIGHT OU LES CONTRIBUTEURS DU LOGICIEL NE SAURAIENT EN AUCUN CAS ÊTRE TENUS POUR RESPONSABLES DES ÉVENTUELLES DOMMAGES DIRECTS, INDIRECTS, CONSÉCUTIFS, SPÉCIAUX, EXEMPLAIRES OU INDUITS (Y COMPRIS MAIS SANS S'Y LIMITER LA FOURNITURE DE BIENS OU SERVICES DE SUBSTITUTION, LA PERTE D'UTILISATION, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉS), QUELLE QU'EN SOIT LA CAUSE, NI DES ÉVENTUELLES PLAINTES, PAR ACTION OU CONTRAT, DÉLIT OU AUTRE (Y COMPRIS LA NÉGLIGENCE OU AUTRES CAUSES) DÉCOULANT DE QUELQUE MANIÈRE QUE CE SOIT DE L'UTILISATION DE CE LOGICIEL, MÊME S'ILS ONT ÉTÉ AVERTIS DE L'ÉVENTUALITÉ DE TELS DOMMAGES.

DROITS RESTREINTS DU GOUVERNEMENT DES ÉTATS-UNIS

Le logiciel et sa documentation sont des « articles commerciaux », conformément à la définition de ce terme dans le document 48 C.F.R. 2.101, comprenant d'une part un « logiciel informatique commercial » et d'autre part une « documentation de logiciel informatique commercial », conformément à la définition de ces termes dans le document 48 C.F.R. 12.212. Selon les termes des documents 48 C.F.R. 12.212 et 48 C.F.R. 227.7202-1 à 227.7202-4, tous les utilisateurs finaux appartenant au Gouvernement des États-Unis acquièrent le logiciel et sa documentation avec uniquement les droits décrits dans le présent document.

Fournisseur/Éditeur du logiciel: Dell Products, L.P., One Dell Way, Round Rock, Texas 78682.

CONSIGNES GÉNÉRALES

Cette licence reste en vigueur jusqu'à son expiration. Elle expire selon les conditions décrites ci-dessus, ou si vous ne respectez pas certaines des conditions du présent contrat. À l'expiration de la licence, vous acceptez de détruire le logiciel et les documents associés, ainsi que toutes les copies existantes. Ce contrat est régi par les lois de l'État du Texas. Chaque disposition de ce contrat est dissociable. Si une disposition n'est pas applicable, cela n'affecte en aucune manière l'applicabilité des autres dispositions, termes ou conditions du contrat. Ce contrat lie vos successeurs et délégués. Dell accepte et vous acceptez de renoncer dans les limites maximales autorisées par la loi, à tout droit de procédure juridique concernant le logiciel ou le présent contrat. Comme cette renonciation n'est pas valide dans certaines juridictions, cette clause peut ne pas s'appliquer à votre cas. Vous reconnaissez que vous avez lu le présent contrat, que vous le comprenez, que vous acceptez d'être lié par ses conditions, et qu'il s'agit de l'expression complète et exclusive de l'accord conclu entre vous et Dell concernant le logiciel.

13

Gestion de la structure d'E/S

Le châssis peut contenir jusqu'à six modules d'E/S (IOM), chacun jouant le rôle d'un module d'intercommunication ou de commutateur. Les IOM sont répartis en trois groupes (A, B et C) comportant chacun deux logements (1 et 2).

Les logements sont désignés par des lettres, de gauche à droite, en suivant l'arrière du châssis : A1 | B1 | C1 | C2 | B2 | A2. Chaque serveur comporte des logements pour deux cartes Mezzanine (MC) qui se connectent aux IOM. La carte MC et l'IOM correspondant doivent avoir la même structure.

Les E/S de châssis sont réparties entre trois chemins de données discrets : A, B et C. Ces chemins sont appelés STRUCTURES, et prennent en charge Ethernet, Fibre Channel ou InfiniBand. Ces chemins de structure discrets sont divisés en deux banques d'E/S, 1 et 2. Chaque adaptateur d'E/S de serveur (carte Mezzanine ou LOM) peut comporter deux ou quatre ports, en fonction de leurs fonctionnalités. Ces ports sont répartis de façon égale entre les banques IOM 1 et 2 pour établir la redondance. Lorsque vous déployez des réseaux Ethernet, iSCSI ou FibreChannel, répartissez leurs liaisons redondantes entre les deux banques, pour une disponibilité maximale. Le module IOM discret est identifié par l'ID de structure et le numéro de banque.

Exemple : A1 désigne la structure A de la banque 1. C2 indique la structure C de la banque 2.

Le châssis prend en charge trois types de structure ou de protocole. Les modules IOM et cartes Mezzanine d'un groupe doivent avoir le même type de structure ou un type compatible.

- Les modules d'E/S du groupe A sont toujours connectés aux adaptateurs Ethernet intégrés des serveurs ; le type de structure du groupe A sera donc toujours Ethernet.
- Dans le groupe B, les logements IOM sont connectés en permanence au premier logement de carte Mezzanine de chaque module de serveur.
- Dans le groupe C, les logements IOM sont connectés en permanence à la deuxième carte Mezzanine de chaque module de serveur.

REMARQUE : Dans l'interface de ligne de commande (CLI) CMC, les modules d'E/S (IOM) sont désignés par la convention « commutateur-n » : A1=commutateur-1, A2=commutateur-2, B1=commutateur-3, B2=commutateur-4, C1=commutateur-5 et C2=commutateur-6.

Liens connexes

Présentation de la gestion des structures
Configurations non valides
Scénario de nouveau démarrage
Surveillance de l'intégrité des modules d'E/S (IOM)
Configuration des paramètres réseau pour les modules IOM
Gestion des VLAN pour les modules IOM
Gestion des opérations de contrôle de l'alimentation pour les modules IOM
Activation ou désactivation du clignotement des LED des IOM
Restauration des paramètres IOM par défaut définis en usine

Présentation de la gestion des structures

La gestion des structures permet d'éviter les problèmes d'alimentation électrique, de configuration ou de connectivité provoqués par l'installation d'un module IOM ou MC dont le type de structure est incompatible avec celui du châssis.

Les configurations matérielles non valides peuvent provoquer des problèmes électriques ou fonctionnels dans le châssis ou ses composants. La gestion des structures empêche l'allumage de configurations non valides.

La figure suivante affiche l'emplacement des modules d'E/S (IOM) du châssis. L'emplacement de chaque IOM est désigné par son code de groupe (A, B ou C). Ces chemins de structure discrets sont divisés en deux banques d'E/S, 1 et 2. Dans le châssis, les noms de logement IOM sont marqués A1, A2, B1, B2, C1 et C2.

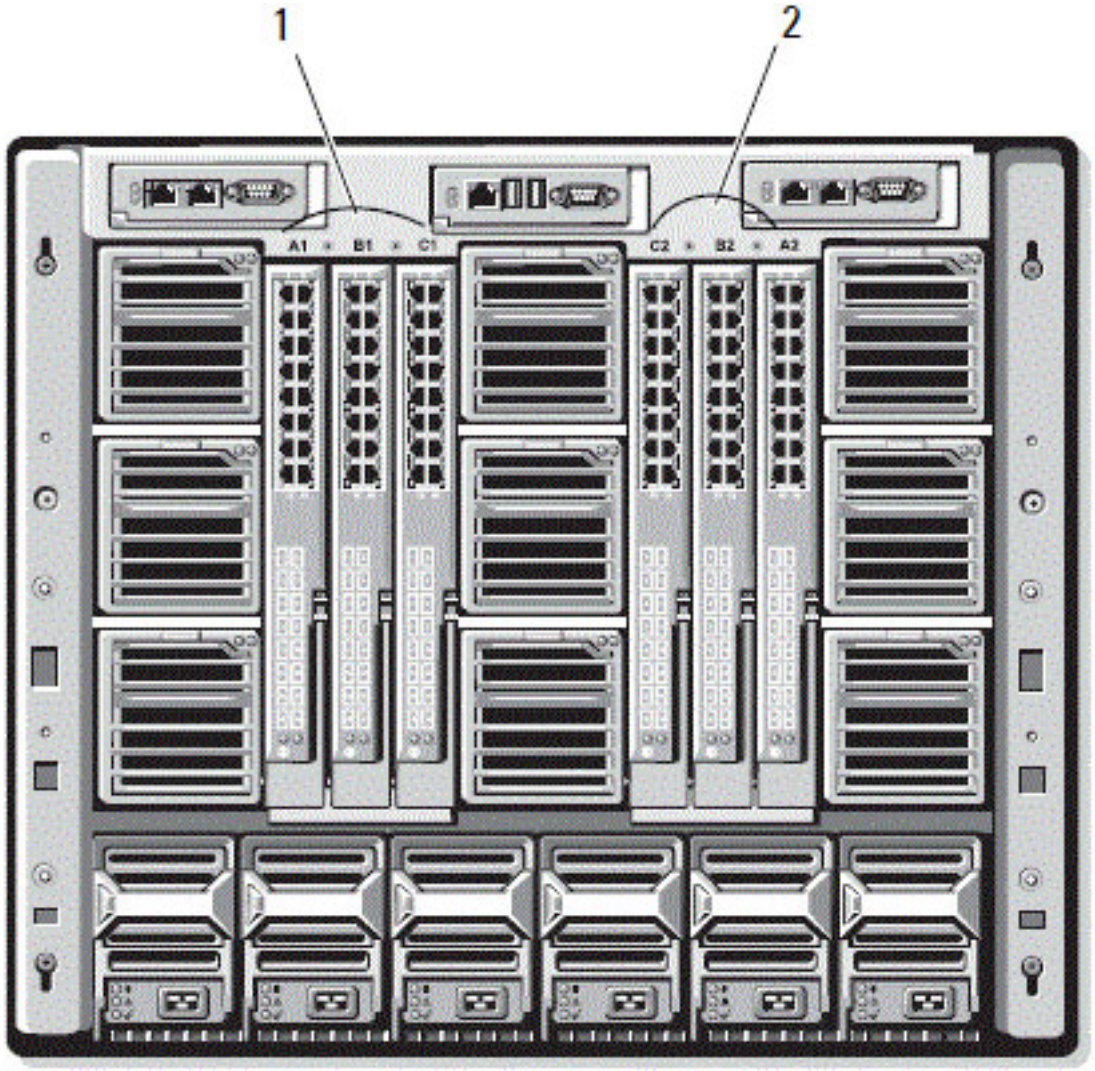


Figure 4. Vue de dos d'un châssis, montrant l'emplacement des modules d'E/S

1	Banque 1 (Logements A1, B1, C1)	2	Banque 2 (Logements A2, B2, C2)

CMC crée à la fois des entrées dans le journal du matériel et dans le journal CMC pour les configurations matérielles non valides.

Par exemple :

- Un module MC Ethernet connecté à un IOM Fibre Channel n'est pas une configuration valide. Toutefois, un MC Ethernet connecté à la fois à un commutateur Ethernet et à un IOM d'intercommunication Ethernet installé dans le même groupe IOM est une configuration valide.
- L'installation d'un module d'E/S (IOM) d'intercommunication Fibre Channel et d'un IOM de commutateur Fibre Channel dans les logements B1 et B2 constitue une configuration valide si le premier MC de chacun des

serveurs est également de type Fibre Channel. Dans ce cas, CMC allume les IOM et les serveurs. Toutefois, certains logiciels de redondance Fibre Channel risquent de ne pas prendre en charge cette configuration ; toutes les configurations valides ne sont pas forcément des configurations prises en charge.

La vérification de structure des modules IOM et MC des serveurs est réalisée uniquement lorsque le châssis est allumé. Lorsque le châssis est en attente d'alimentation, les iDRAC des modules de serveur restent éteints et ne peuvent donc pas signaler le type de structure des MC du serveur. Le type de structure MC ne peut être signalé dans l'interface utilisateur CMC qu'une fois l'iDRAC du serveur allumé. De plus, si le châssis est allumé, la vérification de structure est effectuée lorsque vous insérez un module de serveur ou un module IOM (facultatif). Si une non-correspondance de structures est détectée, le serveur ou l'IOM est autorisé à s'allumer, et la LED d'état clignote en orange.

Configurations non valides

Il existe trois types de configurations non valides :

- Configuration MC ou LOM non valide : le type de structure d'un serveur nouvellement installé est différent de la structure IOM existante. Autrement dit, le LOM ou le MC d'un seul serveur n'est pas pris en charge par le module IOM correspondant. Dans ce cas, tous les autres serveurs du châssis sont en cours d'exécution, mais le serveur avec la carte MC non correspondante ne peut pas être allumé. L'interrupteur du serveur clignote en orange pour vous signaler la non-correspondance de structure.
- Configuration IOM-MC non valide : le type de structure d'un module d'E/S (IOM) nouvellement installé et les types de structure des modules MC résidents ne correspondent pas, ou sont incompatibles. Le module IOM non correspondant est maintenu à l'état Éteint. Le CMC ajoute une entrée dans le journal du CMC et le journal du matériel pour signaler la configuration non valide, en spécifiant le nom de l'IOM. CMC provoque le clignotement de la LED d'erreur du module IOM non conforme. Si vous avez configuré CMC pour envoyer des alertes, il envoie des alertes par e-mail et/ou SNMP pour cet événement.
- Configuration IOM-IOM non valide : un module d'E/S (IOM) nouvellement installé possède un type de structure différent ou incompatible, par rapport à un IOM déjà installé dans son groupe. CMC garde éteint le module IOM nouvellement installé, déclenche le clignotement de la LED d'erreur de l'IOM, et journalise la non-correspondance dans les journaux du CMC et du matériel.

Scénario de nouveau démarrage

Une fois le châssis branché et allumé, les modules d'E/S (IOM) sont prioritaires sur les serveurs. Le premier IOM de chaque groupe est autorisé à s'allumer avant les autres. À ce stade, aucune vérification du type de structure n'est réalisée. Si n'y a aucun IOM dans le premier logement d'un groupe, le module installé dans le deuxième logement de ce groupe s'allume. Si les deux logements contiennent des modules IOM, le module du deuxième logement est comparé au premier pour vérifier la cohérence.

Après démarrage des modules d'E/S, les serveurs démarrent et CMC vérifie la cohérence de la structure des serveurs.

Vous pouvez placer un module d'intercommunication et un commutateur dans le même groupe si leur structure est identique. Cette coexistence de commutateurs et modules d'intercommunication dans un même groupe est possible même s'ils sont fabriqués par des fournisseurs différents.

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

Pour plus d'informations sur la surveillance de l'intégrité des modules IOM, voir « Affichage des informations et de la condition d'intégrité de tous les modules IOM » et « Affichage des informations et de la condition d'intégrité de chaque module IOM ».

Configuration des paramètres réseau pour les modules 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 configurer les paramètres réseau des modules IOM, vérifiez que ces modules sont allumés.

Pour configurer les paramètres réseau, vous devez disposer des privilèges suivants :

- Privilèges Administrateur sur la structure A pour configurer les IOM du groupe A.
- Privilèges Administrateur sur la structure B pour configurer les IOM du groupe B.
- Privilèges Administrateur sur la structure C pour configurer les IOM du groupe C.

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

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

Configuration des paramètres réseau pour les IOM avec l'interface Web CMC

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

1. Dans l'arborescence système, accédez à **Présentation du module d'E/S**, puis cliquez sur **Configuration** ou développez l'entrée **Présentation du module d'E/S**, sélectionnez le module d'E/S (IOM) voulu, puis cliquez sur **Configuration**.

   La page **Déployer les modules d'E/S** affiche les modules IOM allumés.
2. Pour les IOM requis, activez DHCP, entrez l'adresse IP, le masque de sous-réseau et l'adresse de passerelle.
3. Pour les IOM gérables, entrez le mot de passe racine, la chaîne de communauté RO SNMP et l'adresse IP du serveur Syslog. Pour plus d'informations sur les champs, voir l'*aide en ligne CMC*.

   REMARQUE : L'adresse IP définir sur les IOM depuis CMC n'est pas enregistrée dans la configuration permanente de démarrage du commutateur. Pour enregistrer définitivement la configuration d'adresse IP, vous devez entrer la commande `connect switch-n` ou la commande RACADM `racadm connect switch -n`, ou utiliser une interface directe avec l'interface utilisateur graphique (GUI) du module IOM pour enregistrer cette adresse dans le fichier de configuration du démarrage.
4. Cliquez sur **Appliquer**.

   Les paramètres réseau sont configurés pour les IOM.

   REMARQUE : Pour les IOM gérables, vous pouvez réinitialiser les VLAN, les propriétés réseau et les ports d'E/S sur les configurations par défaut.

Configuration des paramètres réseau pour les IOM avec RACADM

Pour configurer les paramètres réseau des modules d'E/S (IOM) avec RACADM, définissez la date et l'heure. Voir la section traitant de la commande **deploy** dans le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC).

Vous pouvez définir le nom d'utilisateur, le mot de passe et la chaîne SNMP d'un IOM avec la commande RACADM **deploy** :

```
racadm deploy -m switch-<n> -u root -p <mot de passe>
```

```
racadm deploy -m switch-<n> -u root -p <mot de passe> -v SNMPv2 <chaîne de communauté SNMP> ro
```

```
racadm deploy -a [server|switch] -u root -p <mot de passe>
```

Restauration des paramètres IOM par défaut définis en usine

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

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

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

1. Dans l'arborescence système, accédez à **Présentation du module d'E/S**, puis cliquez sur **Configuration** ou développez l'entrée **Présentation du module d'E/S**, sélectionnez le module d'E/S (IOM) voulu, puis cliquez sur **Configuration**.

   La page **Déployer les modules d'E/S** affiche les modules IOM allumés.
2. Pour les IOM requis, cliquez sur **Réinitialiser**.

   Un message d'avertissement s'affiche.
3. Cliquez sur **OK** pour continuer.

Liens connexes

Présentation de la gestion des structures
Configurations non valides
Scénario de nouveau démarrage
Surveillance de l'intégrité des modules d'E/S (IOM)
Configuration des paramètres réseau pour les modules IOM
Gestion des VLAN pour les modules IOM
Gestion des opérations de contrôle de l'alimentation pour les modules IOM
Activation ou désactivation du clignotement des LED des IOM

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 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 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 **Logiciel et micrologiciel IOM** s'affiche.

   Ou alors, accédez à l'une des pages suivantes :

   - **Présentation du châssis → Mise à jour**
   - **Présentation du châssis → Contrôleur de châssis → Mise à jour**
   - **Présentation du châssis → iKVM → 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 **Logiciel et micrologiciel IOM**, dans la section **Logiciel IOM**, 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 logiciel**.

   Ou alors, pour revenir aux versions antérieures du logiciel, cochez 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 est affichée 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.

   Une fois la restauration ou mise à jour terminée, vous perdez brièvement la connexion au périphérique IOM car il est réinitialisé, et le nouveau micrologiciel apparaît dans la page **Logiciel et micrologiciel IOM**.

Gestion des VLAN pour les modules IOM

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 avec le 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.

Liens connexes

Configuration des paramètres VLAN des IOM avec l'interface Web CMC
Affichage des paramètres VLAN des IOM avec l'interface Web CMC
Affichage des paramètres VLAN actuels des IOM avec l'interface Web CMC
Ajout de VLAN marqués pour les IOM avec l'interface Web CMC
Suppression de VLAN pour les IOM avec l'interface Web CMC
Mise à jour des VLAN non marqués pour les IOM avec l'interface Web CMC
Réinitialisation de VLAN pour les IOM avec l'interface Web CMC

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

REMARQUE : Vous ne pouvez configurer les paramètres VLAN que sur un module d'E/S (IOM) PowerEdge M I/O Aggregator. Les autres IOM, y compris le MXL 10/40 Gbits Ethernet, ne sont pas pris en charge.

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

1. Dans l'arborescence système, accédez à **Présentation du module d'E/S**, puis cliquez sur **Configuration Gestionnaire VLAN**.

   La page Gestionnaire VLAN affiche les modules IOM 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.

   Pour plus d'informations sur les champs, voir l'*aide en ligne CMC*.

3. Dans la section **Spécifier une plage de ports**, sélectionnez la plage de ports de structure à attribuer aux IOM sélectionnés.

   Pour plus d'informations sur les champs, voir l'*aide en ligne CMC*.

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, sous forme de plage ou d'entrées séparées par une virgule. Exemple : 1,5,10,100-200.

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**.

   Pour plus d'informations sur les champs, voir l'*aide en ligne CMC*.

   REMARQUE : La section de 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 stocker 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. Dans l'arborescence système, 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. Dans l'arborescence système, 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.

Ajout de VLAN marqués pour les IOM avec l'interface Web CMC

Pour ajouter des VLAN marqués pour les modules d'E/S (IOM) avec l'interface Web CMC :

1. Dans l'arborescence système, 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.

   Pour plus d'informations sur les champs, voir l'*aide en ligne CMC*.
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 **Ajouter des VLAN marqués** dans la liste déroulante, puis cliquez sur **Appliquer**.

   Les VLAN marqués sont attribués aux IOM sélectionnés.

   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. Dans l'arborescence système, 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 :

1. Dans l'arborescence système, 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.

   Pour plus d'informations sur les champs, voir l'*aide en ligne CMC*.

4. Utilisez les options **Sélectionner/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. Dans l'arborescence système, 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 des opérations de contrôle de l'alimentation pour les modules IOM

Pour plus d'informations sur la définition des opérations de contrôle de l'alimentation pour les modules d'E/S (IOM), voir « Exécution d'opérations de contrôle de l'alimentation sur un module d'E/S ».

Activation ou désactivation du clignotement des LED des IOM

Pour plus d'informations sur l'activation du clignotement des LED pour les modules d'E/S (IOM), voir « Configuration des LED pour l'identification des composants du châssis ».

14

Configuration et utilisation d'iKVM

Le module KVM d'accès local du châssis de serveurs Dell M1000e est appelé Avocent Integrated KVM Switch Module (iKVM). L'iKVM est un commutateur analogique clavier, écran et souris, qui se branche sur le châssis. Il s'agit d'un module facultatif, échangeable à chaud sur le châssis, qui permet d'accéder localement par clavier, écran et souris aux serveurs du châssis et à la ligne de commande du CMC actif.

Liens connexes

Interface utilisateur d'iKVM
Principales fonctions iKVM
Interfaces de connexion physique

Interface utilisateur d'iKVM

Le module iKVM emploie l'interface utilisateur graphique OSCAR (On Screen Configuration and Reporting, configuration et rapports à l'écran), activée à l'aide d'une touche de fonction. OSCAR vous permet de sélectionner le serveur (ou la ligne de commande Dell CMC) auquel vous souhaitez accéder avec le clavier, l'écran et la souris locaux. Le système n'autorise qu'une seule session iKVM par châssis.

Liens connexes

Utilisation d'OSCAR

Principales fonctions iKVM

- Sécurité : protège le système à l'aide d'un mot de passe d'économiseur d'écran. À la fin du délai défini par l'utilisateur, le mode Économiseur d'écran se déclenche et l'accès est impossible tant que l'utilisateur n'a pas entré le mot de passe correct pour réactiver OSCAR.
- Balayage : vous permet de sélectionner une liste de serveurs, qui sont affichés dans l'ordre sélectionné lorsqu'OSCAR est en mode de balayage.
- Identification des serveurs : CMC attribue des noms de logement uniques à tous les serveurs du châssis. Bien qu'il soit possible d'attribuer des noms aux serveurs à l'aide de l'interface OSCAR depuis une connexion multiniveau, les noms attribués par CMC sont prioritaires, et les nouveaux noms que vous avez attribués aux serveurs avec OSCAR sont écrasés.

  Pour renommer les logements à l'aide de l'interface Web CMC, voir « Configuration des noms de logement ».

  Pour renommer un logement avec RACADM, consultez la section traitant de la commande **setslotname** dans le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de la ligne de commande pour iDRAC7 et CMC).
- Vidéo : les connexions vidéo iKVM prennent en charge les résolutions d'affichage vidéo comprises entre 640x480 à 60 Hz et 1 280x1 024 à 60 Hz.
- Plug-and-Play : iKVM prend en charge le Plug-and-Play DDC (Display Data Channel, canal de données d'affichage), qui automatise la configuration de l'écran conformément à la norme VESA DDC2B.
- Mise à niveau Flash : permet de mettre à jour le micrologiciel iKVM avec l'interface Web CMC ou la commande RACADM `fwupdate`.

Liens connexes

Utilisation d'OSCAR
Gestion des serveurs avec iKVM

Gestion d'iKVM depuis CMC
Mise à jour du micrologiciel iKVM

Interfaces de connexion physique

Vous pouvez vous connecter à un serveur ou à la console de l'interface de ligne de commande du CMC via iKVM depuis le panneau avant du châssis, une interface de console analogique (ACI) et le panneau arrière du châssis.

REMARQUE : Les ports sur le panneau de configuration à l'avant du châssis sont conçus pour l'iKVM, qui est facultatif. Si vous ne disposez pas du module iKVM, vous ne pouvez pas utiliser les ports qui figurent sur le panneau de configuration avant.

Priorités de connexion d'iKVM

Une seule connexion iKVM est disponible à la fois. L'iKVM affecte un ordre de priorité pour chaque type de connexion afin que, en présence de plusieurs connexions, une seule connexion soit disponible alors que les autres sont désactivées.

L'ordre de priorité pour les connexions d'iKVM est le suivant :

1. Panneau avant
2. ACI
3. Panneau arrière

Par exemple, si vous disposez de connexions iKVM sur le panneau avant et dans ACI, la connexion du panneau avant reste active alors que la connexion ACI est désactivée. Si vous disposez de connexions arrière et ACI, la connexion ACI a la priorité.

Affectation de plusieurs couches via la connexion de l'ACI

L'iKVM permet des connexions en couches avec les serveurs et la console de ligne de commande CMC de l'iKVM, soit localement par l'intermédiaire d'un port de commutateur Dell Remote Console ou à distance par l'intermédiaire du logiciel Dell RCS. L'iKVM prend en charge les connexions ACI à partir des produits suivants :

- Commutateurs Dell Remote Console 180AS, 2160AS, 2161DS*, 2161DS-2 ou 4161DS
- Système de commutation Avocent AutoView
- Système de commutation Avocent DSR
- Système de commutation Avocent AMX

REMARQUE : 2161DS ne prend pas en charge la connexion de la console Dell CMC.

REMARQUE : L'iKVM prend également en charge une connexion ACI aux Dell 180ES et 2160ES, mais la mise en couches n'est pas transparente. Cette connexion exige un USB à PS2 SIP.

Utilisation d'OSCAR

Cette section fournit des informations pour le lancement, la configuration et l'utilisation de l'interface OSCAR.

Liens connexes

Lancement d'OSCAR
Notions de base sur la navigation
Configuration de l'interface OSCAR

Lancement d'OSCAR

Pour lancer OSCAR :

1. Appuyez sur <Impr. écran>.
   La boîte de dialogue Menu principal s'affiche.
   Si un mot de passe est défini, la boîte de dialogue **Mot de passe** s'affiche lorsque vous appuyez sur <Impr. écran>.
2. Entrez le mot de passe et cliquez sur **OK**.
   La boîte de dialogue Menu principal apparaît.

   REMARQUE : Vous disposez de quatre options pour appeler OSCAR. Vous pouvez activer une ou plusieurs de ces séquences de touches, ou toutes, en cochant les cases appropriées dans la section Appeler OSCAR de la fenêtre Menu principal.

Liens connexes

Paramétrage de la sécurité de la console
Notions de base sur la navigation

Notions de base sur la navigation

Tableau 32. : Navigation dans OSCAR avec le clavier et la souris

Touche ou séquence de touches	Résultat
• <Impr. écran>-<Impr. écran> • <Maj>-<Maj> • <Alt>-<Alt> • <Ctrl>-<Ctrl>	Toutes ces séquences de touches peuvent ouvrir OSCAR, en fonction des paramètres **Appeler OSCAR** définis. Vous pouvez activer deux ou trois séquences de touches, ou toutes, en cochant les cases appropriées dans la section **Appeler OSCAR** de la boîte de dialogue **Menu principal**. Cliquez ensuite sur **OK**.
<F1>	Ouvre l'écran **Aide** de la boîte de dialogue active.
<Échap>	Ferme la boîte de dialogue active sans enregistrer les modifications apportées et retourne à la boîte de dialogue précédente. Dans la boîte de dialogue **Menu principal**, <Échap> ferme l'interface OSCAR et retourne au serveur sélectionné. Dans une boîte de message, il ferme la boîte contextuelle et retourne à la boîte de dialogue active.
<Alt>	Ouvre des boîtes de dialogue, sélectionne ou coche des options, et exécute des actions lorsqu'il est utilisé en conjonction avec les lettres soulignées ou d'autres caractères désignés.
<Alt>+<X>	Ferme la boîte de dialogue active et retourne à la boîte de dialogue précédente.
<Alt>+<O>	Sélectionne **OK** et revient à la boîte de dialogue précédente.
<Entrée>	Termine une opération de commutateur dans la boîte de dialogue **Menu principal** et quitte OSCAR.

Touche ou séquence de touches	Résultat
Simple clic, <Entrée>	Dans une zone de texte, permet de sélectionner le texte pour modification, et active les touches Gauche et Droite pour le déplacement du curseur. Appuyez de nouveau sur <Entrée> pour sortir du mode de modification.
<Impr. écran>, <Retour>	Revient à la sélection précédente en l'absence d'autres séquences de touches.
<Impr. écran>, <Alt>+<0>	Déconnecte immédiatement un utilisateur d'un serveur ; aucun serveur n'est sélectionné. L'indicateur d'état affiche Disponible. (Cette action s'applique uniquement à la touche <0> du clavier, pas à celle du pavé numérique.)
<Impr. écran>, <Pause>	Active immédiatement le mode économiseur d'écran et empêche l'accès à cette console spécifique, si elle est protégée par mot de passe.
Touches fléchées haut/bas	Déplace le curseur de ligne en ligne dans les listes.
Touches fléchées droite/ gauche	Déplace le curseur dans les colonnes lors de la modification d'une zone de texte.
<Accueil>/<Fin>	Déplace le curseur vers le haut (Accueil) ou vers le bas (Fin) d'une liste.
<Suppr>	Supprime des caractères dans une zone de texte.
Touches numérotées	Tapez sur le clavier ou le pavé numérique.
<Verr Maj>	Désactivé. Pour modifier la casse, utilisez la touche <Maj>.

Configuration de l'interface OSCAR

Vous pouvez configurer les paramètres OSCAR à l'aide de la boîte de dialogue **Configuration**.

Accès à la boîte de dialogue Configuration

Pour accéder à la boîte de dialogue **Configuration** :

1. Appuyez sur la touche <Imp écr> pour lancer l'interface OSCAR.
   La boîte de dialogue **Menu principal** s'affiche.
2. Cliquez sur **Configuration**.
   La boîte de dialogue **Configuration** s'affiche.

Fonctionnalité	Objectif
Menu	Change la liste des serveurs soit numériquement par logement, soit alphabétiquement par nom.
Sécurité	– Définit un mot de passe pour restreindre l'accès aux serveurs. – Active un économiseur d'écran et définit un temps d'inactivité avant l'apparition de l'économiseur d'écran et définit le mode d'économie d'écran.
Indicateur	Change l'affichage, la synchronisation, la couleur ou l'emplacement de l'indicateur de condition.
Langue	Change la langue de tous les écrans OSCAR.

Fonctionnalité	Objectif
Diffusion	Configure pour contrôler simultanément plusieurs serveurs par des actions sur le clavier et la souris.
Balayage	Configure une séquence de balayage personnalisée pour un maximum de 16 serveurs.

Liens connexes

Modification du comportement de l'affichage
Attribution de séquences de touches pour OSCAR
Définition du délai d'affichage de l'écran pour OSCAR
Configuration de l'affichage des indicateurs de condition

Modification du comportement de l'affichage

Utilisez la boîte de dialogue **Menu** pour changer l'ordre d'affichage des serveurs et définir un temps de retard d'affichage de l'écran pour OSCAR.

Pour modifier le comportement de l'affichage :

1. Appuyez sur <Impr. écran> pour lancer OSCAR.
   La boîte de dialogue **Menu principal** s'affiche.
2. Cliquez sur **Configuration**, puis sur **Menu.**
   La boîte de dialogue **Menu** s'affiche.
3. Pour choisir l'ordre d'affichage par défaut des serveurs, effectuez l'une des tâches suivantes :
   - Sélectionnez **Nom** pour afficher les serveurs par ordre alphabétique selon le nom.
   - Sélectionnez **Logement** pour afficher les serveurs par numéro de logement.
4. Cliquez sur **OK**.

Attribution de séquences de touches pour OSCAR

Pour attribuer une ou plusieurs séquences de touches pour l'activation d'OSCAR, sélectionnez la séquence voulue dans le menu **Appeler OSCAR**, puis cliquez sur **OK**. La touche par défaut pour l'appel d'OSCAR est <Impr. écran>.

Définition du délai d'affichage de l'écran pour OSCAR

Vous pouvez définir le délai avant affichage de l'écran OSCAR, à partir du moment où vous appuyez sur <Impr. écran>. Pour ce faire, entrez le nombre de secondes (0 à 9) dont il faut retarder l'affichage d'OSCAR, puis cliquez sur **OK**.

Entrez <0> pour lancer OSCAR immédiatement.

Le paramétrage d'un temps de retard d'affichage d'OSCAR vous permet de terminer une commutation logicielle.

Liens connexes

Commutation logicielle

Configuration de l'affichage des indicateurs de condition

L'indicateur de condition s'affiche sur votre bureau et indique le nom du serveur sélectionné ou la condition du logement sélectionné. Utilisez la boîte de dialogue Indicateur pour configurer l'indicateur à afficher par serveur ou pour modifier les attributs suivants des indicateurs : couleur, opacité, période d'affichage et emplacement sur le bureau.

Indicateur	Description
	Type d'indicateur par nom
	Indicateur indiquant que l'utilisateur a été déconnecté de tous les systèmes
	Indicateur indiquant que le mode Diffusion est activé

Pour configurer l'affichage de l'indicateur de condition :

1. Appuyez sur <Impr. écran> pour lancer OSCAR.
   La boîte de dialogue **Menu principal** apparaît.
2. Cliquez sur **Configuration**, puis sur **Indicateur**.
   La boîte de dialogue **Indicateur** apparaît.
3. Sélectionnez **Affiché** pour afficher l'indicateur en permanence ou **Affiché** et **synchronisé** pour afficher l'indicateur pendant seulement cinq secondes après la commutation.

   REMARQUE : Si vous sélectionnez **Synchronisé** uniquement, l'indicateur n'est pas affiché.
4. Dans la section **Couleur d'affichage**, sélectionnez une couleur d'indicateur. Vous avez le choix entre noir, rouge, bleu et violet.
5. Dans **Mode d'affichage**, sélectionnez **Opaque** pour obtenir un indicateur de couleur opaque ou **Transparent** pour voir le bureau à travers l'indicateur.
6. Pour positionner l'indicateur de condition sur le bureau, cliquez sur **Définir la position**.
   L'indicateur **Définir la position** s'affiche.
7. Cliquez avec le bouton gauche de la souris sur la barre de titre et faites-la glisser à l'emplacement de votre choix sur le bureau, puis cliquez avec le bouton droit de la souris pour revenir à la boîte de dialogue **Indicateur**.
8. Cliquez sur **OK** puis de nouveau sur **OK** pour enregistrer les paramètres.

   Pour quitter sans enregistrer les modifications, cliquez sur  .

Gestion des serveurs avec iKVM

Le module iKVM est une matrice de commutation analogique qui prend en charge jusqu'à 16 serveurs. Le commutateur iKVM utilise l'interface utilisateur OSCAR pour sélectionner et configurer les serveurs. De plus, l'iKVM inclut une entrée système permettant d'établir une connexion à CMC à l'aide de la console de ligne de commande CMC.

Si vous disposez d'une session de redirection de console active et si un écran à faible résolution est connecté à l'iKVM, la résolution de la console de serveur peut être réinitialisée si le serveur est sélectionné dans la console locale. Si le serveur exécute un système d'exploitation Linux, vous risquez de ne pas pouvoir afficher une console X11 sur l'écran local. Appuyez sur <Ctrl><Alt><F1> dans l'iKVM pour faire basculer Linux vers une console texte.

Liens connexes

Compatibilité des périphériques et prise en charge

Affichage et sélection de serveurs

Compatibilité des périphériques et prise en charge

iKVM est compatible avec les périphériques suivants :

- Claviers USB PC standard avec dispositions QWERTY, QWERTZ, AZERTY et Japonais 109.
- Moniteurs VGA avec prise en charge DDC.
- Périphériques de pointage USB standard.
- Concentrateurs USB 1.1 auto-alimentés connectés au port USB local sur iKVM.
- Concentrateurs USB 2.0 alimentés connectés à la console du panneau avant du châssis Dell M1000e.

REMARQUE : Vous pouvez utiliser plusieurs claviers et souris sur le port USB local du module iKVM. L'iKVM regroupe les signaux d'entrée. S'il reçoit simultanément des signaux d'entrée provenant de plusieurs claviers ou souris USB, les résultats peuvent être imprévisibles.

REMARQUE : Les connexions USB ne sont possibles que pour les concentrateurs de clavier, souris et USB pris en charge. iKVM ne prend pas en charge les données transmises depuis d'autres périphériques USB.

Affichage et sélection de serveurs

Lorsque vous lancez OSCAR, la boîte de dialogue **Menu principal** apparaît. Utilisez la boîte de dialogue **Menu principal** pour afficher, configurer et gérer les serveurs via le module iKVM. Vous pouvez afficher les serveurs par nom ou par logement. Le numéro de logement correspond au logement du châssis que le serveur occupe. La colonne **Logement** indique le numéro du logement où un serveur est installé.

REMARQUE : La ligne de commande Dell CMC occupe le logement 17. Sélectionnez ce logement pour afficher la ligne de commande CMC, qui permet d'exécuter des commandes RACADM, ou de se connecter à la console série des modules de serveur ou d'E/S (IOM).

REMARQUE : Les noms de serveur et les numéros de logement sont attribués par le contrôleur CMC.

Liens connexes

Commutation logicielle
Affichage de l'état du serveur
Sélection des serveurs

Affichage de l'état du serveur

Les colonnes de droite de la boîte de dialogue **Menu principal** indiquent l'état des serveurs du châssis. Le tableau suivant décrit les symboles d'état.

Tableau 33. Symboles de condition de l'interface OSCAR

Symboles	Description
	Serveur en ligne.
	Serveur hors ligne ou absent du châssis.
	Serveur non disponible.
	Serveur utilisé depuis le canal utilisateur indiqué par la lettre : • A=panneau arrière

Symboles	Description
	• B=panneau avant

Sélection des serveurs

Utilisez la boîte de dialogue **Menu principal** pour sélectionner les serveurs. Lorsque vous sélectionnez un serveur, le module iKVM reconfigure le clavier et la souris sur les paramètres appropriés pour ce serveur.

- Pour sélectionner des serveurs, effectuez l'une des opérations suivantes :
  - Double-cliquez sur le nom de serveur ou le numéro de logement.
  - Si l'ordre d'affichage de votre liste de serveurs est défini sur Par logement (vous avez appuyé sur le bouton Logement), entrez le numéro de logement et appuyez sur <Entrée>.
  - Si l'ordre d'affichage de votre liste de serveurs est défini sur Par nom (vous avez appuyé sur le bouton Nom), entrez les premiers caractères du nom du serveur, vérifiez qu'il est unique et appuyez à deux reprises sur <Entrée>.
- Pour sélectionner le serveur précédent, appuyez sur <Impr. écran>, puis sur <Ret. arr.>. Cette combinaison de touches permet de basculer entre la connexion actuelle et la précédente.
- Pour déconnecter l'utilisateur d'un serveur, effectuez l'une des opérations suivantes :
  - Appuyez sur <Impr. écran> pour accéder à OSCAR, puis cliquez sur Déconnecter.
  - Appuyez sur <Impr. écran>, puis sur <Alt>+<0>. Cela vous laisse à l'état Disponible, sans aucun serveur sélectionné. L'indicateur d'état sur le bureau, s'il est activé, indique Disponible. Voir « **Définition de l'affichage de l'indicateur d'état** ».

Commutation logicielle

La commutation logicielle permet de commuter entre les différents serveurs à l'aide d'une séquence de touches. Appuyez sur <Impr. écran> pour effectuer la commutation logicielle vers un serveur, puis entrez les premiers caractères de son nom ou de son numéro. Si vous avez préalablement définir un délai (nombre de secondes avant l'affichage de la boîte de dialogue **Menu principal**, à partir du moment où vous appuyez sur <Impr. écran>) et si vous appuyez sur les touches voulues avant la fin de ce délai, l'interface OSCAR ne s'affiche pas.

Liens connexes

Configuration de la commutation logicielle
Commutation logicielle vers un serveur

Configuration de la commutation logicielle

Pour configurer OSCAR pour la commutation logicielle :

1. Appuyez sur la touche <Imp écr> pour lancer l'interface OSCAR.
   La boîte de dialogue **Menu principal** apparaît.
2. Cliquez sur **Configuration**, puis sur **Menu**.
   La boîte de dialogue **Menu** s'affiche.
3. Sélectionnez **Nom** ou **Logement** pour la touche Afficher/Trier.
4. Entrez le temps de délai souhaité en secondes dans le champ **Temps de délai d'affichage de l'écran**.
5. Cliquez sur **OK**.

Commutation logicielle vers un serveur

Pour effectuer une commutation logicielle vers un serveur :

- Pour sélectionner un serveur, appuyez sur <Impr. écran>. Si votre liste de serveurs est affichée dans l'ordre des logements d'après votre sélection (vous avez appuyé sur le bouton Logement), entrez le numéro du logement et appuyez sur <Entrée>.

  ou

  Si votre liste de serveurs est affichée dans l'ordre des noms conformément à votre sélection (vous avez appuyé sur le bouton Nom), entrez les premiers caractères du nom du serveur pour vérifier qu'il s'agit d'un nom unique et appuyez sur <Entrée>.
- Pour retourner au serveur précédent, appuyez sur <Impr. écran>, puis sur <Retour>.

Connexions vidéo

Le module iKVM comporte des connexions vidéo sur le panneau arrière et le panneau avant du châssis. Les signaux de connexion du panneau avant sont prioritaires sur ceux du panneau arrière. Si vous branchez un écran sur le panneau avant, la connexion vidéo ne passe pas par le panneau arrière et un message d'OSCAR s'affiche, précisant que les connexions KVI et ACI du panneau arrière sont désactivées. Si l'écran est désactivé (supprimé du panneau avant ou désactivé par une commande CMC), la connexion ACI s'active alors que la connexion KVM du panneau arrière reste inactive.

Liens connexes

Priorités de connexion d'iKVM

Activation ou désactivation de l'accès à iKVM depuis le panneau avant

Avertissement de préemption

Normalement, un utilisateur connecté à une console de serveur via iKVM et un autre utilisateur connecté à la même console de serveur via la fonction de redirection de console de l'interface Web iDRAC ont tous deux accès à la console, et peuvent entrer des données simultanément.

Pour éviter cela, avant de lancer la redirection de console dans l'interface Web iDRAC, l'utilisateur distant peut désactiver la console locale dans cette même interface Web. L'utilisateur iKVM local voit s'afficher un message d'OSCAR indiquant que la connexion a été préemptée par un autre pour une durée spécifique. L'utilisateur local doit finir d'utiliser la console avant que la connexion iKVM au serveur soit arrêtée.

Aucune fonction de préemption n'est disponible pour l'utilisateur iKVM.

REMARQUE : Si un utilisateur iDRAC distant a désactivé la vidéo locale pour un serveur spécifique, les fonctions écran, clavier et souris de ce serveur ne sont pas disponibles pour l'iKVM. L'état du serveur est signalé par un point jaune dans le menu OSCAR afin d'indiquer qu'il est verrouillé ou indisponible pour l'utilisation. Voir « Affichage de l'état du serveur ».

Liens connexes

Affichage de l'état du serveur

Paramétrage de la sécurité de la console

OSCAR vous permet de configurer les paramètres de sécurité de la console iKVM. Vous pouvez définir un mode d'économiseur d'écran, qui se déclenche si la console reste inutilisée pendant un certain temps. Une fois l'économiseur d'écran déclenché, la console reste verrouillée jusqu'à ce que l'utilisateur appuie sur une touche ou déplace la souris. Entrez le mot de passe de l'économiseur d'écran pour continuer.

Utilisez la boîte de dialogue **Sécurité** pour verrouiller la console à l'aide d'un mot de passe, pour définir ou modifier le mot de passe, ou pour activer l'économiseur d'écran.

REMARQUE : Si le mot de passe iKVM est perdu ou oublié, vous pouvez le réinitialiser sur les paramètres par défaut d'iKVM à l'aide de l'interface Web CMC ou RACADM.

Liens connexes

Accès à la boîte de dialogue Sécurité
Définition du mot de passe
Protection de la console par mot de passe
Paramétrage de la fermeture de session automatique
Suppression de la protection par mot de passe depuis la console
Activation du mode d'économiseur d'écran sans protection par mot de passe
Quitter le mode d'économiseur d'écran
Suppression d'un mot de passe perdu ou oublié

Accès à la boîte de dialogue Sécurité

Pour accéder à la boîte de dialogue Sécurité, procédez comme suit:

1. Appuyez sur <Impr. écran>.
   La boîte de dialogue **Menu principal** apparaît.
2. Cliquez sur **Configuration**, puis sur **Sécurité**.
   La boîte de dialogue **Sécurité** apparaît.

Définition du mot de passe

Pour définir le mot de passe :

1. Cliquez une fois et appuyez sur <Entrée> ou double-cliquez dans le champ **Nouveau**.
2. Entrez le nouveau mot de passe, puis appuyez sur <Entrée>. Les mots de passe sont sensibles à la casse et doivent comprendre de 5 à 12 caractères. Ils doivent inclure au moins une lettre et un chiffre. Les caractères autorisés sont les suivants : A–Z, a–z, 0–9, espace et tiret.
3. Entrez à nouveau le mot de passe dans le champ **Répéter**, puis appuyez sur <Entrée>.
4. Cliquez sur **OK** et fermez la boîte de dialogue.

Protection de la console par mot de passe

Pour protéger la console avec un mot de passe :

1. Définissez le mot de passe comme l'indique la rubrique « Définition d'un mot de passe ».
2. Cochez la case **Activer l'économiseur d'écran**.
3. Entrez un nombre de minutes (entre 1 et 99) dans le champ **Durée d'inactivité** pour déterminer le délai avant activation de la protection par mot de passe et de l'économiseur d'écran.
4. Champ **Mode** : si votre écran est compatible ENERGY STAR, sélectionnez **Energy** ; sinon, sélectionnez **Écran**.
   - Si vous choisissez le mode **Energy**, l'appliance met l'écran en mode Veille. En général, cela se manifeste par l'extinction de l'écran et le passage d'une LED d'alimentation verte à une LED orange.
   - Si vous choisissez le mode **Écran**, l'indicateur OSCAR surgit sur l'écran pour toute la durée du test. Avant le début du test, une fenêtre pop-up d'avertissement affiche le message suivant : « Le mode Energy peut endommager l'écran s'il n'est pas compatible ENERGY STAR. Toutefois, une fois le test démarré, vous pouvez le quitter immédiatement en déplaçant la souris ou en appuyant sur une touche. »

   PRÉCAUTION : Le moniteur peut être endommagé s'il est utilisé en mode Energy sans être conforme à la norme Energy Star.
5. Facultatif : pour activer le test d'économiseur d'écran, cliquez sur **Tester**. La boîte de dialogue **Test d'économiseur d'écran** s'affiche. Cliquez sur **OK** pour lancer le test.

Le test prend 10 secondes. Lorsqu'il est terminé, vous revenez à la boîte de dialogue **Sécurité**.

Paramétrage de la fermeture de session automatique

Vous pouvez paramétrer OSCAR pour fermer automatiquement une session sur un serveur après une période d'inactivité.

1. Dans la boîte de dialogue **Menu principal**, cliquez sur **Configuration**, puis sur **Sécurité**.
2. Dans le champ **Temps d'inactivité**, entrez la période de temps pendant laquelle vous souhaitez rester connecté à un serveur avant qu'il ne vous déconnecte automatiquement.
3. Cliquez sur **OK**.

Suppression de la protection par mot de passe depuis la console

Pour supprimer la protection par mot de passe à partir de la console :

1. Dans la boîte de dialogue **Menu principal**, cliquez sur **Configuration**, puis sur **Sécurité**.
2. Dans la boîte de dialogue **Sécurité**, cliquez une fois et appuyez sur <Entrée>, ou double-cliquez dans le champ **Nouveau**.
3. Laissez le champ **Nouveau** vide et appuyez sur <Entrée>.
4. Cliquez une fois et appuyez sur <Entrée>, ou double-cliquez dans le champ **Répéter**.
5. Laissez le champ **Répéter** vide et appuyez sur <Entrée>.
6. Cliquez sur **OK**.

Activation du mode d'économiseur d'écran sans protection par mot de passe

REMARQUE : Si votre console est protégée par un mot de passe, vous devez d'abord supprimer cette protection. Supprimez le mot de passe avant d'activer le mode d'économiseur d'écran sans protection par mot de passe.

Pour activer le mode d'économiseur d'écran sans protection par mot de passe :

1. Sélectionnez **Activer l'économiseur d'écran**.
2. Entrez le nombre de minutes (de 1 à 99) souhaité pour retarder l'activation de l'économiseur d'écran.
3. Sélectionnez **Energy** si votre moniteur est conforme à ENERGY STAR ; sinon, sélectionnez **Écran**.

   PRÉCAUTION : Le moniteur peut être endommagé s'il est utilisé en mode Energy sans être conforme à la norme Energy Star.
4. Facultatif : pour activer le test d'économiseur d'écran, cliquez sur **Tester**. La boîte de dialogue **Test d'économiseur d'écran** s'affiche. Cliquez sur **OK** pour lancer le test.

   Le test prend 10 secondes. Lorsqu'il est terminé, la boîte de dialogue **Sécurité** s'affiche.

   REMARQUE : L'activation du mode **Économiseur d'écran** déconnecte l'utilisateur d'un serveur. Cela signifie qu'aucun serveur n'est sélectionné. L'indicateur d'état affiche **Disponible**.

Quitter le mode d'économiseur d'écran

Pour quitter le mode économiseur d'écran et retourner à la boîte de dialogue **Groupe principal**, appuyez sur une touche quelconque ou déplacez votre souris.

Pour désactiver l'économiseur d'écran, dans la boîte de dialogue **Sécurité**, désélectionnez la case à cocher **Activer l'économiseur d'écran**, puis cliquez sur **OK**.

Pour activer immédiatement l'économiseur d'écran, appuyez sur <Impr. écran>, puis sur <Pause>.

Suppression d'un mot de passe perdu ou oublié

Lorsque vous oubliez ou perdez le mot de passe iKVM, vous pouvez rétablir les valeurs iKVM par défaut, puis changer de mot de passe. Pour réinitialiser le mot de passe, utilisez l'interface Web CMC ou RACADM.

Pour réinitialiser un mot de passe iKVM perdu ou oublié à l'aide de l'interface Web CMC, dans l'arborescence, allez à **Présentation du châssis** → **iKVM**, cliquez sur l'onglet **Configurer** puis sur **Restaurer les valeurs par défaut**.

Vous pouvez modifier le mot de passe par défaut à l'aide d'OSCAR. Pour en savoir plus, voir Définition du mot de passe.

Pour réinitialiser un mot de passe perdu ou oublié à l'aide de RACADM, ouvrez une console texte série/Telnet/SSH vers CMC, ouvrez une session et entrez :

```
racadm racresetcfg -m kvm
```

REMARQUE : L'utilisation de la commande `racresetcfg` réinitialise les paramètres Activation du panneau avant et Activation de la console Dell CMC s'ils diffèrent des valeurs par défaut.

Pour des informations supplémentaires sur la sous-commande `racresetcfg`, voir le *Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC*.

Modification de la langue

Utilisez la boîte de dialogue **Langue** pour changer le texte de l'interface OSCAR afin de l'afficher dans n'importe laquelle des langues prises en charge. Le texte bascule immédiatement vers la langue sélectionnée, dans tous les écrans OSCAR.

Pour changer la langue d'OSCAR :

1. Appuyez sur <Impr. écran>.
   La boîte de dialogue **Menu principal** apparaît.
2. Cliquez sur **Configuration**, puis sur **Langue**.
   La boîte de dialogue **Langue** apparaît.
3. Sélectionnez la langue voulue et cliquez sur **OK**.

Affichage des informations sur la version

Utilisez la boîte de dialogue **Version** pour afficher les versions du micrologiciel et du matériel d'iKVM, et pour identifier la configuration de la langue et du clavier.

Pour afficher les informations sur la version :

1. Appuyez sur <Impr. écran>.
   La boîte de dialogue **Menu principal** s'affiche.
2. Cliquez sur **Commandes**, puis sur **Afficher les versions**.
   La boîte de dialogue **Version** s'affiche. La partie supérieure de la boîte de dialogue **Version** répertorie les versions des sous-systèmes.
3. Cliquez sur la  ou appuyez sur <Échap> pour fermer la boîte de dialogue **Version**.

Balayage du système

En mode de balayage, l'iKVM balaye automatiquement les logements un par un (serveur par serveur). Vous pouvez balayer jusqu'à 16 serveurs en spécifiant les serveurs à balayer et le nombre de secondes d'affichage de chaque serveur.

Liens connexes

Ajout de serveurs à la liste de balayage
Suppression d'un serveur de la liste Balayage
Lancement du mode de balayage
Annulation du mode de balayage

Ajout de serveurs à la liste de balayage

Pour ajouter des serveurs à la liste de balayage :

1. Appuyez sur <Impr. écran>.
   La boîte de dialogue **Menu principal** s'affiche.
2. Cliquez sur **Configuration**, puis sur **Balayage**.
   La boîte de dialogue **Balayage** qui apparaît répertorie tous les serveurs du châssis.
3. Effectuez l'une des opérations suivantes :
   - Sélectionnez les serveurs à balayer.
   - Double-cliquez sur le nom ou le logement du serveur.
   - Appuyez sur <Alt> et sur le numéro des serveurs à balayer. Vous pouvez sélectionner jusqu'à 16 serveurs.
4. Dans le champ **Temps**, entrez le nombre de secondes (de 3 à 99) pendant lesquelles iKVM devra patienter avant que le balayage ne se déplace au serveur suivant dans la séquence.
5. Cliquez sur **Ajouter/Supprimer**, puis sur **OK**.

Suppression d'un serveur de la liste Balayage

Pour supprimer un serveur de la liste Balayage :

1. Dans la boîte de dialogue **Balayage**, procédez comme suit :
   - Sélectionnez le serveur à supprimer.
   - Double-cliquez sur le nom ou le logement du serveur.
   - Cliquez sur le bouton **Effacer** pour supprimer tous les serveurs de la liste **Balayage**.
2. Cliquez sur **Ajouter/Supprimer** puis sur **OK**.

Lancement du mode de balayage

Pour lancer le mode de balayage :

1. Appuyez sur <Impr. écran>.
   La boîte de dialogue **Menu principal** s'affiche.
2. Cliquez sur **Commandes**.
   La boîte de dialogue **Commande** s'affiche.
3. Cochez la case **Activation du balayage**.
4. Cliquez sur **OK**.
   Un message indiquant que la souris et le clavier ont été réinitialisés apparaît.

5. Cliquez sur la  pour fermer la fenêtre de message.

Annulation du mode de balayage

Pour annuler le mode de balayage :

1. Si l'interface OSCAR est ouverte et que la boîte de dialogue **Menu principal** est affichée, sélectionnez un serveur dans la liste.

   ou

   Si l'interface OSCAR est fermée, déplacez la souris ou appuyez sur une touche du clavier.

   La boîte de dialogue **Menu principal** apparaît. Sélectionnez un serveur dans la liste.
2. Cliquez sur **Commandes**.

   La boîte de dialogue **Commandes** s'affiche.
3. Désélectionnez l'option **Activation du balayage** et cliquez sur **OK**.

Diffusion aux serveurs

Vous pouvez contrôler simultanément plusieurs serveurs du système afin de vous assurer que tous les serveurs sélectionnés reçoivent les mêmes informations. Vous pouvez choisir de diffuser indépendamment les appuis sur les touches du clavier et/ou les mouvements de la souris :

- Diffusion des frappes de touche : lorsque vous diffusez les frappes de touche, l'état du clavier doit être identique pour tous les serveurs qui reçoivent une diffusion, afin que l'utilisation des touches soit interprétée à l'identique. En particulier, les modes <Verr. maj> et <Verr. num> doivent être identiques pour tous les claviers. Lorsque le module iKVM tente d'envoyer les frappes de touche simultanément à tous les serveurs sélectionnés, certains serveurs peuvent être inhibés, ce qui retarde la transmission
- Diffusion des mouvements de la souris : pour que la souris fonctionne correctement, tous les serveurs doivent posséder le même pilote de souris, le même bureau (icônes placées au même endroit, etc.) et la même résolution vidéo. La souris doit aussi se trouver exactement au même endroit sur tous les écrans. Comme ces conditions sont extrêmement difficiles à réunir, la diffusion des mouvements de la souris à plusieurs serveurs peut avoir des résultats imprévisibles.

REMARQUE : Vous pouvez diffuser simultanément vers un maximum de 16 serveurs.

Pour diffuser aux serveurs :

1. Appuyez sur <Impr. écran>.

   La boîte de dialogue **Menu principal** s'affiche.
2. Cliquez sur **Configuration**, puis sur **Diffuser**.

   La boîte de dialogue **Diffusion** s'affiche.
3. Activez la souris et/ou le clavier pour les serveurs qui doivent recevoir les commandes de diffusion en cochant les cases correspondantes.

   ou

   Appuyez sur les touches Haut ou Bas pour déplacer le curseur vers un serveur cible. Ensuite, appuyez sur <Alt> +<K> pour cocher la case du clavier et/ou sur <Alt>+<M pour cocher la case de la souris. Répétez l'opération pour les autres serveurs.
4. Cliquez sur **OK** pour enregistrer les paramètres et revenir à la boîte de dialogue **Configuration**.
5. Cliquez sur  ou appuyez sur <Échap> pour revenir à la boîte de dialogue **Menu principal**.
6. Cliquez sur **Commandes**.

La boîte de dialogue **Commandes** s'affiche.

7. Cochez la case **Activation de la diffusion** pour activer la diffusion.
   La boîte de dialogue **Avertissement de diffusion** s'affiche.
8. Cliquez sur **OK** pour activer la diffusion. Pour annuler et revenir à la boîte de dialogue **Commandes**, cliquez sur  ou appuyez sur <Échap
9. Si la diffusion est activée, entrez les informations et/ou réalisez les mouvements de souris à diffuser depuis la station de gestion. Seuls les serveurs de la liste sont accessibles.

Gestion d'iKVM depuis CMC

Vous pouvez effectuer les opérations suivantes :

- Afficher la condition et les propriétés d'iKVM
- Mettre à jour le micrologiciel iKVM
- Activer ou désactiver l'accès à iKVM depuis le panneau avant
- Activer ou désactiver l'accès à iKVM depuis la console Dell CMC

Liens connexes

Mise à jour du micrologiciel iKVM
Activation ou désactivation de l'accès à iKVM depuis le panneau avant
Affichage des informations et de la condition d'intégrité iKVM
Activation de l'accès à iKVM depuis la console Dell CMC

Activation ou désactivation de l'accès à iKVM depuis le panneau avant

Vous pouvez activer ou désactiver l'accès à iKVM depuis le panneau avant à l'aide de l'interface Web ou de RACADM.

Activation ou désactivation de l'accès à iKVM depuis le panneau avant avec l'interface Web

Pour activer ou désactiver l'accès à iKVM depuis le panneau avant à l'aide de l'interface Web CMC :

1. Dans l'arborescence système, accédez à **Présentation du châssis** → **iKVM**, puis cliquez sur l'onglet **Configuration**.
   La page **Configuration d'iKVM** s'affiche.
2. Pour activer la fonction, sélectionnez l'option **USB/Vidéo du panneau avant activé**. Pour désactiver la fonction, désélectionnez l'option **USB/Vidéo du panneau avant activé**.
3. Cliquez sur **Appliquer** pour enregistrer le paramètre.

Activation et désactivation de l'accès à iKVM depuis le panneau avant à l'aide de RACADM

Pour activer ou désactiver l'accès à iKVM depuis le panneau avant à l'aide de RACADM, ouvrez une console texte série/Telnet/SSH vers CMC, ouvrez une session et entrez :

```
racadm config -g cfgKVMInfo -o cfgKVMFrontPanelEnable <valeur>
```

où <valeur> est 1 (activer) ou 0 (désactiver). Pour en savoir plus sur la sous-commande

```
config
```

, voir le *RACADM Command Line Reference Guide for iDRAC7 and CMC (Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC.*

Activation de l'accès à iKVM depuis la console Dell CMC

Pour activer l'accès à l'interface de ligne de commande (CLI) CMC depuis iKVM avec l'interface Web CMC, dans l'arborescence système, accédez à **Présentation du châssis → iKVM**, puis cliquez sur l'onglet **Configuration**. Sélectionnez l'option **Autoriser l'accès à la CLI CMC à partir d'iKVM**, puis cliquez sur **Appliquer** pour enregistrer le paramètre.

Pour activer l'accès à l'interface de ligne de commande (CLI) CMC depuis l'iKVM à l'aide de RACADM, ouvrez une console texte série/Telnet/SSH pour CMC, connectez-vous et entrez :

```
racadm config -g cfgKVMInfo -o cfgKVMAccessToCMCEnable 1
```

Liens connexes

Connexion à CMC avec la console série, Telnet ou SSH

15

Gestion et surveillance de l'alimentation

L'enceinte de serveurs Dell PowerEdge M1000e est l'enceinte pour serveurs modulaires la plus économe en énergie. Elle est conçue pour inclure des blocs d'alimentation et ventilateurs très économes, avec une disposition optimisée qui permet une circulation plus facile du flux d'air dans l'ensemble du système. Enfin, vous trouverez des composants économes en énergie dans l'ensemble de l'enceinte. Cette conception matérielle optimisée est associée à des fonctions avancées de gestion de l'alimentation, intégrées aux modules Chassis Management Controller (CMC), aux blocs d'alimentation et à l'iDRAC. Elles vous permettent de gérer encore plus efficacement l'alimentation et de contrôler réellement votre environnement électrique.

Les fonctions de gestion de l'alimentation du M1000e aident les administrateurs à configurer l'enceinte de manière à réduire la consommation électrique et à ajuster l'alimentation en fonction des besoins spécifiques de l'environnement.

L'enceinte modulaire PowerEdge M1000e utilise une alimentation CA et répartit la charge de traitement sur l'ensemble des unités de bloc d'alimentation (PSU) internes actives. Le système peut générer jusqu'à 16 685 Watts CA, alloués aux modules de serveur et à l'infrastructure d'enceinte associée.

L'enceinte PowerEdge M1000e peut être configurée pour n'importe laquelle des trois règles de redondance affectant le comportement des unités d'alimentation et déterminant la manière dont l'état de redondance du châssis est signalé aux administrateurs.

Vous pouvez également contrôler la gestion de l'alimentation via la fonctionnalité **Console PM3** (Power Measure, Mitigate, and Manage Console - Console de mesure, d'économie et de gestion de l'alimentation). Lorsque vous contrôlez l'alimentation en externe avec PM3, le CMC continue à gérer les éléments suivants :

- Règle de redondance
- Journalisation distante de l'alimentation
- Performances du serveur avant redondance de l'alimentation
- Enclenchement dynamique des blocs l'alimentation
- Opération 110 VCA

PM3 gère alors:

- l'alimentation du serveur
- La priorité du serveur
- Capacité maximale de l'alimentation d'entrée du système
- Mode de conservation de puissance maximale

REMARQUE : La puissance de sortie réelle est basée sur la configuration et la charge de travail.

Vous pouvez utiliser l'interface Web CMC ou RACADM pour gérer et configurer le contrôle de l'alimentation du CMC :

- Consulter l'allocation d'alimentation, la consommation électrique et l'état d'alimentation du châssis, des serveurs et des blocs d'alimentation
- Configurer le bilan de puissance et la stratégie de redondance du châssis
- Exécuter des opérations de contrôle de l'alimentation (mise sous tension, mise hors tension, réinitialisation du système, cycle d'alimentation) du châssis

Liens connexes

Vous pouvez exécuter les opérations de contrôle de l'alimentation suivantes pour le châssis, les serveurs et les IOM.

Stratégies de redondance

La stratégie de redondance est un ensemble de propriétés configurable qui détermine la façon dont CMC gère l'alimentation du châssis. Vous pouvez configurer les stratégies de redondance suivantes avec ou sans DPSE (Dynamic Power Supply Engagement - Enclenchement dynamique des blocs d'alimentation) :

- Redondance de l'alimentation alternative
- Redondance des blocs d'alimentation
- Sans redondance

Stratégie de redondance de l'alimentation CA

L'objectif de la stratégie de redondance de l'alimentation CA est de permettre à un système d'enceinte modulaire de fonctionner dans un mode où il peut tolérer les pannes de l'alimentation CA. Ces pannes peuvent provenir du réseau électrique CA, du câblage et de la distribution, ou du bloc d'alimentation proprement dit.

Lorsque vous configurez un système pour la redondance d'alimentation CA, les blocs d'alimentation sont répartis en deux réseaux électriques : les blocs d'alimentation des logements 1, 2 et 3 sont sur le premier réseau, alors que les blocs d'alimentation des logements 4, 5 et 6 sont sur le deuxième. CMC gère l'alimentation de manière à ce qu'en cas d'échec d'un des deux réseaux électriques, le système continue à fonctionner sans dégradation. La redondance d'alimentation CA permet aussi de tolérer les pannes d'un seul bloc d'alimentation.

REMARQUE : Puisque l'un des rôles de la redondance d'alimentation alternative est d'assurer un fonctionnement sans faille du serveur malgré une panne du réseau électrique, la plus grande puissance est utilisée pour maintenir la redondance d'alimentation alternative lorsque les capacités des deux réseaux sont à peu près égales.

REMARQUE : La redondance d'alimentation alternative n'est atteinte que lorsque les conditions de charge ne dépassent pas la capacité du réseau ayant la plus faible puissance.

Niveaux de redondance d'alimentation alternative

La configuration minimale nécessaire pour utiliser la redondance d'alimentation CA consiste à installer un bloc d'alimentation (PSU) dans chaque réseau électrique. Il est possible de réaliser des configurations supplémentaires avec chaque combinaison comportant au moins un bloc d'alimentation dans chaque réseau. Toutefois pour disposer d'un maximum de puissance, vous devez utiliser dans chaque branche un nombre total de blocs d'alimentation aussi égal que possible. La limite maximale de puissance disponible en maintenant la redondance d'alimentation CA est la puissance disponible sur le plus faible des deux réseaux électriques. La figure suivante montre 2 blocs d'alimentation (PSU) par réseau électrique et une panne d'alimentation sur le réseau 1.

Si, pour une raison quelconque, CMC est incapable de maintenir la redondance d'alimentation CA, des alertes par e-mail et/ou SNMP sont envoyées aux administrateurs si l'événement Redondance perdue est configuré pour générer des alertes.

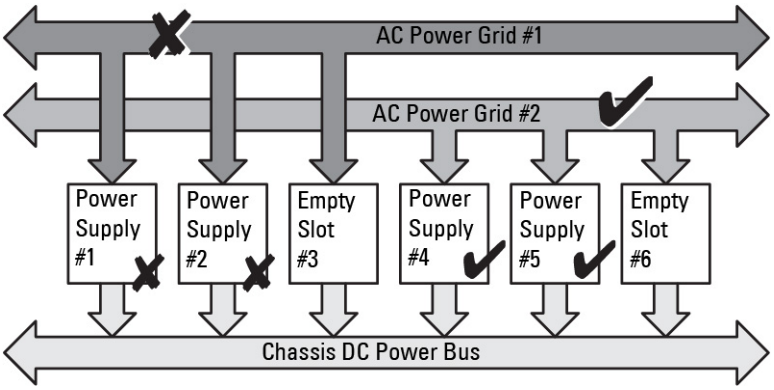


Figure 5. blocs d'alimentation par réseau électrique avec une panne électrique sur le réseau 1

Dans cette configuration, si un seul bloc d'alimentation (PSU) échoue, les autres PSU du réseau électrique défaillant sont marqués comme En ligne. Ainsi, l'un d'eux peut échouer sans que cela interrompe le fonctionnement du système. Si un PSU échoue, l'intégrité du châssis est marquée comme Non critique. Si le réseau électrique le plus petit ne peut pas prendre en charge l'allocation totale de puissance au châssis, l'état de la redondance CA est signalé comme **Sans redondance** et la zone Intégrité du châssis indique **Critique**.

Stratégie de redondance des blocs d'alimentation

La stratégie de redondance des blocs d'alimentation s'avère utile lorsque vous n'avez pas de réseaux électriques d'alimentation redondants, mais que vous souhaitez protéger le système afin que l'échec d'un seul bloc d'alimentation (PSU) n'éteigne pas les serveurs dans une enceinte modulaire. Le bloc d'alimentation de capacité supérieure est gardé en réserve en ligne dans ce but. Cela crée un pool de blocs d'alimentation. La figure ci-dessous illustre le mode de redondance de blocs d'alimentation.

Les unités d'alimentation se trouvant au-delà de celles exigées pour la puissance et la redondance sont encore disponibles et seront ajoutées au pool en cas de défaillance.

Contrairement à la redondance d'alimentation alternative, lorsque la redondance du bloc d'alimentation est sélectionnée, CMC n'a pas besoin que les unités d'alimentation soient présentes dans des positions de logement spécifiques.

REMARQUE : DPSE (Dynamic Power Supply Engagement - Enclenchement dynamique des blocs d'alimentation) permet de mettre des blocs d'alimentation (PSU) en veille. Cet état de veille est un état physique : le bloc ne fournit aucune alimentation. Lorsque vous activez DPSE, les PSU en excès peuvent être mis en veille pour augmenter l'efficacité du système et économiser l'énergie.

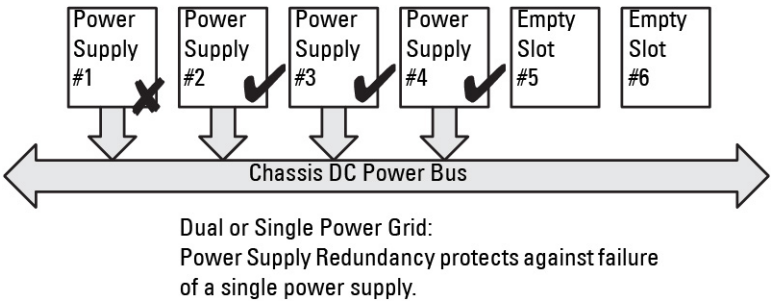


Figure 6. Redondance des blocs d'alimentation : 4 blocs d'alimentation au total avec un bloc d'alimentation en panne.

Stratégie Sans redondance

Le mode Sans redondance est le paramètre par défaut défini en usine pour la configuration à trois blocs d'alimentation (PSU), ce qui indique que le châssis est configuré sans aucune redondance d'alimentation. Dans cette configuration, l'état global de redondance du châssis indique toujours Sans redondance. La figure suivante illustre le mode Sans redondance, paramétrage d'usine par défaut pour la configuration à trois PSU.

CMC n'a pas besoin que les unités d'alimentation soient présentes dans des positions de logement spécifiques lorsque le mode **Sans redondance** est configuré.

REMARQUE : Tous les blocs d'alimentation (PSU) du châssis sont **En ligne** si vous désactivez DPSE alors que le système est en mode **Sans redondance**. Lorsque vous activez DPSE, tous les blocs d'alimentation (PSU) actifs du châssis sont répertoriés comme étant **En ligne**, et vous pouvez mettre des blocs d'alimentation supplémentaires à l'état **En veille** pour augmenter l'efficacité de l'alimentation du système.

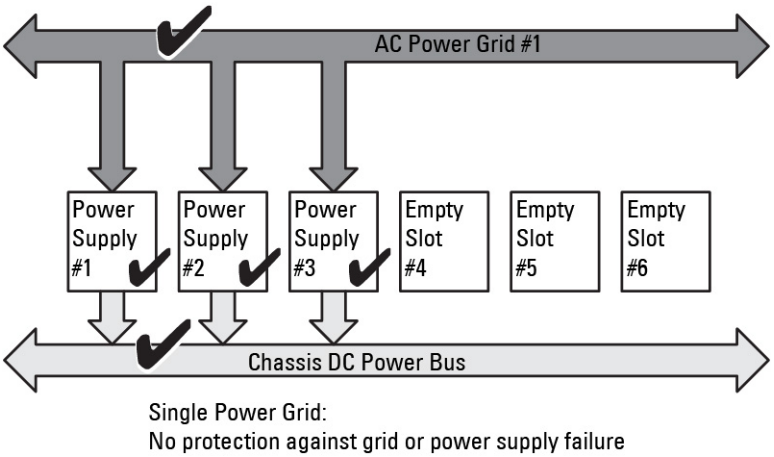


Figure 7. Mode Sans redondance avec trois blocs d'alimentation dans le châssis

L'échec d'un bloc d'alimentation (PSU) sort les autres PSU du mode En veille selon les besoins, afin de prendre en charge les allocations d'alimentation du châssis. Si vous avez configuré quatre PSU alors que vous en utilisez seulement trois, le quatrième PSU est mis en ligne si l'un des trois autres échoue. Les six PSU d'un châssis peuvent être en ligne.

Lorsque vous activez DPSE, les PSU non indispensables peuvent être mis en mode En veille pour renforcer l'efficacité et économiser l'énergie. Pour plus d'informations, voir « Configuration de redondance par défaut ».

Enclenchement dynamique des blocs l'alimentation

Le mode DPSE (Dynamic Power Supply Engagement - Enclenchement dynamique des blocs d'alimentation) est désactivé par défaut. DPSE permet d'économiser de l'énergie en optimisant l'efficacité des blocs d'alimentation (PSU) qui alimentent le châssis. Cela augmente aussi la durée de vie des PSU et réduit la génération de chaleur.

CMC surveille l'allocation globale d'alimentation de l'enceinte, et fait passer les PSU à l'état En veille, ce qui permet d'assurer l'allocation totale d'alimentation du châssis avec un nombre réduit de PSU. Comme les PSU en ligne sont plus efficaces à un taux d'utilisation supérieur, cela augmente leur efficacité tout en allongeant la durée de vie des PSU de secours.

Pour faire fonctionner les unités d'alimentation restantes à leur maximum d'efficacité :

- Le mode **Sans redondance** avec DPSE est particulièrement efficace pour économiser l'énergie, avec des blocs d'alimentation (PSU) optimaux en ligne. Les PSU non indispensables sont basculés en mode En veille.
- Le mode **Redondance des PSU** avec DPSE permet également une alimentation efficace. Au moins deux blocs d'alimentation (PSU) sont en ligne, l'un pour alimenter la configuration et l'autre pour assurer la redondance en

cas d'échec de ce premier PSU. Le mode de redondance des PSU vous protège en cas d'échec d'un seul PSU mais n'offre aucune protection en cas de perte de l'alimentation secteur CA.

- Le mode **Redondance de l'alimentation alternative** avec DPSE, dans lequel au moins deux blocs d'alimentation sont actifs, un sur chaque réseau d'alimentation, offre un bon compromis entre efficacité et disponibilité maximale pour une enceinte modulaire partiellement remplie.
- La désactivation de l'enclenchement dynamique des blocs d'alimentation (DPSE) offre la plus faible efficacité étant donné que tous les six blocs d'alimentations sont actifs et partagent la charge, entraînant une plus faible utilisation de chaque bloc d'alimentation.

Le mode Enclenchement dynamique des blocs d'alimentation peut être activé pour les trois configurations de redondance des blocs d'alimentation présentées ci-dessus : **Sans redondance**, **Redondance des blocs d'alimentation** et **Redondance de l'alimentation alternative.**

- Dans une configuration **Sans redondance** avec DPSE, le M1000e peut comporter jusqu'à cinq blocs d'alimentation à l'état **En veille**. Dans une configuration à six blocs d'alimentation (PSU), certains PSU sont mis en mode **En veille** et restent inutilisés pour améliorer l'efficacité de l'alimentation. Dans cette configuration, si vous retirez un PSU en ligne ou s'il échoue, un PSU **De secours** est mis **En ligne** ; toutefois, les PSU de secours peuvent mettre jusqu'à deux secondes pour s'activer ; certains modules de serveur peuvent donc perdre leur alimentation pendant la transition, dans la configuration **Sans redondance**.

  REMARQUE : Dans une configuration à trois blocs d'alimentation (PSU), la charge de traitement du serveur peut empêcher le passage d'un PSU au mode En veille.
- Dans une configuration avec **Redondance des blocs d'alimentation**, l'enceinte maintient toujours un bloc d'alimentation (PSU) supplémentaire allumé et marqué **En ligne**, en plus des PSU nécessaires pour alimenter l'enceinte. La consommation électrique est surveillée et il est possible de mettre en mode En veille jusqu'à quatre PSU, en fonction de la charge de traitement globale du système. Dans une configuration à six PSU, deux blocs d'alimentation (au minimum) restent toujours allumés.

  Comme une enceinte avec configuration de **Redondance des blocs d'alimentation** comporte toujours un bloc d'alimentation (PSU) supplémentaire déclenché, l'enceinte peut tolérer la perte d'un seul PSU en ligne, car elle aura quand même assez d'alimentation pour les modules de serveur installés. La perte du PSU en ligne provoque la mise en ligne d'un PSU de secours. Si plusieurs PSU échouent simultanément, cela peut provoquer la perte d'alimentation de certains modules de serveur, pendant que les PSU de secours démarrent.
- Dans la configuration de **Redondance de l'alimentation CA**, tous les blocs d'alimentation sont activés au démarrage du châssis. La consommation électrique est surveillée. Si la configuration du système et la consommation électrique le permettent, les blocs d'alimentation (PSU) basculent en mode **En veille**. Comme l'état **En ligne** des PSU d'un réseau électrique d'alimentation est le miroir de l'autre réseau, l'enceinte peut supporter la perte d'alimentation d'un réseau électrique entier sans que l'alimentation de l'enceinte ne soit coupée.

  Si les besoins d'alimentation de la configuration avec **redondance de l'alimentation CA** augmentent, certains PSU sortent du mode **En veille**. Cela maintient la configuration en miroir nécessaire pour la redondance à deux réseaux électriques.

  REMARQUE : Lorsque le mode Enclenchement dynamique des blocs d'alimentation est activé, les unités d'alimentation en veille sont mises dans l'état **En ligne** afin de récupérer de l'alimentation si la demande en alimentation augmente dans les trois modes de règles de redondance.

Configuration de redondance par défaut

La configuration de redondance par défaut d'un châssis dépend du nombre de blocs d'alimentation (PSU) qu'il contient, comme le montre le tableau suivant.

Tableau 34. Configuration de redondance par défaut

Configuration des unités d'alimentation	Règle de redondance par défaut	Paramètre par défaut d'enclenchement dynamique des unités d'alimentation
Six unités d'alimentation	Redondance de l'alimentation alternative	Désactivée
Trois unités d'alimentation	Sans redondance	Désactivée

Redondance de l'alimentation alternative

En mode de redondance CA avec six PSU, les six PSU sont toutes actives. Les trois PSU sur la gauche doivent se connecter à un réseau d'alimentation en CA, alors que les trois PSU à droite se connectent à un autre réseau d'alimentation en CA.

PRÉCAUTION : Pour éviter une panne système et pour garantir l'efficacité de la redondance d'alimentation en CA, une série équilibrée d'unités d'alimentation doit être correctement câblée pour séparer les réseaux d'alimentation en CA.

En cas de défaillance de l'un des réseaux d'alimentation alternative, les unités d'alimentation du réseau d'alimentation alternative opérationnel prennent la relève sans interruption pour les serveurs ou l'infrastructure.

PRÉCAUTION : En mode de redondance CA, il doit exister des ensembles de PSU équilibrés (au moins une PSU dans chaque réseau). Si cette condition n'est pas remplie, la redondance CA pourra ne pas être possible.

Redondance des blocs d'alimentation

Lorsque vous activez la redondance d'alimentation, l'un des blocs d'alimentation (PSU) du châssis est gardé comme bloc de secours, ce qui garantit que la panne d'un seul PSU ne provoque pas l'arrêt des serveurs ou du châssis. Le mode de redondance de l'alimentation nécessite jusqu'à quatre PSU. Les PSU supplémentaires, s'il y en a, sont utilisés pour améliorer l'efficacité de l'alimentation du système si le mode DPSE est activé. Après la perte de la redondance, les échecs suivants peuvent provoquer l'arrêt des serveurs du châssis.

Sans redondance

Une alimentation excédant l'alimentation nécessaire pour le châssis est disponible, même lors d'une panne, afin que le châssis continue d'être alimenté.

PRÉCAUTION : Le mode Sans redondance utilise les unités de bloc d'alimentation (PSU) de façon optimale si DPSE est activé, afin de répondre aux besoins du châssis. L'échec d'une seule PSU peut provoquer la perte de l'alimentation des serveurs et générer une perte de données.

Bilan de puissance pour les modules matériels

CMC offre un service d'établissement d'un bilan de puissance qui vous permet de configurer le bilan de puissance, la redondance et l'alimentation dynamique du châssis.

Le service de gestion de l'alimentation permet l'optimisation de la consommation électrique et la réattribution de l'alimentation aux différents modules en fonction de la demande.

La figure suivante montre un châssis contenant six blocs d'alimentation (PSU) numérotés de 1 à 6 à partir de la gauche de l'enceinte.

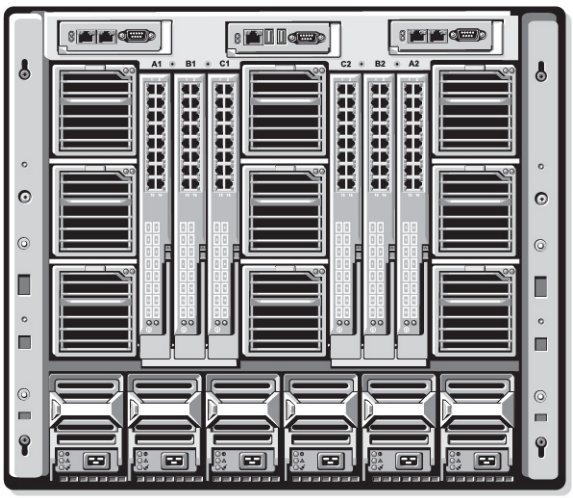


Figure 8. Châssis avec six PSU

CMC maintient un bilan de puissance de l'enceinte qui réserve la puissance nécessaire pour tous les serveurs et composants installés.

CMC alloue de la puissance à l'infrastructure CMC et aux serveurs du châssis. L'infrastructure CMC regroupe les composants du châssis, notamment les ventilateurs, les modules d'E/S (IOM) et le module iKVM (s'il est présent). Le châssis peut contenir jusqu'à 16 serveurs, qui communiquent avec le châssis via l'iDRAC. Pour plus d'informations, voir le manuel « *iDRAC7 User's Guide* » (Guide d'utilisation d'iDRAC7), à l'adresse **support.dell.com/manuals**.

L'iDRAC fournit à CMC l'enveloppe de puissance dont il a besoin, avant d'allumer le serveur. L'enveloppe de puissance est déterminée par les niveaux de puissance minimal et maximal nécessaires pour garantir le bon fonctionnement du serveur. L'estimation initiale de l'iDRAC repose sur sa connaissance initiale des composants du serveur. Une fois le système en fonctionnement, des composants supplémentaires sont détectés, et l'iDRAC peut augmenter ou réduire les besoins d'alimentation par rapport aux valeurs initiales.

Lorsqu'un serveur est allumé dans une enceinte, le logiciel iDRAC refait une estimation des besoins en alimentation et demande la modification de l'enveloppe de puissance en conséquence.

CMC attribue la puissance demandée au serveur et la quantité de watts allouée est déduite du bilan total disponible. Lorsque la demande d'alimentation d'un serveur est satisfaite, le logiciel iDRAC de ce serveur surveille en permanence la consommation électrique réelle. L'enveloppe de puissance iDRAC peut évoluer au fil du temps en fonction des besoins réels d'alimentation. L'iDRAC demande une augmentation de la puissance uniquement si les serveurs consomment l'intégralité de la puissance allouée.

Si la charge de traitement est trop importante, les performances des processeurs du serveur peuvent être dégradées pour garantir que la consommation d'énergie reste inférieure à la *limite de puissance d'entrée système* configurée par l'utilisateur.

L'enceinte PowerEdge M1000e peut fournir suffisamment de puissance pour des performances optimales dans la plupart des configurations de serveur, mais de nombreuses configurations ne consomment pas la puissance maximale disponible dans l'enceinte. Pour aider les centres de données à provisionner les enceintes, le M1000e vous permet de définir une *limite de puissance d'entrée système* afin de garantir que la consommation électrique CA globale du système reste sous le seuil défini. CMC vérifie d'abord qu'il y a suffisamment de puissance pour faire fonctionner les ventilateurs, les modules d'E/S (IOM), l'iKVM (s'il est présent) et CMC lui-même. Cette allocation de puissance est appelée *puissance d'entrée allouée à l'infrastructure de châssis*. Après l'infrastructure de châssis, les serveurs de l'enceinte sont allumés. Toute tentative de définition d'une *limite de puissance d'entrée système* inférieure à la consommation réelle échoue.

Si nécessaire, pour que le bilan de puissance total reste inférieur à la valeur *Limite de la puissance d'entrée système*, CMC alloue aux serveurs une puissance inférieure à celle qu'ils demandent. L'allocation de puissance aux serveurs

repose sur le paramètre *Priorité des serveurs*. Les serveurs avec la priorité maximale reçoivent le maximum de puissance, les serveurs de priorité 2 sont alimentés après les serveurs de priorité 1, etc. Les serveurs de priorité faible peuvent obtenir moins de puissance que les serveurs de priorité 1, en fonction de la *capacité de puissance maximale d'entrée du système* et du paramètre de *limite de puissance d'entrée système* défini par l'utilisateur.

Les changements de configuration, comme l'ajout d'un serveur dans le châssis, peuvent entraîner une augmentation de la *limite de puissance d'entrée système*. Les besoins d'alimentation d'une enceinte modulaire augmentent également lors d'un changement de température, lorsque les ventilateurs doivent tourner plus rapidement, ce qui provoque une consommation électrique supplémentaire. L'insertion de modules d'E/S ou iKVM peut également augmenter les besoins d'alimentation de l'enceinte modulaire. Les serveurs consomment relativement peu d'énergie, même s'ils sont arrêtés pour garantir que le contrôleur de gestion reste allumé.

Vous ne pouvez allumer des serveurs supplémentaires dans l'enceinte modulaire que si la puissance disponible est suffisante. Vous pouvez à tout moment augmenter la *limite de puissance d'entrée système*, jusqu'à un maximum de 16 685 watts pour permettre l'allumage de serveurs supplémentaires.

Les changements dans l'enceinte modulaire permettant de réduire l'allocation de puissance sont :

- Mise hors tension du serveur
- Serveur
- Module d'E/S
- Suppression du module iKVM
- Transition du châssis à un état hors tension

Vous pouvez reconfigurer la *limite de la puissance d'entrée système* lorsque le châssis est sous ou hors tension.

Paramètres de priorité de l'alimentation des logements du serveur

CMC vous permet de définir la priorité d'alimentation de chacun des seize logements d'une enceinte. Les paramètres de priorité vont de 1 (le plus élevé) à 9 (le plus faible). Ces paramètres sont attribués aux logements du châssis et tout serveur inséré dans un logement hérite de la priorité de ce logement. CMC utilise la priorité de logement pour allouer la puissance d'alimentation aux serveurs de l'enceinte dont le niveau de priorité est le plus élevé.

Avec le paramètre par défaut de priorité des logements de serveur, la puissance est répartie également entre tous les logements. La modification des priorités de logement permet aux administrateurs de hiérarchiser les serveurs auxquels donner la priorité pour l'allocation d'alimentation. Si les modules de serveur les plus critiques sont maintenus au niveau de priorité de logement par défaut (priorité 1) et si vous basculez les modules de serveur moins importants vers un niveau de priorité plus faible (2 ou plus), les modules de priorité 1 sont allumés en premier. Ces serveurs de priorité élevée obtiennent l'allocation de puissance maximale, alors que les serveurs de priorité faible risquent de recevoir une puissance insuffisante pour fonctionner avec des performances optimales. Ils peuvent même ne pas s'allumer du tout, selon la valeur de limite de puissance d'entrée système et des besoins d'alimentation des serveurs.

Si un administrateur allume manuellement des modules de serveur de priorité faible avant les modules de priorité élevée, les modules de priorité faible sont les premiers dont l'allocation de puissance est réduite à la valeur minimale, pour donner la préférence aux serveurs de priorité élevée. Par conséquent, une fois la puissance disponible pour allocation entièrement consommée, CMC récupère de la puissance auprès des serveurs de priorité inférieure ou égale, jusqu'à ce qu'ils atteignent le niveau d'alimentation minimal.

REMARQUE : Les modules d'E/S (IOM), les ventilateurs et l'iKVM (s'il est présent) reçoivent la priorité la plus élevée. CMC récupère de la puissance uniquement auprès des périphériques de priorité faible, pour répondre aux besoins d'alimentation d'un module ou serveur de priorité élevée.

Affectation de niveaux de priorité aux serveurs

Les niveaux de priorité déterminent les serveurs qui doivent alimenter le contrôleur CMC lorsqu'il a besoin de puissance supplémentaire.

REMARQUE : La priorité attribuée à un serveur est liée à son emplacement, et pas au serveur lui-même. Si vous placez le serveur dans un autre logement, vous devez reconfigurer la priorité pour le nouveau logement.

REMARQUE : Vous devez disposer du privilège **Administrateur de configuration du châssis** pour effectuer des tâches de gestion de l'alimentation.

Affectation de niveaux de priorité aux serveurs à l'aide de l'interface Web du CMC

Pour affecter des niveaux de priorité à l'aide de l'interface Web du CMC :

1. Dans l'arborescence, allez à **Présentation du serveur**, puis cliquez sur **Alimentation** → **Priorité**.

   La page **Priorité des serveurs** affiche tous les serveurs du châssis.
2. Sélectionnez un niveau de priorité (1–9, où 1 est la priorité la plus élevée) pour un ou plusieurs serveurs ou pour tous les serveurs. La valeur par défaut est 1. Vous pouvez affecter le même niveau de priorité à plusieurs serveurs.
3. Cliquez sur **Appliquer** pour enregistrer vos modifications.

Affectation de niveaux de priorité aux serveurs avec RACADM

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

```
racadm config -g cfgServerInfo -o cfgServer Priority -i <numéro de logement>
<niveau de priorité>
```

où <*numéro de logement*> (de 1 à 16) correspond au logement du serveur, et <*niveau de priorité*> est une valeur comprise entre 1 et 9.

Par exemple, pour définir le niveau de priorité 1 pour le serveur installé dans le logement 5, entrez la commande suivante :

```
racadm config -g cfgServerInfo -o cfgServer Priority -i 5 1
```

Affichage de la condition de la consommation électrique

CMC fournit la consommation électrique d'entrée réelle de l'ensemble du système.

Affichage de la condition de la consommation énergétique à l'aide de l'interface Web du CMC

Pour afficher la condition de la consommation énergétique à l'aide de l'interface Web du CMC, dans l'arborescence allez à **Présentation du châssis**, puis cliquez sur **Alimentation** → **Surveillance de l'alimentation** . La page Surveillance de l'alimentation affiche l'intégrité de l'alimentation, la condition de l'alimentation du système, les statistiques d'alimentation en temps réel et les statistiques énergétiques en temps réel. Pour en savoir plus, voir l'*Aide en ligne du CMC*.

REMARQUE : Vous pouvez également afficher la condition de la redondance de l'alimentation sous Blocs d'alimentation dans l'**onglet Condition** → **Arborescence système**.

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 la condition du bilan de puissance

Vous pouvez afficher l'état du bilan de puissance avec l'interface Web CMC ou RACADM.

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

Pour afficher l'état du bilan de puissance avec l'interface Web CMC, accédez à l'arborescence système, puis à **Présentation du châssis** et cliquez sur **Alimentation** → **Condition du bilan de puissance**. La page **Condition du bilan de puissance** affiche la configuration de stratégie d'alimentation du système, les détails du bilan de puissance, l'alimentation allouée aux modules de serveur et les détails des blocs d'alimentation du châssis. Pour plus d'informations, voir l'*Aide en ligne CMC*.

Affichage de l'état du bilan de puissance avec RACADM

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

```
racadm getpbinfo
```

Pour plus d'informations sur la commande **getpbinfo**, y compris les détails de sortie, voir la section traitant de la commande **getpbinfo** dans le manuel « *RACADM Command Line Reference Guide for iDRAC6 and CMC* » (Guide de référence de la ligne de commande RACADM d'iDRAC6 et de CMC).

Condition de la redondance et intégrité énergétique globale

L'état de redondance est un facteur déterminant dans l'intégrité d'alimentation globale. Par exemple, si vous définissez la stratégie de redondance sur Redondance de l'alimentation alternative et si l'état 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 d'alimentation CA redondante, l'état 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 : 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 alternative. Ainsi, la configuration de la stratégie de redondance peut provoquer une perte ou un rétablissement instantané de la redondance.

Liens connexes

- Défaillance d'une unité d'alimentation avec règle de redondance dégradée ou absente
- Retraits d'unités d'alimentation avec règle de redondance dégradée ou absente
- Règle d'enclenchement d'un nouveau serveur
- Modifications d'alimentation et de la règle de redondance dans le journal des événements système

Défaillance d'une unité d'alimentation avec règle de redondance dégradée ou absente

CMC réduit l'alimentation des serveurs en cas d'événements de puissance insuffisante, comme lors d'une panne d'un bloc d'alimentation (PSU). Après la réduction de la puissance des serveurs, CMC réévalue les besoins d'alimentation du châssis. Si ces besoins restent insatisfaits, CMC éteint les serveurs de priorité inférieure.

La puissance des serveurs de priorité élevée est restaurée par incréments, tant que les besoins d'alimentation restent dans le bilan alloué. Pour définir la stratégie de redondance, voir « Configuration du bilan d'alimentation et de la redondance ».

Retraits d'unités d'alimentation avec règle de redondance dégradée ou absente

CMC peut commencer à faire des économies d'énergie lorsque vous retirez un bloc d'alimentation (PSU) ou le câble CA correspondant. CMC réduit l'alimentation des serveurs de priorité faible jusqu'à ce que l'allocation de puissance soit prise en charge par les PSU restant dans le châssis. Si vous retirez plusieurs PSU, CMC évalue à nouveau les besoins en alimentation lors du retrait du deuxième PSU, afin de déterminer la réponse du micrologiciel. Si les besoins en alimentation ne sont pas satisfaits, CMC peut éteindre les serveurs de priorité faible.

Limites

- CMC ne prend pas en charge l'arrêt *automatisé* d'un serveur à priorité inférieure en vue de permettre la mise sous tension d'un serveur à priorité supérieure. Ce type d'arrêt peut néanmoins être exécuté à l'initiative d'un utilisateur.
- Les modifications de la stratégie de redondance des PSU sont limitées par le nombre de PSU du châssis. Vous pouvez sélectionner n'importe lequel des trois paramètres de configuration de redondance des PSU figurant dans la zone Configuration de redondance par défaut.

Règle d'enclenchement d'un nouveau serveur

Lorsqu'un nouveau serveur est allumé, CMC peut être amené à réduire la puissance des serveurs de priorité inférieure pour en attribuer davantage au nouveau serveur, si son ajout provoque un dépassement de la puissance disponible pour le châssis. Cela peut se produire si l'administrateur a configuré pour le châssis une limite de puissance inférieure à la quantité nécessaire pour une allocation de puissance complète aux serveurs, ou bien si la puissance disponible est insuffisante pour le cas le plus défavorable pour les besoins d'alimentation de tous les serveurs du châssis. S'il est impossible de libérer de la puissance en réduisant celle allouée aux serveurs de priorité inférieure, le nouveau serveur risque de ne pas être autorisé à s'allumer.

La quantité la plus élevée de puissance continue nécessaire pour faire fonctionner le châssis et tous les serveurs, y compris le nouveau, à puissance optimale est appelée cas le plus défavorable pour les besoins d'alimentation. Si cette quantité de puissance est disponible, aucun serveur ne reçoit une allocation de puissance inférieure au cas le plus défavorable et le nouveau serveur est autorisé à s'allumer.

Lorsque le cas le plus défavorable pour les besoins d'alimentation ne peut être résolu, l'alimentation est réduite sur les serveurs à priorité inférieure jusqu'à ce qu'une quantité suffisante soit libérée pour mettre sous tension le nouveau serveur.

Le tableau suivant indique les opérations réalisées par CMC lorsqu'un serveur est allumé selon le scénario décrit plus haut.

Tableau 35. Réponse de CMC lors de la tentative d'allumage d'un serveur

L'alimentation du cas le plus défavorable est disponible	Prise en charge par CMC	Allumage du serveur
Oui	La préservation de l'alimentation n'est pas nécessaire	Autorisé
Non	Passage en mode d'économie d'énergie : • L'alimentation nécessaire au nouveau serveur est disponible • L'alimentation nécessaire au nouveau serveur n'est pas disponible.	Autorisé Non autorisé

Si un bloc d'alimentation (PSU) échoue, le système passe à l'état d'erreur d'intégrité non critique et un événement d'échec de PSU est généré. Le retrait d'un PSU provoque un événement de retrait de PSU.

Si l'un des deux événements provoque une perte de redondance, selon les allocations d'alimentation, un événement de *perte de redondance* est généré.

Si la capacité d'alimentation qui suit (ou celle définie par l'utilisateur) dépasse les allocations des serveurs, ces derniers voient leurs performances diminuer ou, au pire, s'arrêtent. Ces deux événements se produisent dans l'ordre inverse des priorités : les serveurs de priorité la plus faible sont arrêtés en premier.

Le tableau suivant montre la réponse du micrologiciel en cas d'arrêt ou de retrait d'un bloc d'alimentation (PSU) dans le cadre de différentes configurations de redondance des blocs d'alimentation.

Tableau 36. Impact de l'échec ou du retrait d'un bloc d'alimentation sur le châssis

Configuration des unités d'alimentation	Enclenchement dynamique des unités d'alimentation	Prise en charge par le micrologiciel
Redondance de l'alimentation alternative	Désactivée	CMC vous alerte lors de la perte de redondance d'alimentation alternative.
Redondance des blocs d'alimentation	Désactivée	CMC vous alerte lors de la perte de redondance des blocs d'alimentation.
Sans redondance	Désactivée	Réduit l'alimentation des serveurs à priorité inférieure (le cas échéant).
Redondance de l'alimentation alternative	Activé	CMC vous avertit de la perte de la redondance d'alimentation CA. Les PSU en mode veille (s'il y en a) sont allumés pour compenser la perte de bilan d'alimentation dû à l'échec ou au retrait d'un PSU.
Redondance des blocs d'alimentation	Activé	CMC vous avertit de la perte de la redondance des blocs d'alimentation (PSU). Les PSU en mode veille (s'il y en a) sont allumés pour compenser la perte de bilan d'alimentation dû à l'échec ou au retrait d'un PSU.
Sans redondance	Activé	Réduit l'alimentation des serveurs à priorité inférieure (le cas échéant).

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 37. Événements du journal SEL relatifs aux modifications des blocs d'alimentation

Événement d'alimentation	Entrée du journal d'événements système (SEL)
Insertion	La présence d'un bloc d'alimentation a été confirmée.
Retrait	La présence d'un bloc d'alimentation a été déconfirmée.
Alimentation alternative reçue	La perte de l'entrée d'alimentation a été déconfirmée.
perte de l'alimentation alternative	La perte de l'entrée d'alimentation a été confirmée.
sortie CC produite	La panne d'un bloc d'alimentation a été déconfirmée.
perte de sortie en CC	La panne d'un bloc d'alimentation a été confirmée.
Fonctionnement 110 V non reconnu détecté	L'entrée d'alimentation basse tension (110) a été confirmée.
Fonctionnement 110 V reconnu	L'entrée d'alimentation basse tension (110) a été déconfirmée.

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 modulaire configurée avec la stratégie d'alimentation **Redondance de l'alimentation alternative** ou **Redondance des blocs d'alimentation**. Le tableau suivant répertorie les entrées SEL liées aux modifications de la redondance d'alimentation.

Événement de stratégie d'alimentation	Entrée du journal d'événements système (SEL)
Perte de la redondance	La perte de redondance a été confirmée.
Regain de la redondance	La perte de redondance a été déconfirmée.

Configuration du bilan d'alimentation et de la redondance

Vous pouvez configurer le bilan de puissance, la redondance et l'alimentation dynamique de l'ensemble du châssis (châssis, serveurs, modules d'E/S (IOM), iKVM, CMC et blocs d'alimentation), qui utilise six blocs d'alimentation (PSU). Le service de gestion de l'alimentation optimise la consommation électrique 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
- Performances du serveur avant redondance de l'alimentation
- Activer l'enclenchement dynamique des blocs d'alimentation
- Désactiver le bouton d'alimentation du châssis
- Autoriser les opérations 110 V CA
- Mode d'économie d'énergie maximum
- Journalisation distante de l'alimentation
- Intervalle de journalisation distante de l'alimentation
- Gestion de l'alimentation basée sur le serveur

Liens connexes

Économie d'énergie et bilan de puissance
Mode de conservation de puissance maximale
Réduction de l'alimentation des serveurs afin de préserver le bilan d'alimentation

Économie d'énergie et bilan de puissance

CMC réalise des économies d'énergie lorsque le système atteint la limite de puissance maximale configurée par l'utilisateur. Lorsque la demande d'alimentation dépasse la valeur Limite de la puissance d'entrée système définie par l'utilisateur, CMC réduit l'alimentation des serveurs, dans l'ordre inverse des priorités, pour libérer de la puissance pour les serveurs et autres modules de priorité élevée installés dans le châssis.

Si plusieurs logements du châssis (ou tous) sont configurés avec le même niveau de priorité, CMC réduit l'alimentation des serveurs dans l'ordre croissant des numéros de logement. Par exemple, si les serveurs des logements 1 et 2 ont le même niveau de priorité, l'alimentation du serveur du logement 1 est réduite avant celle du serveur du logement 2.

REMARQUE : Vous pouvez attribuer un niveau de priorité à chaque serveur du châssis, en associant les numéros 1 à 9 à chaque serveur. Le niveau de priorité par défaut pour tous les serveurs est 1. Plus le numéro est faible, plus le niveau de priorité est élevé.

Le bilan de puissance est limité à un maximum, égal à la puissance de l'ensemble de trois blocs d'alimentation (PSU) le plus faible. Si vous tentez de définir une valeur de puissance d'alimentation CA dépassant la valeur *Limite de la puissance d'entrée système*, CMC affiche un message d'erreur. Le bilan de puissance est limité à 16 685 Watts.

Mode de conservation de puissance maximale

CMC assure la conservation de la puissance maximale lorsque :

- Le mode de conservation de puissance maximale est activé.
- Un script de ligne de commande automatisé, émis par un onduleur, sélectionne le mode de conservation maximale.

En mode de conservation de puissance maximale, tous les serveurs commencent à fonctionner avec leur niveau de puissance minimal et toute demande d'allocation supplémentaire de puissance aux serveurs est refusée. Dans ce mode, les performances des serveurs allumés peuvent être dégradées. Il est impossible d'allumer des serveurs supplémentaires, quelle que soit leur priorité.

Le système revient à ses performances optimales lorsque vous désactivez le mode de conservation de puissance maximale.

Réduction de l'alimentation des serveurs afin de préserver le bilan d'alimentation

CMC réduit l'allocation de puissance des serveurs de priorité faible lorsqu'il a besoin de plus de puissance pour maintenir la consommation électrique du système sous la *limite de puissance d'entrée système* définie par l'utilisateur. Par exemple, lors de la mise en place d'un nouveau serveur, CMC peut réduire l'alimentation des serveurs de priorité faible pour en attribuer davantage au nouveau serveur. Si la puissance d'alimentation reste insuffisante après réduction de l'allocation de puissance des serveurs de priorité faible, CMC réduit les performances des serveurs jusqu'à libérer suffisamment de puissance pour alimenter le nouveau serveur.

CMC réduit l'allocation d'alimentation des serveurs dans deux cas :

- La consommation électrique globale dépasse la *limite de puissance d'entrée système* configurable.

- Une panne d'alimentation survient dans le cadre d'une configuration non redondante

Fonctionnement d'alimentation CA des blocs d'alimentation (PSU) 110 V

Certains blocs d'alimentation (PSU) prennent en charge le fonctionnement avec une entrée 110 VCA. Cette entrée peut dépasser la limite autorisée pour le circuit de branchement. Si des PSU sont connectés en 110 VCA, l'utilisateur doit configurer CMC pour le fonctionnement normal de l'enceinte. S'il ne le fait pas et si des PSU 110 V sont détectés, toutes les demandes d'allocation de puissance aux serveurs qui suivent sont refusées. Dans ce cas, il est impossible d'allumer des serveurs supplémentaires, quel que soit leur niveau de priorité. Vous pouvez configurer CMC pour utiliser des PSU 110 V avec l'interface Web ou avec RACADM.

Des entrées liées aux blocs d'alimentation sont journalisées dans le journal SEL :

- Lorsque des blocs d'alimentation 110 V sont détectés ou retirés.
- Lorsque le fonctionnement sur entrée 110 VCA est activé ou désactivé.

L'intégrité globale de l'alimentation a l'état Non critique ou supérieur si le châssis fonctionne en mode 110 V et si l'utilisateur n'a pas activé le fonctionnement en 110 V. L'icône « Avertissement » s'affiche dans la page principale de l'interface Web lorsque le système a l'état Non critique.

Le fonctionnement mixte 110 V et 220 V n'est pas pris en charge. Si CMC détecte que vous utilisez les deux tensions, une seule tension est sélectionnée, et les blocs d'alimentation connectés avec l'autre sont éteints et marqués En échec.

Performances du serveur avant redondance de l'alimentation

Lorsque vous l'activez, cette option favorise les performances et l'allumage des serveurs, aux dépens du maintien de la redondance d'alimentation. Lorsque vous désactivez l'option, le système favorise la redondance de l'alimentation, au prix d'une réduction des performances des serveurs. Si l'option est désactivée et que les blocs d'alimentation du châssis ne fournissent pas suffisamment de puissance pour garantir à la fois la redondance et des performances optimales, alors, pour préserver la redondance, certains serveurs :

- ne reçoivent pas assez de puissance pour des performances optimales ;
- Sous tension

Journalisation distante

Vous pouvez générer un rapport de la consommation électrique sur un serveur syslog distant. Il est possible de journaliser la consommation électrique totale du châssis, ainsi que la consommation minimale, maximale et moyenne sur une période donnée. Pour plus d'informations sur l'activation de cette fonction et sur la configuration de l'intervalle de collecte/journalisation, voir les sections correspondantes ci-après.

Gestion externe de l'alimentation

Vous pouvez, si vous le souhaitez, contrôler la gestion d'alimentation du CMC à l'aide de la console PM3 (Power Measure, Mitigate, and Manage Console, console de mesure, d'économie et de gestion de l'alimentation). Pour plus d'informations, voir le manuel « *PM3 User's Guide* » (Guide d'utilisation de PM3).

Lorsque la gestion externe d'alimentation est activée, PM3 gère :

- Alimentation serveur des serveurs de 12e génération
- Priorité des serveurs 12e génération
- Capacité maximale de l'alimentation d'entrée du système

- Mode de conservation de puissance maximale

Le CMC continue à maintenir et à gérer :

- Règle de redondance
- Journalisation distante de l'alimentation
- Performance du serveur contre redondance de l'alimentation
- Enclenchement dynamique des blocs l'alimentation
- Alimentation serveur de serveurs de 11e génération et antérieure

PM3 gère ensuite les niveaux de priorité et l'alimentation des serveurs lames 12e génération du châssis, à l'aide de la puissance disponible après allocation de puissance à l'infrastructure de châssis et aux serveurs lames de génération précédente. La journalisation de l'alimentation à distance n'est pas affectée par la gestion externe de l'alimentation.

Après l'activation du mode Gestion de l'alimentation basée sur le serveur, le châssis est préparé pour la gestion par PM3. Tous les serveurs 12e génération sont configurés sur le niveau de priorité 1 (Élevé). PM3 gère directement l'alimentation et le niveau de priorité des serveurs. Comme PM3 contrôle l'allocation de puissance aux serveurs compatibles, CMC ne contrôle plus le mode Conservation de puissance maximale. Par conséquent, cette option est désactivée.

Lorsque vous activez le mode Conservation de puissance maximale, le CMC définit la capacité de puissance en entrée du système sur le maximum que le châssis peut gérer. Le CMC interdit tout dépassement de la capacité de puissance maximale. Toutefois, PM3 gère toutes les autres limitations de capacité de puissance.

Lorsque la gestion de l'alimentation PM3 est désactivée, le CMC revient à l'état des paramètres de priorité du serveur avant l'activation de la gestion externe.

REMARQUE : Si vous désactivez la gestion PM3, le CMC ne revient pas au paramètre de puissance de châssis maximale précédent. Ouvrez le **journal CMC** pour connaître le paramètre précédent et restaurer manuellement cette valeur.

Configuration du bilan de puissance et de la redondance avec l'interface Web CMC

REMARQUE : Vous devez disposer du privilège **Administrateur de configuration du châssis** pour effectuer des tâches de gestion de l'alimentation.

Pour configurer le bilan de puissance à l'aide de l'interface Web :

1. Dans l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **Alimentation** → **Configuration**.
   La page **Configuration du bilan/de la redondance** s'affiche.
2. Sélectionnez certaines propriétés ou toutes, selon vos besoins. Pour plus d'informations sur chaque champ, voir l'*aide en ligne CMC*.
   - Activation de la Gestion de l'alimentation basée sur le serveur
   - Limite de la puissance d'entrée système
   - Règle de redondance
   - Performances du serveur avant redondance de l'alimentation
   - Activer l'enclenchement dynamique des blocs d'alimentation
   - Désactiver le bouton d'alimentation du châssis
   - Autoriser les opérations 110 V CA
   - Mode d'économie d'énergie maximum
   - Activation de la journalisation d'alimentation à distance
   - Intervalle de journalisation distante de l'alimentation
3. Cliquez sur **Appliquer** pour enregistrer les modifications.

Configuration du bilan de puissance et de la redondance à l'aide de RACADM

REMARQUE : Vous devez disposer du privilège **Administrateur de configuration du châssis** pour effectuer des 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 <valeur>
     ```
     où <valeur> est 0 (Sans redondance), 1 (Redondance de l'alimentation alternative), 2 (Redondance des blocs d'alimentation). La valeur par défaut est 0.

     Par exemple, la commande suivante définit la stratégie de redondance sur 1 :
     ```
     racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy 1
     ```
   - Pour définir la valeur de bilan de puissance, entrez :
     ```
     racadm config -g cfgChassisPower -o cfgChassisPowerCap <valeur>
     ```
     où <*valeur*> est un nombre compris entre 2 715 et 16 685 qui représente la limite d'alimentation maximale en watts. La valeur par défaut est 16 685.

     Par exemple, la commande suivante définit le bilan de puissance maximal sur 5 400 watts :
     ```
     racadm config -g cfgChassisPower -o cfgChassisPowerCap 5400
     ```
     .
   - Pour activer ou désactiver l'enclenchement dynamique des unités d'alimentation, entrez la commande :
     ```
     racadm config -g cfgChassisPower -o
     cfgChassisDynamicPSUEngagementEnable <valeur>
     ```
     où <valeur> est 0 (désactiver), 1 (activer). La valeur par défaut est 0.

     Par exemple, la commande suivante désactive le déclenchement dynamique des blocs d'alimentation (PSU) :
     ```
     racadm config -g cfgChassisPower -o
     cfgChassisDynamicPSUEngagementEnable 0
     ```
     .
   - 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
     ```
   - Activer les unités d'alimentation 110 VCA :
     ```
     racadm config -g cfgChassisPower -o cfgChassisAllow110VACOperation 1
     ```
   - Activer Performance du serveur contre redondance de l'alimentation :
     ```
     racadm config -g cfgChassisPower -o
     cfgChassisPerformanceOverRedundancy 1
     ```
   - Désactiver la fonction Performances du serveur contre redondance de l'alimentation :
     ```
     racadm config -g cfgChassisPower -o
     cfgChassisPerformanceOverRedundancy 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 de la configuration préalable des hôtes syslog distants. Vous devez activer la journalisation sur un ou plusieurs hôtes syslog distants. Sinon, la consommation électrique n'est pas journalisée. Vous pouvez effectuer l'opération dans l'interface utilisateur graphique (GUI) Web ou dans l'interface de ligne de commande (CLI) RACADM. Pour plus d'informations, voir les instructions de configuration des journaux syslog distants.

- Pour activer la gestion de l'alimentation à distance avec PM3, entrez :

  ```
  racadm config -g cfgChassisPower -o cfgChassisServerBasedPowerMgmtMode
  1
  ```

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

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

Pour plus d'informations sur les commandes RACADM relatives à l'alimentation du châssis, voir les sections **config**, **getconfig**, **getpbinfo** et **cfgChassisPower** dans le manuel « *RACADM Command Line Reference Guide for iDRAC6 and CMC* » (Guide de référence de la ligne de commande RACADM pour iDRAC6 et CMC).

Exécution d'opérations de contrôle de l'alimentation

Vous pouvez exécuter les opérations de contrôle de l'alimentation suivantes pour le châssis, les serveurs et les IOM.

REMARQUE : Les opérations de contrôle de l'alimentation affectent l'intégralité du châssis.

Liens connexes

Exécution d'opérations de contrôle de l'alimentation sur le châssis
Exécution d'opérations de contrôle de l'alimentation sur un serveur
Exécution d'opérations de contrôle de l'alimentation sur un module d'E/S (IOM)

Exécution d'opérations de contrôle de l'alimentation sur le châssis

CMC vous permet d'exécuter à distance plusieurs opérations de gestion de l'alimentation, comme une séquence d'arrêt correcte, sur l'ensemble du châssis (châssis, serveurs, modules d'E/S, iKVM et unités d'alimentation).

REMARQUE : Vous devez disposer du privilège **Administrateur de configuration du châssis** pour effectuer des opérations de gestion de l'alimentation.

Exécution d'opérations de contrôle de l'alimentation sur le châssis avec l'interface Web

Pour exécuter des opérations de contrôle de l'alimentation sur le châssis avec l'interface Web CMC :

1. Dans l'arborescence système, accédez à **Présentation du châssis** et cliquez sur **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 CMC*.
   - 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 vous invite à confirmer l'opération.
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 pour valeur powerup (allumage), powerdown (extinction), powercycle (cycle d'alimentation), nongraceshutdown (arrêt anormal) ou reset (réinitialisation).

Exécution d'opérations de contrôle de l'alimentation sur un serveur

Vous pouvez exécuter à distance des opérations de gestion de l'alimentation pour plusieurs serveurs simultanément ou pour un seul serveur d'un châssis.

REMARQUE : Vous devez disposer du privilège **Administrateur de configuration du châssis** pour effectuer des tâches de gestion de l'alimentation.

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 l'arborescence système, accédez à **Présentation du serveur** et cliquez sur **Alimentation** → **Contrôle**.
   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
   - Mettre le serveur sous tension
   - Mettre le serveur hors tension
   - Arrêt normal
   - Réinitialiser le serveur (redémarrage à chaud)
   - Exécuter un cycle d'alimentation sur le serveur (redémarrage à froid)

   Pour plus d'informations sur les options, voir l'*Aide en ligne CMC*.
3. Cliquez sur **Appliquer**.
   Une boîte de dialogue vous invite à confirmer l'opération.
4. Cliquez sur **OK** pour lancer la tâche de gestion de l'alimentation (réinitialisation du serveur, par exemple).

Exécution d'opérations de contrôle de l'alimentation sur un serveur avec l'interface Web CMC

Pour exécuter une opération de contrôle de l'alimentation sur un seul serveur avec l'interface Web CMC :

1. Dans l'arborescence système, accédez à **Présentation du châssis** et cliquez sur **Présentation du serveur**.
2. Cliquez sur le serveur pour lequel vous voulez exécuter l'opération de contrôle de l'alimentation, puis cliquez sur l'onglet **Alimentation**.

   La page **Gestion de l'alimentation des serveurs** s'affiche.
3. Sélectionnez l'une des opérations de contrôle de l'alimentation suivantes :

   - 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 plus d'informations sur les options, voir l'*Aide en ligne CMC*.
4. Cliquez sur **Appliquer**.

   Une boîte de dialogue vous invite à confirmer l'opération.
5. Cliquez sur **OK** pour lancer la tâche de gestion de l'alimentation (réinitialisation du serveur, par exemple).

Exécution d'opérations de contrôle de l'alimentation sur un serveur avec RACADM

Pour exécuter des opérations de contrôle de l'alimentation sur un serveur avec RACADM, ouvrez une console texte série/Telnet/SSH sur le CMC, connectez-vous et entrez :

```
racadm serveraction -m <module> <action>
```

où <*module*> désigne le serveur par son numéro de logement (serveur-1 à serveur-16) dans le châssis, et <*action*> indique l'opération à exécuter :

```
powerup (allumage), powerdown (extinction), powercycle (cycle d'alimentation),
graceshutdown (arrêt normal) ou hardreset (réinitialisation matérielle).
```

Exécution d'opérations de contrôle de l'alimentation sur un module d'E/S (IOM)

Vous pouvez exécuter à distance une opération de réinitialisation ou lancer un cycle d'alimentation sur un module d'E/S.

REMARQUE : Vous devez disposer du privilège **Administrateur de configuration du châssis** pour effectuer des tâches de gestion de l'alimentation.

Exécution d'opérations de contrôle de l'alimentation sur les IOM avec l'interface Web CMC

Pour exécuter des opérations de contrôle de puissance sur un module d'E/S à l'aide de l'interface Web CMC :

1. Dans l'arborescence système, accédez à **Présentation du châssis** → **Présentation du module d'E/S**, puis cliquez sur **Alimentation**.

   La page **Contrôle de l'alimentation** s'affiche.
2. Pour un module d'E/S (IOM) de la liste, ouvrez le menu déroulant, sélectionnez l'opération à réaliser (réinitialisation ou cycle d'alimentation).
3. Cliquez sur **Appliquer**.

   Une boîte de dialogue vous invite à confirmer l'opération.
4. Cliquez sur **OK** pour exécuter l'opération de gestion de l'alimentation (par exemple, lancer un cycle d'alimentation du module d'E/S).

Exécution d'opérations de contrôle de l'alimentation sur les modules d'E/S (IOM) avec RACADM

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

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

où <*n*> est un nombre compris entre 1 et 6 qui indique le module IOM (A1, A2, B1, B2, C1, C2) et où <action> est l'opération à exécuter : powercycle (cycle d'alimentation) ou reset (réinitialisation).

16

Dépannage et restauration

Cette section détaille les tâches de récupération et de dépannage des problèmes se produisant sur un système distant via 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.
- Journaux et codes d'erreur

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

La sous-commande `racdump` fournit une commande unique d'obtention de la condition complète du châssis, des informations sur l'état de configuration et des journaux.

La sous-commande `racdump` affiche les informations suivantes :

- informations générales sur le système/RAC
- informations sur CMC
- informations sur le châssis
- Informations sur les sessions
- Informations du capteur
- informations sur le numéro du micrologiciel

Interfaces prises en charge

- CLI RACADM
- Interface RACADM distante
- RACADM Telnet

Racdump (Vidage RAC) inclut les sous-systèmes suivants et regroupe les commandes RACADM suivantes. Pour plus d'informations sur RACADM, voir le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de l'interface de ligne de commande RACADM pour iDRAC7 et CMC).

Sous-système	Commande RACADM
Informations générales sur le système/RAC	`getsysinfo`
Informations sur les sessions	`getssinfo`
Informations du capteur	`getsensorinfo`
Informations du commutateur (module d'E/S)	`getioinfo`
Informations de la carte mezzanine (carte fille)	`getdcinfo`
Informations de tous les modules	`getmodinfo`
Informations du bilan de puissance	`getpbinfo`
Informations KVM	`getkvminfo`
Informations de NIC (module CMC)	`getniccfg`
Informations de redondance	`getredundancymode`
Information du journal de suivi	`gettracelog`
Journal des événements RAC	`gettraclog`
Journal des événements système	`getsel`

Téléchargement du fichier MIB (base d'information de gestion) SNMP

Le fichier MIB SNMP du CMC définit des types de châssis, des événements et des indicateurs. CMC vous permet de télécharger le fichier MIB avec l'interface Web.

Pour télécharger le fichier MIB (Management Information Base, base d'informations de gestion) SNMP du CMC avec l'interface Web CMC :

1. Dans l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **Réseau** → **Services** → **SNMP**.
   La section **Configuration SNMP** s'affiche.
2. Cliquez sur **Enregistrer** pour télécharger le fichier **MIB** du CMC vers votre système local.
   Pour plus d'informations sur le fichier **MIB** SNMP, voir le manuel « *Dell OpenManage Server Administrator SNMP Reference Guide* » (Guide de référence SNMP Dell OpenManage Server Administrator), à l'adresse **dell.com/support/manuals**.

Premières étapes de dépannage d'un système distant

Les questions suivantes aident souvent à dépanner les problèmes de haut niveau dans le système géré :

- Le système est-il sous tension ou hors tension ?
- S'il est allumé, est-ce que le système d'exploitation fonctionne, est-il tombé en panne ou est-il seulement bloqué ?
- S'il est hors tension, est-ce que l'alimentation a 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 : stratégie de redondance de l'alimentation** configurée sur **Redondance de l'alimentation alternative**, et un événement de perte de redondance des blocs d'alimentation est survenu.
  - **Solution A :** cette configuration nécessite au moins un bloc d'alimentation côté 1 (trois logements de gauche) et un autre côté 2 (trois logements de droite), installés et fonctionnels dans l'enceinte modulaire. De plus, la capacité de chaque côté doit être suffisante pour prendre en charge le total d'allocation de puissance nécessaire pour maintenir la **redondance d'alimentation CA** du châssis. (Pour une redondance d'alimentation CA complète, vérifiez que vous disposez d'une configuration complète avec 6 blocs d'alimentation (PSU).)
  - **Solution B :** vérifiez que tous les blocs d'alimentation sont correctement connectés aux deux réseaux électriques CA ; les blocs d'alimentation côté 1 doivent être connectés à l'un des réseaux électriques de courant alternatif, ceux du côté 2 doivent être raccordés à l'autre réseau, et les deux réseaux CA doivent fonctionner. La **redondance d'alimentation CA** est perdue si l'un des réseaux électriques CA ne fonctionne pas.
- **Problème :** l'état des blocs d'alimentation (PSU) est **En échec (Pas d'alimentation CA)**, même lorsqu'un cordon secteur est connecté et que l'unité de distribution électrique produit une sortie CA satisfaisante.
  - **Solution A :** vérifiez et remplacez le cordon d'alimentation secteur. Vérifiez que l'unité de distribution électrique (PDU) qui alimente le bloc d'alimentation fonctionne comme prévu. Si le problème persiste, contactez le service clientèle Dell pour obtenir un bloc d'alimentation de rechange.
  - **Solution B :** vérifiez que le bloc d'alimentation (PSU) est connecté avec la même tension que les autres blocs. Si CMC détecte un bloc d'alimentation avec une tension différente, le PSU est éteint et marqué comme En échec.
- **Problème :** l'enclenchement dynamique des blocs d'alimentation est activé, mais aucun des blocs d'alimentation ne s'affiche à l'état **Veille**.
  - **Solution A :** puissance excédentaire insuffisante. Un ou plusieurs blocs d'alimentation sont placés à l'état En attente uniquement lorsque le surplus de puissance disponible dans l'enceinte dépasse la capacité d'au moins un bloc d'alimentation.
  - **Solution B :** il est impossible de prendre entièrement en charge le mode DPSE (Dynamic Power Supply Engagement - Enclenchement dynamique des blocs d'alimentation) avec les blocs d'alimentation présents dans l'enceinte. Pour vérifier si tel est le cas, utilisez l'interface Web pour désactiver la fonction DPSE, puis réactivez-la. Un message s'affiche si le système ne prend pas entièrement en charge DPSE.
- **Problème :** un nouveau serveur a été inséré dans l'enceinte contenant assez de blocs d'alimentation, mais la mise sous tension du serveur ne peut s'effectuer.
  - **Solution A :** vérifiez le paramètre de limite de puissance d'entrée système ; il se peut qu'il soit configuré sur un niveau trop faible pour permettre l'allumage de serveurs supplémentaires.
  - **Solution B :** recherchez les éléments qui fonctionnent en 110 V. Si un bloc d'alimentation est connecté à un circuit de branchement 110 V, vous devez explicitement reconnaître cela comme configuration valide pour que l'allumage des serveurs soit autorisé. Pour plus d'informations, voir les paramètres de configuration de l'alimentation.
  - **Solution B :** vérifiez le paramètre de conservation de puissance maximale. Si cette valeur est définie, les serveurs sont autorisés à s'allumer. Pour plus d'informations, voir les paramètres de configuration de l'alimentation.
  - **Solution D :** vérifiez la priorité de puissance de logement de serveur correspondant au logement du serveur nouvellement inséré et veillez à ce qu'elle soit supérieure ou égale à toutes les autres priorités de puissance de logement de serveur.
- **Problème :** la puissance disponible ne cesse d'évoluer, même lorsque la configuration de l'enceinte modulaire n'a pas changé.

- **Solution :** CMC version 1.2 et supérieures intègre une fonction de gestion dynamique de l'alimentation des ventilateurs, qui réduit brièvement la puissance allouée aux serveurs si l'enceinte 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 au-dessous de la **limite de puissance d'entrée système** définie. Ce comportement est normal.

- **Problème :** la valeur 2 000 W est signalée pour le paramètre **Surplus pour un maximum de performance**.
  - **Résolution :** L'enceinte dispose de 2000 W de puissance excédentaire disponible dans la configuration actuelle, et la **limite de puissance d'entrée système** peut être réduite en toute sécurité en fonction de cette quantité signalée sans affecter les performances du serveur.
- **Problème :** un sous-ensemble de serveurs a perdu son alimentation suite à une panne du réseau électrique CA, alors que le châssis fonctionnait en mode de configuration **Redondance de l'alimentation alternative** avec six blocs d'alimentation.
  - **Solution :** cela peut se produire si les blocs d'alimentation sont mal connectés aux réseaux électriques CA redondants au moment où la panne de réseau CA se produit. La stratégie **Redondance de l'alimentation alternative** exige que les trois blocs d'alimentation (PSU) de gauche soient connectés à un circuit électrique CA et que les trois blocs d'alimentation de droite soient connectés à un autre. Si deux PSU sont mal connectés, par exemple si PSU3 et PSU4 sont connectés aux mauvais circuits électriques CA, une panne de courant d'un circuit peut provoquer la perte d'alimentation des serveurs de moindre priorité.
- **Problème :** les serveurs de priorité inférieure ne sont plus alimentés, suite à la panne d'un bloc d'alimentation (PSU).
  - **Solution :** il s'agit du comportement attendu si vous avez configuré la stratégie d'alimentation de l'enceinte sur **Sans redondance**. Pour éviter que les pannes d'alimentation futures arrêtent les serveurs, vérifiez que le châssis comporte au moins quatre blocs d'alimentation et qu'il est bien configuré pour la stratégie **Redondance des blocs d'alimentation**, afin d'éviter qu'une panne de PSU ait un impact sur le fonctionnement des serveurs.
- **Problème :** les performances globales du serveur diminuent lorsque la température ambiante augmente dans le centre de données.
  - **Solution :** cela peut se produire si vous avez défini l'option **Limite de la puissance d'entrée système** sur une valeur qui provoque une augmentation des besoins d'alimentation des ventilateurs, qui doit être compensée par une réduction de la puissance allouée aux serveurs. L'utilisateur peut configurer l'option **Limite de la puissance d'entrée système** sur une valeur plus élevée, qui permet d'allouer de la puissance supplémentaire aux ventilateurs sans aucun impact sur les performances des serveurs.

Dépannage des alertes

Utilisez le journal CMC et le journal de 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 réseau ou un outil comme l'utilitaire snmputil de Microsoft pour suivre les paquets sur le système géré.

Liens connexes

Configuration de CMC pour envoyer des alertes

Affichage des journaux d'événements

Vous pouvez afficher les journaux du matériel et du CMC pour en savoir plus sur les événements critiques qui se produisent sur le système géré.

Liens connexes

Affichage du journal du matériel

Affichage du journal CMC

Affichage du journal du matériel

CMC génère un journal du matériel pour les événements qui se produisent sur le châssis. Vous affichez ce journal avec l'interface Web ou avec RACADM.

REMARQUE : Vous devez disposer du privilège **Administrateur d'effacement des journaux** pour effacer le journal du matériel.

REMARQUE : Vous pouvez configurer CMC afin d'envoyer un e-mail ou une interruption SNMP lorsque des événements spécifiques se produisent. Pour plus d'informations sur la configuration de CMC pour l'envoi d'alertes, voir « Configuration de CMC pour envoyer des alertes ».

Exemples d'entrées du journal du matériel

```
Événement logiciel système critique : redondance perdue Mer 09 mai 2007
15:26:28 Événement logiciel système normal : effacement du journal confirmé Mer
09 mai 2007 16:06:00 Événement logiciel système d'avertissement : échec prévu
confirmé Mer 09 mai 2007 15:26:31 Événement logiciel système critique : journal
plein confirmé Mer 09 mai 2007 15:47:23 Événement logiciel système inconnu :
événement inconnu
```

Liens connexes

Affichage des journaux d'événements

Affichage des journaux du matériel avec l'interface Web CMC

Vous pouvez afficher, enregistrer et effacer le journal du matériel. Vous pouvez trier les entrées de journal sur la base des champs Gravité, Date/Heure ou Description, en cliquant sur l'en-tête de colonne approprié. Un autre clic sur l'en-tête choisi inverse le tri.

Pour afficher les journaux du matériel avec l'interface Web CMC, accédez à l'arborescence système, ouvrez **Présentation du châssis**, puis cliquez sur **Journaux → Journal du matériel**. La page **Journal du matériel** s'affiche. Pour enregistrer une copie du journal du matériel sur votre station ou votre réseau de gestion, cliquez sur **Enregistrer le journal** et spécifiez l'emplacement du fichier journal au format texte.

REMARQUE : Comme le journal est enregistré dans un fichier texte, les images utilisées pour indiquer la gravité dans l'interface utilisateur ne s'affichent pas. Dans le fichier texte, la gravité est signalée par les mots OK, Informatif, Inconnu, Avertissement et Grave. Les entrées de date et d'heure sont triées dans l'ordre croissant. Si la mention <AMORÇAGE SYSTÈME> apparaît dans la colonne **Date/Heure**, cela signifie que l'événement s'est produit pendant l'arrêt ou le démarrage de l'un des modules, lorsque l'heure et la date n'étaient pas disponibles.

Pour effacer le journal du matériel, cliquez sur **Effacer le journal**.

REMARQUE : CMC crée une nouvelle entrée du journal qui indique que celui-ci a été effacé.

Affichage des journaux du matériel avec RACADM

Pour afficher le journal du matériel avec RACADM, ouvrez une console texte série, Telnet ou SSH sur le CMC, connectez-vous, puis entrez :

```
racadm getsel
```

Pour effacer le journal du matériel, entrez :

```
racadm clrsel
```

Affichage du journal CMC

CMC génère un journal des événements liés au châssis.

REMARQUE : Pour effacer le journal CMC, vous devez disposer du privilège **Administrateur d'effacement des journaux**.

Liens connexes

Affichage des journaux d'événements

Affichage des journaux CMC avec l'interface Web

Vous pouvez afficher, enregistrer et effacer le journal CMC. Vous pouvez trier les entrées de journal sur la base des champs Source, Date/Heure ou Description, en cliquant sur l'en-tête de colonne approprié. Un autre clic sur l'en-tête choisi inverse le tri.

Pour afficher le journal CMC avec l'interface Web CMC, accédez à l'arborescence système, puis à **Présentation du châssis**. Cliquez sur **Journaux → Journal CMC**. La page **Journal CMC** s'affiche.

Pour enregistrer une copie du journal CMC sur votre station ou votre réseau de gestion, cliquez sur **Enregistrer le journal**, puis spécifiez l'emplacement d'enregistrement du fichier journal.

Affichage des journaux CMC avec RACADM

Pour afficher les informations du journal CMC avec RACADM, ouvrez une console texte série, Telnet ou SSH sur le CMC, connectez-vous, puis entrez :

```
racadm getraclog
```

Pour effacer le journal du matériel, entrez :

```
racadm clrraclog
```

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 utilisateur expert ou si vous suivez les instructions du support technique.

REMARQUE : Vous devez disposer du privilège **Administrateur de commandes de débogage** pour modifier ces paramètres.

Pour accéder à la console de diagnostic avec l'interface Web CMC :

1. Dans l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **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 CMC*.
   La page Résultats des diagnostics apparaît.

Réinitialisation des composants

Vous pouvez réinitialiser le CMC actif, réinitialiser l'iDRAC sans redémarrer le système d'exploitation, ou réinstaller virtuellement les serveurs afin qu'ils fonctionnent comme s'ils avaient été retirés et réinsérés. Si le châssis comporte un CMC de secours, la réinitialisation du CMC actif provoque un basculement et le CMC de secours devient actif.

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

Pour réinitialiser les composants avec l'interface Web CMC

1. Dans l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **Dépannage → Réinitialiser les composants**.

   La page **Réinitialiser les composants** s'affiche.

2. Pour réinitialiser le CMC actif, dans la section **État du CMC**, cliquez sur **Réinitialiser/Basculer CMC**. Si un CMC de secours est présent et que le châssis est entièrement redondant, un basculement se produit et le CMC de secours devient actif.

3. Pour réinitialiser uniquement l'iDRAC, sans redémarrer le système d'exploitation, dans la section **Réinitialiser le serveur**, cliquez sur **Réinitialiser iDRAC** dans le menu déroulant **Réinitialiser** pour les serveurs dont vous souhaitez réinitialiser l'iDRAC, puis cliquez sur **Appliquer les sélections**. Cette opération réinitialise les iDRAC des serveurs sans redémarrer le système d'exploitation.

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

   Pour réinitialiser uniquement l'iDRAC, sans redémarrer le système d'exploitation, à l'aide de RACADM, voir le manuel *« RACADM Command Line Reference Guide for iDRAC7 and CMC »* (Guide de référence de la ligne de commande RACADM pour iDRAC7 et CMC).

   REMARQUE : Lorsque l'iDRAC est réinitialisé, les ventilateurs sont configurés sur 100 % pour le serveur.

   REMARQUE : Il est recommandé d'essayer de réinitialiser l'iDRAC avant de tenter de réinstaller virtuellement les serveurs.

4. Pour réinstaller virtuellement le serveur, dans la section **Réinitialiser le serveur**, cliquez sur **Réinstallation virtuelle** dans la zone déroulante **Réinitialiser**, pour les serveurs que vous souhaitez réinstaller, puis cliquez sur **Appliquer les sélections**.

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

   Cette opération oblige les serveurs à se comporter comme s'ils avaient été retirés et réinsérés.

Enregistrement ou restauration de la configuration de châssis

Pour enregistrer la configuration de châssis ou restaurer une sauvegarde avec l'interface Web CMC :

1. Dans l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **Configuration → Sauvegarde du châssis**. La page **Sauvegarde du châssis** s'affiche.

2. Pour enregistrer la configuration de châssis, cliquez sur **Enregistrer**. Remplacez le chemin de fichier par défaut (facultatif) et cliquez sur **OK** pour enregistrer le fichier.

   REMARQUE : Le nom par défaut du fichier de sauvegarde contient le numéro de service du châssis. Vous pouvez utiliser ultérieurement ce fichier de sauvegarde pour restaurer les paramètres et certificats pour ce châssis uniquement.

3. Pour restaurer la configuration de châssis, cliquez sur **Choisir un fichier**, spécifiez 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 d'heure distant sur le réseau, il peut s'écouler 2-3 minutes avant que la date et l'heure soient modifiées. Si aucun changement ne s'est produit après ce délai, il existe peut-être un problème que vous devez corriger. 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 corriger ces problèmes, consultez les informations du journal de suivi CMC. Ce journal contient un message d'erreur pour chaque échec lié à NTP. Si le CMC ne peut se synchroniser avec aucun des serveurs NTP distants configurés, l'horloge du CMC est synchronisée avec l'horloge système locale et le journal de suivi stocke une entrée semblable à celle-ci :

```
Jan 8 20:02:40 cmc ntpd[1423] : synchronisé sur LOCAL(0), couche 10
```

Vous pouvez également vérifier la condition ntpd en tapant la commande RACADM suivante :

```
racadm getractime –n
```

Si l'astérisque (*) n'apparaît pas pour l'un des serveurs configurés, ses paramètres sont peut-être incorrects. 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] : impossible de trouver l'interface existante
pour l'adresse 1.2.3.4 Jan 8 19:59:24 cmc ntpd[1423] : la configuration de
1.2.3.4 a échoué
```

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] : nom d'hôte introuvable : blabla Aug 21
14:34:27 cmc ntpd_initres[1298] : impossible de résoudre `blabla', abandon de
l'opération
```

Pour plus d'informations sur la saisie de la commande `gettracelog` afin de vérifier le journal de suivi dans l'interface Web CMC, voir « Utilisation de la console de diagnostic ».

Interprétation des couleurs des LED et séquences de clignotement

Les LED du châssis indiquent la condition des composants par les signaux suivants :

- Une LED verte qui reste allumée signale que le composant est allumé. Si la LED verte clignote, cela signale un événement critique mais habituel, comme le téléversement d'un micrologiciel, pendant lequel l'unité n'est pas opérationnelle. Il ne s'agit pas d'une défaillance.
- Une LED orange clignotant sur un module indique une panne de ce module.
- Des LED bleues clignotantes peuvent être configurées par l'utilisateur pour l'identification (voir « Téléchargement du fichier MIB (base d'information de gestion) SNMP »).

Tableau 38. Couleur des LED et séquences de clignotement

Composant	Couleur de la LED, séquence de clignotement	Signification
CMC	Vert, continu	Sous tension
	Vert, clignotant	Micrologiciel en cours de téléversement
	Vert, foncé	Hors tension
	Bleu, continu	Actif
	Bleu, clignotant	Identificateur d'un module activé par l'utilisateur
	Orange, continu	Inutilisé
	Orange, clignotant	Panne
	Bleu, foncé	En veille
iKVM	Vert, continu	Sous tension
	Vert, clignotant	Micrologiciel en cours de téléversement
	Vert, foncé	Hors tension
	Orange, continu	Inutilisé
	Orange, clignotant	Panne
	Orange, foncé	Pas de panne
Serveur	Vert, continu	Sous tension
	Vert, clignotant	Micrologiciel en cours de téléversement
	Vert, foncé	Hors tension
	Bleu, continu	Normal
	Bleu, clignotant	Identificateur d'un module activé par l'utilisateur
	Orange, continu	Inutilisé
	Orange, clignotant	Panne

Composant	Couleur de la LED, séquence de clignotement	Signification
	Bleu, foncé	Pas de panne
Module d'E/S (courant)	Vert, continu	Sous tension
	Vert, clignotant	Micrologiciel en cours de téléversement
	Vert, foncé	Hors tension
	Bleu, continu	Normal/maître de la pile
	Bleu, clignotant	Identificateur d'un module activé par l'utilisateur
	Orange, continu	Inutilisé
	Orange, clignotant	Panne
	Bleu, foncé	Pas de panne/esclave de la pile
Module d'E/S (transfert)	Vert, continu	Sous tension
	Vert, clignotant	Inutilisé
	Vert, foncé	Hors tension
	Bleu, continu	Normal
	Bleu, clignotant	Identificateur d'un module activé par l'utilisateur
	Orange, continu	Inutilisé
	Orange, clignotant	Panne
	Bleu, foncé	Pas de panne
Ventilateur	Vert, continu	Ventilateur en marche
	Vert, clignotant	Inutilisé
	Vert, foncé	Hors tension
	Orange, continu	Type de ventilateur non reconnu, mettre à jour le micrologiciel CMC
	Orange, clignotant	Défaillance du ventilateur ; tachymètre hors de portée
	Orange, foncé	Inutilisé
le bloc d'alimentation	(Ovale) Vert, continu	Alimentation en courant alternatif OK
	(Ovale) Vert, clignotant	Inutilisé
	(Ovale) Vert, foncé	Alimentation en courant alternatif défaillante
	Orange, continu	Inutilisé
	Orange, clignotant	Panne
	Orange, foncé	Pas de panne

Composant	Couleur de la LED, séquence de clignotement	Signification
	(Cercle) Vert, continu	Alimentation en courant continu OK
	(Cercle) Vert, foncé	Alimentation en courant continu défaillante

Dépannage d'un CMC qui ne répond pas

Si vous ne pouvez pas vous connecter à CMC via l'une des interfaces (interface Web, Telnet, SSH, RACADM distant ou interface série), vous pouvez vérifier le bon fonctionnement du CMC en observant les LED du module CMC, en obtenant les informations de restauration via le port série DB-9 ou en restaurant l'image de micrologiciel CMC.

REMARQUE : Il est impossible de se connecter sur le contrôleur CMC de secours à l'aide d'une console série.

Observation des LED afin d'isoler le problème

Lorsque vous regardez le CMC de face (tel qu'il est installé dans le châssis), vous voyez deux LED du côté gauche de la carte :

- LED supérieure : la LED verte du haut indique l'alimentation. Si elle est éteinte :
  - Vérifiez qu'une alimentation secteur est présente sur au moins l'un des blocs d'alimentation.
  - Vérifiez que la carte CMC est correctement insérée. Vous pouvez libérer ou tirer le levier d'éjection, retirer le CMC, puis le réinstaller en vous assurant que la carte est bien poussée à fond et que le loquet se ferme correctement.
- LED inférieure : la LED du bas est multicolore. Lorsque le CMC est actif et en cours d'exécution sans aucun problème, la LED du bas est bleue. Elle devient orange si un échec est détecté. Il peut s'agir de l'un des trois événements suivants :
  - Échec du noyau. Vous devez alors remplacer la carte CMC.
  - Échec de l'auto-test. Vous devez alors remplacer la carte CMC.
  - Corruption de l'image. Dans ce cas, téléversez l'image du micrologiciel CMC pour restaurer le CMC.

  REMARQUE : Au cours d'un amorçage ou d'une réinitialisation standard, le CMC prend plus d'une minute pour s'amorcer entièrement dans son système d'exploitation avant d'être disponible pour la connexion. La LED bleue est activée sur le CMC actif. Dans une configuration redondante avec deux CMC, seule la LED supérieure verte est activée sur le CMC de secours.

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

Lorsque la LED inférieure est orange, des 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 câble de modem NULL entre CMC et un ordinateur client.
2. Ouvrez l'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 <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` (restaurer), puis appuyez sur <Entrée>.

Exemples d'invites :

```
recover1[self test] CMC 1 self test failure

recover2[Bad FW images] CMC2 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 de micrologiciel incorrectes**, suivez les étapes de la rubrique « Restauration de l'image de micrologiciel » pour résoudre le problème.

Restauration d'une image de micrologiciel

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, **firmimg.cmc**. Il s'agit du même fichier d'image de micrologiciel que celui utilisé pour les mises à jour normales du micrologiciel. Le processus de restauration affiche ses activités en cours et effectue l'amorçage dans le système d'exploitation du CMC lorsqu'il est terminé.

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 <adresse IP du serveur TFTP>` 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 CMC ou dans RACADM. Voir la section traitant de la commande `gettracelog` dans le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de la ligne de commande RACADM pour iDRAC7 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.

Réinitialisation du mot de passe administrateur

PRÉCAUTION : La plupart des réparations ne peuvent être effectuées que par un technicien de maintenance agréé. N'effectuez que les opérations de dépannage et les petites réparations autorisées par la documentation de votre produit et suivez les instructions fournies en ligne ou par téléphone par l'équipe de maintenance et d'assistance technique. Tout dommage causé par une réparation non autorisée par Dell est exclu de votre garantie. Consultez et respectez les consignes de sécurité fournies avec votre produit.

Pour réaliser des opérations de gestion, l'utilisateur doit disposer de privilèges **Administrateur**. Le logiciel CMC comporte une fonction de protection par mot de passe que vous pouvez désactiver si vous oubliez le mot de passe du compte d'administrateur. En cas d'oubli du mot de passe du compte d'administrateur, vous pouvez le restaurer à l'aide du cavalier PASSWORD_RSET de la carte CMC.

La carte CMC dispose d'un connecteur de réinitialisation du mot de passe à deux broches, illustré dans la figure suivante. Si vous installez un cavalier sur le connecteur de réinitialisation, le compte et le mot de passe d'administrateur par défaut sont activés, et configurés sur les valeurs par défaut, à savoir `nom d'utilisateur = root` et `mot de passe = calvin`. Le compte d'administrateur est réinitialisé même s'il avait été supprimé ou si le mot de passe avait été modifié.

REMARQUE : Assurez-vous que le module CMC est en mode passif avant de démarrer.

Pour réaliser des opérations de gestion, l'utilisateur doit disposer de privilèges **Administrateur**. En cas d'oubli du mot de passe du compte d'administrateur, vous pouvez le restaurer à l'aide du cavalier PASSWORD_RSET de la carte CMC.

Le cavalier PASSWORD_RST utilise un connecteur à deux broches comme indiqué dans la figure suivante.

Pendant que le cavalier PASSWORD_RST est installé, le compte d'administrateur et le mot de passe par défaut sont activés et définis sur les valeurs par défaut suivantes :

```
nom d'utilisateur: root
mot de passe: calvin
```

Le compte administrateur est temporairement réinitialisé, même si le compte d'administrateur a été supprimé ou si le mot de passe a été changé.

REMARQUE : Lorsque le cavalier PASSWORD_RST est installé, une configuration console en série par défaut est utilisée (plutôt que les valeurs de propriété de configuration), comme suit :

```
cfgSerialBaudRate=115200
cfgSerialConsoleEnable=1
cfgSerialConsoleQuitKey=^\
cfgSerialConsoleIdleTimeout=0
cfgSerialConsoleNoAuth=0
cfgSerialConsoleCommand=""
cfgSerialConsoleColumns=0
```

1. Appuyez sur le loquet de libération de la carte CMC, sur la poignée, et éloignez la poignée du panneau avant du module. Faites glisser le module CMC hors de l'enceinte.

   REMARQUE : Les décharges électrostatiques (ESD) peuvent endommager le CMC. Dans certaines conditions, l'électricité statique peut s'accumuler dans votre corps ou dans un objet, puis se décharger dans votre CMC. Pour éviter tout dommage, vous devez prendre des précautions afin d'évacuer l'électricité statique de votre corps lorsque vous manipulez le CMC et y accédez hors du châssis.

2. Retirez le bouchon de cavalier du connecteur de réinitialisation du mot de passe, puis insérez un cavalier à 2 broches pour activer le compte d'administrateur par défaut. Pour trouver le cavalier de mot de passe sur la carte CMC voir la figure suivante.

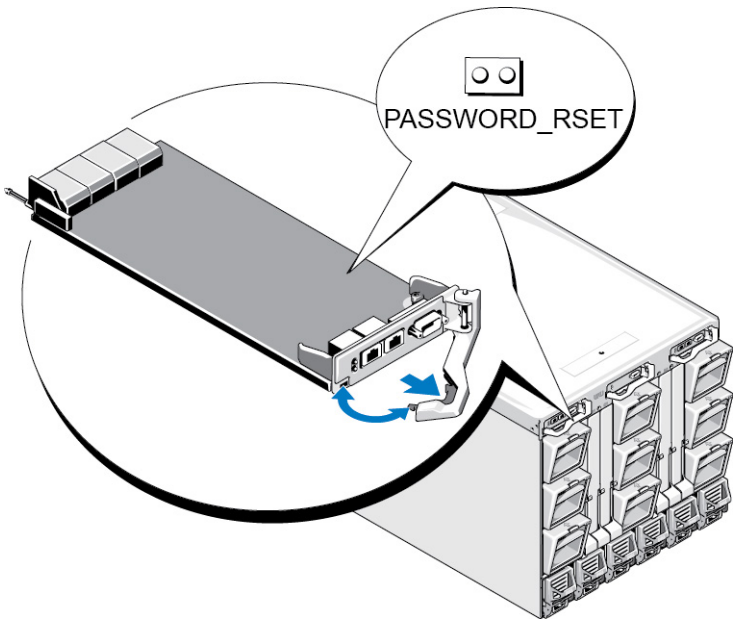


Figure 9. Emplacement du cavalier de réinitialisation du mot de passe

Tableau 39. Paramètres du cavalier de mot de passe CMC

PASSWORD_RSET		(par défaut)	La fonction de réinitialisation du mot de passe est désactivée.
			La fonction de réinitialisation du mot de passe est activée.

3. Faites glisser le module CMC dans l'enceinte. Reconnectez les câbles débranchés.

   REMARQUE : Vérifiez que ce module CMC devient bien le module actif et qu'il le reste jusqu'à ce que les étapes restantes aient été réalisées.

4. Si le module CMC avec cavalier est le seul CMC, attendez qu'il ait fini de redémarrer. S'il y a des CMC redondants dans le châssis, lancez un échange pour rendre actif le module CMC avec cavalier. Dans l'interface Web, dans l'arborescence système, accédez à **Présentation du châssis**, puis cliquez sur **Alimentation → Contrôle**, sélectionnez **Réinitialiser le CMC (amorçage à chaud)**, puis cliquez sur **Appliquer**.

   Le CMC bascule automatiquement sur le module redondant qui devient maintenant actif.

5. Connectez-vous au CMC actif avec le nom d'utilisateur et le mot de passe d'administrateur par défaut (à savoir, root et calvin), puis restaurez les paramètres de compte d'utilisateur nécessaires. Les comptes et mots de passe existants ne sont pas désactivés, et restent actifs.

6. Effectuez les opérations de gestion requises, y compris la création d'un nouveau mot de passe administrateur.

7. Retirez le cavalier PASSWORD_RST à 2 broches, puis replacez la fiche de cavalier.
   a) Appuyez sur le loquet de libération de la carte CMC, sur la poignée, et éloignez la poignée du panneau avant du module. Faites glisser le module CMC hors de l'enceinte.
   b) Retirez le cavalier 2 broches et remettez en place la fiche de cavalier.
   c) Faites glisser le module CMC dans l'enceinte. Reconnectez les câbles débranchés. Répétez l'étape 4 pour faire du module CMC sans cavalier le module actif.

17

Utilisation de l'interface de l'écran LCD

Vous pouvez utiliser l'écran LCD du châssis pour procéder à la configuration et aux diagnostics, et pour obtenir des informations sur l'état du châssis et de son contenu.

La figure suivante illustre l'écran LCD. Cet écran affiche des menus, des icônes, des images et des messages.

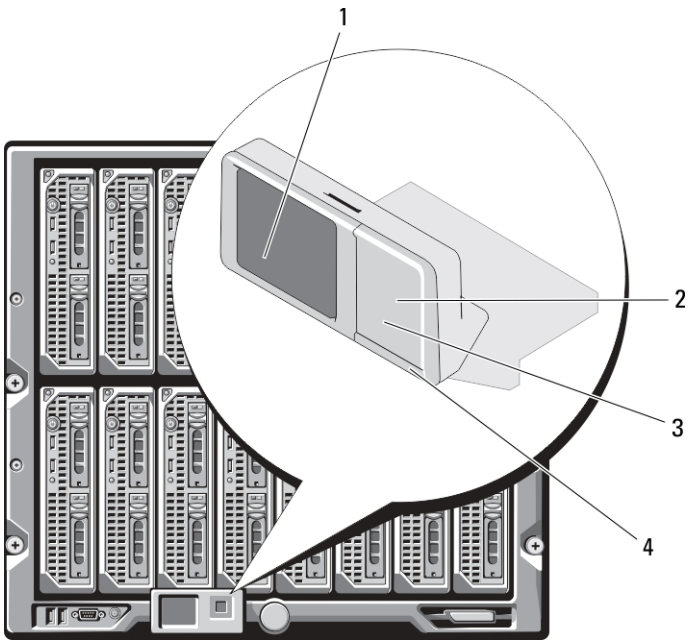


Figure 10. Affichage LCD

1	Écran LCD	2	bouton de sélection
3	boutons de défilement (4)	4	indicateur de condition LED

Liens connexes

- Navigation sur l'écran LCD
- Diagnostics
- Dépannage du matériel du LCD
- Messages du panneau avant de l'écran LCD
- Messages d'erreur de l'écran LCD
- Informations d'état des serveurs et modules sur l'écran LCD

Navigation sur l'écran LCD

Le côté droit de l'écran LCD comporte cinq boutons : quatre boutons flèche (haut, bas, gauche et droite) ainsi qu'un bouton central.

- *Pour passer d'un écran à l'autre, utilisez les touches fléchées Droite (Suivant) et Gauche (Précédent). Vous pouvez à tout moment revenir à un écran précédent pendant l'utilisation de l'écran.*
- *Pour faire défiler les options d'un écran, utilisez les touches fléchées Bas et Haut.*
- *Pour sélectionner et enregistrer un élément d'écran, et passer à l'écran suivant, utilisez le bouton central.*

Les boutons Haut, Bas, Gauche et Droite permettent de modifier votre sélection (élément de menu ou icône à l'écran). L'élément sélectionné s'affiche avec une bordure ou un fond bleu clair.

Lorsque les messages affichés sur l'écran LCD débordent de l'écran, utilisez les boutons flèches gauche et droite pour faire défiler le texte vers la gauche et vers la droite.

Les icônes décrites dans le tableau suivant permettent de naviguer d'un écran à l'autre du panneau LCD.

Tableau 40. Icônes de navigation de l'écran LCD

Icône normale	Icône en surbrillance	Nom et description de l'icône
		**Précédent** — Mettez cette icône en surbrillance et appuyez sur le bouton central pour revenir à l'écran précédent.
		**Accepter/Oui** — Mettez cette icône en surbrillance et appuyez sur le bouton central pour accepter une modification, puis revenir à l'écran précédent.
		**Ignorer/Suivant** — Mettez cette icône en surbrillance et appuyez sur le bouton central pour ignorer toutes les modifications, puis passer à l'écran suivant.
		**Non** — Mettez cette icône en surbrillance et appuyez sur le bouton central pour répondre « Non » à une question, puis passer à l'écran suivant.
		**Rotation** — Mettez cette icône en surbrillance et appuyez sur le bouton central pour passer de la vue graphique de face à la vue de dos du châssis, et inversement. **REMARQUE :** L'arrière-plan orange indique que la vue opposée comporte des erreurs.

Identifier le composant — Fait clignoter la LED bleue d'un composant.

REMARQUE : Un rectangle bleu clignotant entoure cette icône lorsque l'identification de composant est activée.

Un indicateur d'état LED de l'écran LCD fournit une indication de l'intégrité générale du châssis et de ses composants.

- Un voyant bleu continu indique une intégrité satisfaisante.
- Un voyant orange clignotant indique qu'au moins un composant est défaillant.
- Un voyant bleu clignotant est un signal d'identification d'un châssis au sein d'un groupe de châssis.

Liens connexes

Main Menu (Menu principal)
Menu Configuration de l'écran LCD
Écran de configuration de la langue
Écran par défaut
Écran Condition du serveur graphique
Écran Condition du module graphique
Écran Menu de l'enceinte
Écran Condition du module
Écran Condition de l'enceinte
Écran Résumé IP

Main Menu (Menu principal)

Vous pouvez naviguer vers l'un des écrans suivants depuis le **menu principal** :

- **Menu de configuration de l'écran LCD** — Permet de sélectionner la langue à utiliser et l'écran LCD qui s'affiche lorsque personne n'utilise l'écran LCD.
- **Serveur** — Affiche des informations sur la condition des serveurs.
- **Enceinte** : affiche des informations sur la condition du châssis.

Utilisez les boutons flèche haut et bas pour mettre un élément en surbrillance.

Appuyez sur le bouton central pour activer votre sélection.

Menu Configuration de l'écran LCD

Le menu **Configuration de l'écran LCD** affiche un menu d'éléments pouvant être configurés :

- **Configuration de la langue** : choisissez la langue que vous souhaitez utiliser pour le texte et les messages de l'écran LCD.
- **Écran par défaut** : choisissez l'écran qui s'affiche en l'absence d'activité sur l'écran LCD.

Utilisez les boutons fléchés Haut et Bas pour mettre un élément en surbrillance dans le menu, ou mettez en surbrillance l'icône **Précédent** pour revenir au menu **Principal**.

Appuyez sur le bouton central pour activer votre sélection.

Écran de configuration de la langue

L'écran **Configuration de la langue** vous permet de choisir la langue utilisée pour les messages du panneau LCD. La langue actuellement active est mise en surbrillance sur fond bleu clair.

1. Utilisez les boutons flèche haut, bas, gauche et droite pour mettre la langue souhaitée en surbrillance.
2. Appuyez sur le bouton central. L'icône **Accepter** s'affiche et est mise en surbrillance.
3. Appuyez sur le bouton central pour confirmer la modification. Le menu **Configuration de l'écran LCD** s'affiche.

Écran par défaut

La zone **Écran par défaut** vous permet de modifier l'écran que le panneau LCD affiche en l'absence de toute activité. L'écran par défaut défini en usine est l'écran **Menu principal**. Vous pouvez choisir d'afficher l'un des écrans suivants :

- **Menu principal**
- **Condition du serveur** (affichage graphique avant du châssis)
- **Condition du module** (affichage graphique arrière du châssis)
- **Personnalisé** (logo Dell avec le nom du châssis)

L'écran par défaut actif est mis en surbrillance en bleu clair.

1. Utilisez les boutons flèche haut et bas pour mettre en surbrillance l'écran que vous souhaitez définir comme écran par défaut.
2. Appuyez sur le bouton central. L'icône **Accepter** est mise en surbrillance.
3. Appuyez de nouveau sur le bouton central pour confirmer la modification. L'**écran par défaut** s'affiche.

Écran Condition du serveur graphique

L'écran **Graphiques d'état des serveurs** affiche des icônes pour chaque serveur installé dans le châssis et indique l'état général d'intégrité de chacun. L'intégrité du serveur est représentée par la couleur de l'icône de serveur :

- Gris : le serveur est hors tension sans erreurs
- Vert : le serveur est sous tension sans erreurs
- Jaune : le serveur présente une ou plusieurs erreurs non critiques
- Rouge : le serveur présente une ou plusieurs erreurs critiques
- Noir : le serveur n'est pas présent

Un rectangle bleu clair clignotant autour d'une icône de serveur indique que le serveur est en surbrillance.

Pour afficher l'écran **Graphiques d'état des modules**, mettez en surbrillance l'icône de rotation, puis appuyez sur le bouton central.

Pour afficher l'écran d'état d'un serveur, utilisez les touches fléchées pour mettre en surbrillance le serveur voulu, puis appuyez sur le bouton central. L'écran **Condition du serveur** s'affiche.

Pour revenir au menu principal, utilisez les touches fléchées pour mettre en surbrillance l'icône **Précédent**, puis appuyez sur le bouton central.

Écran Condition du module graphique

L'écran **Graphiques d'état des modules** affiche tous les modules installés à l'arrière du châssis et fournit des informations récapitulatives sur l'intégrité de chaque module. L'intégrité du module est représentée par la couleur de l'icône de module :

- Gris : le module est hors tension ou sous tension en veille sans erreurs
- Vert : le module est sous tension sans erreurs
- Jaune : le module présente une ou plusieurs erreurs non critiques
- Rouge : le serveur présente une ou plusieurs erreurs critiques
- Noir : le module n'est pas présent

Un rectangle bleu clair clignotant autour d'une icône de module indique que le module est mis en surbrillance.

Pour afficher l'écran **Graphiques d'état des modules**, mettez en surbrillance l'icône de rotation, puis appuyez sur le bouton central.

Pour afficher l'écran d'état d'un module, utilisez les touches Haut, Bas, Gauche et Droite pour mettre en surbrillance le module voulu, puis appuyez sur le bouton central. L'écran **Condition du module** s'affiche.

Pour revenir au **Menu principal**, utilisez les touches fléchées pour mettre en surbrillance l'icône Précédent, puis appuyez sur le bouton central. L'écran **Menu principal** s'affiche.

Écran Menu de l'enceinte

Cet écran vous permet de naviguer vers les écrans suivants :

- **Écran Condition du module**
- **Écran Condition de l'enceinte**
- **Écran Résumé IP**
- **Menu principal**

Utilisez les boutons de navigation pour mettre en surbrillance l'élément voulu (mettez en surbrillance l'icône **Précédent** pour revenir au **Menu principal**), puis appuyez sur le bouton central. L'écran sélectionné s'affiche.

Écran Condition du module

L'écran **Condition du module** affiche des informations et des messages d'erreur concernant un module. Pour connaître les messages susceptibles d'apparaître dans cet écran, voir « Informations de condition des serveurs et modules sur l'écran LCD » et « Messages d'erreur de l'écran LCD ».

Utilisez les touches Haut et Bas pour passer d'un message à l'autre. Utilisez les touches Gauche et Droite pour faire défiler les messages qui débordent de l'écran.

Mettez en surbrillance l'icône **Précédent** et appuyez sur le bouton central pour retourner à l'écran **Graphiques d'état des modules**.

Écran Condition de l'enceinte

L'écran **Condition de l'enceinte** affiche des informations et des messages d'erreur concernant l'enceinte. Pour connaître les messages susceptibles d'apparaître dans cet écran, voir « Messages d'erreur de l'écran LCD ». Utilisez les flèches Haut et Bas pour vous déplacer dans les messages.

Utilisez les touches fléchées gauche et droite pour faire défiler les messages qui débordent de l'écran.

Mettez en surbrillance l'icône **Précédent** et appuyez sur le bouton central pour retourner à l'écran **Condition de l'enceinte**.

Écran Résumé IP

L'écran **Résumé IP** affiche des informations IP pour les contrôleurs CMC et iDRAC de chaque serveur installé.

Utilisez les touches Haut et Bas pour passer d'une entrée de la liste à une autre. Utilisez les touches Gauche et Droite pour faire défiler les messages sélectionnés qui débordent de l'écran.

Utilisez les boutons flèche haut et bas pour sélectionner l'icône **Précédent** et appuyez sur le bouton central pour retourner au menu **Enceinte**.

Diagnostics

L'écran LCD vous aide à diagnostiquer les problèmes d'un serveur ou module du châssis. En cas de problème ou d'échec dans le châssis, ou dans un serveur ou autre module de ce châssis, l'indicateur d'état de l'écran LCD clignote en orange. Dans le menu principal, une icône sur fond orange s'affiche en regard de l'option de menu (serveur ou enceinte) menant au serveur ou module défectueux.

En suivant les icônes orange dans tout le système de menus de l'écran LCD, vous pouvez afficher l'écran d'état et les messages d'erreur concernant l'élément où le problème s'est produit.

Vous pouvez supprimer les messages d'erreur de l'écran LCD en retirant le module ou serveur cause du problème, ou bien en effaçant le journal du matériel de ce module ou serveur. Pour les erreurs de serveur, utilisez l'interface Web ou l'interface de ligne de commande (CLI) de l'iDRAC pour effacer le journal d'événements système (System Event Log, SEL) du serveur. Pour les erreurs de châssis, utilisez l'interface Web ou l'interface CLI du CMC pour effacer le journal du matériel.

Dépannage du matériel du LCD

Si vous rencontrez des problèmes avec l'écran LCD lors de votre utilisation de CMC, suivez les éléments de dépannage matériel suivants pour déterminer si le problème vient du matériel de l'écran LCD ou d'une connexion à l'écran LCD.

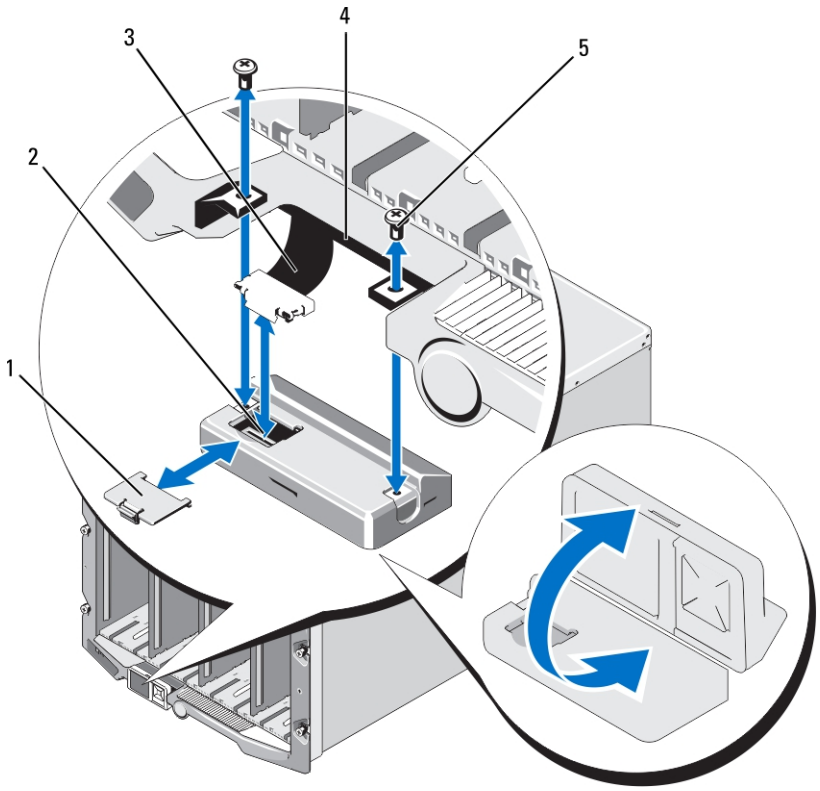


Figure 11. Retrait et installation du module LCD

1	cache-câble	2	module LCD
3	câble ruban	4	charnières (2)
5	vis (2)		

Tableau 41. Éléments de dépannage du matériel LCD

Symptôme	Problème	Action de restauration
Message d'alerte de l'écran `CMC ne répond pas` et la LED clignote orange	Perte de la communication entre le CMC et le panneau avant LCD.	Vérifiez que le CMC démarre, puis réinitialisez-le à l'aide de l'interface graphique ou des commandes de l'utilitaire RACADM.
Message de l'écran d'alerte : « `CMC ne répond pas` ». LED orange fixe ou éteinte.	Les communications du module LCD sont bloquées lors de basculement du CMC ou lors de redémarrages.	Consultez le journal du matériel à l'aide des commandes de l'interface utilisateur graphique (GUI) ou de RACADM. Recherchez un message indiquant : « `Impossible de communiquer avec le contrôleur LCD` ». Réinstallez le câble ruban du module LCD.
Le texte de l'écran LCD est brouillé	Écran LCD défectueux	Remplacez le module LCD.

Le LED et l'écran LCD sont éteints.	Le câble LCD n'est pas branché correctement ou est défectueux ; ou le module LCD est défectueux.	Consultez le journal du matériel à l'aide des commandes de l'interface utilisateur graphique (GUI) ou de RACADM. Recherchez un message indiquant : • `Le câble du module LCD n'est pas branché ou n'est pas branché correctement.` • `Le câble du panneau de commandes est débranché ou n'est pas branché correctement.` Réinstallez les câbles.
Message de l'écran LCD `CMC introuvable`	Aucun CMC n'est présent dans le châssis	Insérez un CMC dans le châssis ou remplacez le CMC existant s'il ne fonctionne pas.

Messages du panneau avant de l'écran LCD

Cette section contient deux sous-sections qui répertorient les informations sur les erreurs et les conditions qui apparaissent sur le panneau avant de l'écran LCD.

Les *Messages d'erreur* de l'écran LCD présentent un format similaire à celui du journal d'événements système (SEL) affiché dans l'interface de ligne de commande (CLI) ou l'interface Web.

Les tableaux de la section traitant des erreurs répertorient les messages d'erreur et d'avertissement affichés sur les différents écrans LCD, avec la cause possible de chaque message. Le texte entre chevrons (< >) peut varier.

Les *Informations de condition* affichées sur l'écran LCD incluent des informations descriptives concernant les modules du châssis. Les tableaux de cette section décrivent les informations affichées pour chaque composant.

Messages d'erreur de l'écran LCD

Tableau 42. Écrans d'état CMC

Gravité	Message	Cause
Critique	La batterie CMC <numéro> a échoué.	La batterie CMOS de CMC est manquante ou absence de tension.
Critique	La pulsation LAN de CMC <numéro> a été perdue.	La connexion NIC de CMC a été retirée ou n'est pas connectée.
Avertissement	A firmware or software incompatibility detected between iDRAC in slot <number> and CMC. (Détection d'une incompatibilité micrologicielle ou logicielle entre l'iDRAC du logement <numéro> et CMC.)	Le micrologiciel entre les deux périphériques ne correspond pas pour prendre en charge une ou plusieurs fonctionnalités.
Avertissement	A firmware or software incompatibility detected between system BIOS in slot <number> and CMC. (Détection d'une incompatibilité micrologicielle ou logicielle entre le BIOS du système du logement <numéro> et CMC.)	Le micrologiciel entre les deux périphériques ne correspond pas pour prendre en charge une ou plusieurs fonctionnalités.

Gravité	Message	Cause
Avertissement	A firmware or software incompatibility detected between CMC 1 and CMC 2. (Détection d'une incompatibilité micrologicielle ou logicielle entre CMC 1 et CMC 2.)	Le micrologiciel entre les deux périphériques ne correspond pas pour prendre en charge une ou plusieurs fonctionnalités.

Tableau 43. Écran État de l'enceinte/Condition du châssis

Gravité	Message	Cause
Critique	Le ventilateur <numéro> est retiré.	Ce ventilateur est nécessaire pour refroidir correctement l'enceinte/le châssis.
Avertissement	Power supply redundancy is degraded. (Dégradation de la redondance du bloc d'alimentation.)	Une ou plusieurs unités d'alimentation sont défaillantes ou ont été retirées, et le système ne peut plus prendre en charge la redondance complète des unités d'alimentation.
Critique	Power supply redundancy is lost. (Perte de la redondance du bloc d'alimentation.)	Une ou plusieurs unités d'alimentation sont défaillantes ou ont été retirées, et le système n'est plus redondant.
Critique	The power supplies are not redundant. Insufficient resources to maintain normal operations. (Les blocs d'alimentation ne sont pas redondants. Il n'y a pas suffisamment de ressources pour conserver un fonctionnement normal.)	Un ou plusieurs blocs d'alimentation (PSU) sont défectueux ou ont été retirés, et le système n'a plus assez de puissance pour assurer son fonctionnement normal. Cela peut provoquer l'arrêt des serveurs.
Avertissement	La température ambiante du panneau de configuration est supérieure au seuil d'avertissement maximal.	La température d'entrée du châssis/enceinte a dépassé le seuil d'avertissement.
Critique	La température ambiante du panneau de configuration est supérieure au seuil d'avertissement maximal.	La température d'entrée du châssis/enceinte a dépassé le seuil d'avertissement.
Critique	La redondance CMC est perdue.	Les CMC ne sont plus redondants. Cela se produit si vous retirez le CMC de secours.
Critique	All event logging is disabled. (Désactivation de la journalisation de tous les événements.)	Le châssis/L'enceinte ne peut pas stocker les événements dans les journaux. Cela indique généralement un problème du panneau de contrôle ou de son câble.
Avertissement	Log is full. (Le journal est plein.)	Le châssis a détecté qu'une ou plusieurs entrées uniquement peuvent être ajoutées au journal matériel CEL avant que celui-ci soit plein.
Avertissement	Log is almost full. (Le journal est presque plein.)	Le journal des événements du châssis est plein à 75 %.

Tableau 44. Écrans État du ventilateur

Gravité	Message	Cause
Critique	Les rotations par minute du ventilateur <numéro> sont en dessous du seuil critique minimal.	La vitesse du ventilateur spécifié ne suffit pas pour refroidir suffisamment le système.
Critique	Le nombre de rotations par minute du ventilateur <numéro> dépasse le seuil critique maximal.	La vitesse du ventilateur spécifié est trop haute. Ceci se produit généralement suite à une pale de ventilateur cassée.

Tableau 45. Écrans État du module d'E/S (IOM)

Gravité	Message	Cause
Avertissement	Détection d'une non-correspondance de structure dans le module d'E/S <numéro>.	La structure du module d'E/S ne correspond pas à celle du serveur ou du module d'E/S redondant.
Avertissement	Détection d'un échec de réglage de lien du module d'E/S <numéro>.	Le module d'E/S n'a pas pu être défini pour une utilisation correcte du NIC sur un ou plusieurs serveurs.
Critique	Détection d'une panne sur le module d'E/S <numéro>.	Le module d'E/S a connu un échec. La même erreur peut également s'afficher si l'alerte thermique du module d'E/S se déclenche.

Tableau 46. Écran État iKVM

Gravité	Message	Cause
Avertissement	La console n'est pas disponible pour le KVM local.	Panne secondaire, par exemple micrologiciel corrompu.
Critique	Le KVM local ne peut pas détecter d'hôtes.	Échec de l'énumération des hôtes USB.
Critique	OSCAR, l'affichage n'est pas opérationnel pour le KVM local.	Échec de l'interface OSCAR.
Irrécupérable	Le KMV local n'est pas opérationnel et est mis hors tension.	Échec RIP série ou échec de la puce de l'hôte USB.

Tableau 47. Écrans État PSU

Gravité	Message	Cause
Critique	Power supply <number> failed. (Panne du bloc d'alimentation <numéro>.)	L'unité d'alimentation est défaillante.
Critique	The power input for power supply <number> is lost. (Perte de l'entrée d'alimentation du bloc d'alimentation <numéro>.)	Perte de l'alimentation en CA - secteur ou cordon en CA - secteur débranché.
Avertissement	Power supply <number> is operating at 110 volts, and could cause a circuit breaker fault. (Le bloc d'alimentation <numéro> fonctionne à 110 volts et pourrait entraîner un court-circuit.)	Le bloc d'alimentation est branché sur une source de 110 volts.

Tableau 48. Écran Condition du serveur

Gravité	Message	Cause
Avertissement	La température ambiante de la carte système est inférieure au seuil d'avertissement minimal.	La température du serveur se rafraîchit.
Critique	La température ambiante de la carte système est inférieure au seuil critique minimal.	La température du serveur baisse.
Avertissement	La température ambiante de la carte système est supérieure au seuil d'avertissement maximal.	La température du serveur monte.
Critique	La température ambiante de la carte système est supérieure au seuil critique maximal.	La température du serveur est trop élevée.
Critique	Le courant du verrou actuel de la carte système dépasse la plage autorisée.	Le courant a franchi un seuil de dégradation.
Critique	Échec de la batterie de la carte système.	La batterie CMOS n'est pas présente ou n'a pas de tension.
Avertissement	The storage battery is low. (La batterie de stockage est faible.)	Le niveau de charge de la batterie ROMB est faible.
Critique	Échec de la batterie de stockage.	La batterie CMOS n'est pas présente ou n'a pas de tension.
Critique	La tension <nom du capteur de tension> de l'UC <numéro> dépasse la plage autorisée.	
Critique	La tension <nom du capteur de tension> de la carte système est hors de la plage autorisée.	
Critique	La tension <nom du capteur de tension> de la carte mezzanine <numéro> est hors de la plage autorisée.	
Critique	La tension <nom du capteur de tension> du stockage est hors de la plage autorisée.	
Critique	CPU <number> has an internal error (IERR). (L'UC <numéro> est confrontée à une erreur interne (IERR).)	Panne de l'UC.
Critique	CPU <number> has a thermal trip (over-temperature) event. (Événement de déclenchement thermique de l'UC <numéro> (surchauffe).)	UC surchauffée.
Critique	CPU <number> configuration is unsupported. (Configuration de l'UC <numéro> non prise en charge.)	Type de processeur incorrect ou dans un emplacement erroné.
Critique	CPU <number> is absent. (L'UC <numéro> est absente.)	L'UC requise est manquante ou est absente.

Gravité	Message	Cause
Critique	Condition de la carte Mezz B<numéro de logement> : capteur de carte d'extension de la carte Mezz B<numéro de logement>, l'erreur d'installation a été confirmée	Carte mezzanine incorrecte installée pour la structure d'E/S
Critique	État de la carte Mezz C<numéro de logement> : capteur de carte d'extension de la carte Mezz B<numéro de logement>, erreur d'installation confirmée	Carte mezzanine incorrecte installée pour la structure d'E/S
Critique	Drive <number> is removed. (Retrait du lecteur <numéro>.)	Le lecteur de stockage a été retiré.
Critique	Panne détectée dans le lecteur <numéro>.	Échec du lecteur de stockage.
Critique	La tension à sécurité intégrée de la carte système dépasse la plage autorisée.	Cet événement est généré lorsque les tensions de la carte système ne sont pas aux niveaux normaux
Critique	The watchdog timer expired. (Le registre d'horloge de la surveillance a expiré.)	Le registre d'horloge de la surveillance d'iDRAC expire et aucune action n'est définie.
Critique	The watchdog timer reset the system. (Le registre d'horloge de la surveillance a réinitialisé le système.)	La surveillance iDRAC a détecté que le système est tombé en panne (délai expiré car aucune réponse n'a été reçue de l'hôte) et que l'action est définie sur redémarrage.
Critique	The watchdog timer powered off the system. (Le registre d'horloge de la surveillance a mis le système hors tension.)	La surveillance iDRAC a détecté que le système est tombé en panne (délai expiré car aucune réponse n'a été reçue de l'hôte) et que l'action est définie sur Éteindre.
Critique	The watchdog timer power cycled the system. (Le registre d'horloge de la surveillance a coupé puis rétabli l'alimentation du système.)	La surveillance iDRAC a détecté que le système est tombé en panne (délai expiré car aucune réponse n'a été reçue de l'hôte) et que l'action est définie sur Cycle d'alimentation.
Critique	Log is full. (Le journal est plein.)	Le périphérique du journal SEL détecte qu'une seule entrée peut être ajoutée au journal SEL avant qu'il ne soit plein.
Avertissement	Détection d'erreurs de la mémoire permanente corrigeable sur un périphérique mémoire de l'emplacement <emplacement>.	
Avertissement	Le taux d'erreur de la mémoire permanente corrigeable a augmenté pour un périphérique mémoire de l'emplacement <emplacement>.	Les erreurs corrigeables de l'ECC atteignent un taux critique.
Critique	Détection d'erreurs de la mémoire multibit sur un périphérique mémoire à l'emplacement <emplacement>.	Une erreur ECC non corrigeable a été détectée.
Critique	Détection d'une interruption non masquable (NMI) lors d'une vérification d'un canal d'E/S	Une interruption critique est générée dans le canal d'E/S.

Gravité	Message	Cause
	sur un composant du périphérique <numéro> de fonction <numéro> du bus <numéro>.	
Critique	Détection d'une interruption non masquable (NMI) lors d'une vérification d'un canal d'E/S sur un composant du logement <numéro>.	Une interruption critique est générée dans le canal d'E/S.
Critique	Détection d'une erreur de parité PCI sur un composant du périphérique <numéro> de fonction <numéro> du bus <numéro>.	Une erreur de parité a été détectée sur le bus PCI.
Critique	A PCI parity error was detected on a component at slot <number>. (Détection d'une erreur de parité PCI sur un composant du logement <numéro>.)	Une erreur de parité a été détectée sur le bus PCI.
Critique	Détection d'une erreur du système PCI sur un composant du bus <numéro>, périphérique <numéro>, fonction <numéro>.	Erreur PCI détectée par un périphérique.
Critique	A PCI system error was detected on a component at slot <number>. (Détection d'une erreur du système PCI sur un composant du logement <numéro>.)	Erreur PCI détectée par un périphérique.
Critique	Désactivation de la journalisation de la mémoire permanente corrigeable pour un périphérique mémoire de l'emplacement <emplacement>.	La journalisation d'erreurs d'un seul bit est désactivée lorsque trop d'erreurs d'un seul bit (SBE) sont journalisées pour un périphérique mémoire.
Critique	All event logging is disabled. (Désactivation de la journalisation de tous les événements.)	
Irrécupérable	Détection d'une erreur de protocole de l'UC.	Le protocole du processeur est passé à l'état irrécupérable.
Irrécupérable	CPU bus parity error detected. (Détection d'une erreur de parité du bus de l'UC.)	Le PERR du bus du processeur est passé à l'état irrécupérable.
Irrécupérable	Détection d'une erreur d'initialisation de l'UC.	L'initialisation du processeur est passée à l'état Irrécupérable.
Irrécupérable	Détection du machine check (vérification de machine) de l'UC.	La vérification machine du processeur est passée à l'état Irrécupérable.
Critique	Memory redundancy is lost. (Perte de la redondance de la mémoire.)	
Critique	Détection d'une erreur fatale du bus sur un composant du bus <numéro>, périphérique <numéro>, fonction <numéro>.	Une erreur fatale a été détectée sur le bus PCIe.
Critique	Détection d'une interruption non masquable (NMI) du logiciel sur un composant du bus <numéro>, périphérique <numéro>, fonction <numéro>.	Une erreur de puce a été détectée.

Gravité	Message	Cause
Critique	Échec de la programmation de l'adresse MAC virtuelle sur un composant du périphérique <numéro> de fonction <numéro> du bus <numéro>.	L'adresse flex n'a pas pu être programmée pour ce périphérique
Critique	Device option ROM on mezzanine card <number> failed to support Link Tuning or FlexAddress. (Échec de la prise en charge du réglage de liaison ou de FlexAddress par la mémoire morte en option du périphérique de la carte mezzanine <numéro>.)	La mémoire morte en option ne prend pas en charge l'adresse flex ou le réglage de liaison.
Critique	Failed to get Link Tuning or FlexAddress data from iDRAC. (Échec d'obtention de données de réglage de liaison ou de FlexAddress depuis iDRAC.)	

REMARQUE : Pour des informations supplémentaires sur des messages LCD du serveur, voir le « Guide d'utilisation du serveur ».

Informations d'état des serveurs et modules sur l'écran LCD

Les tableaux figurant dans cette section décrivent les éléments de condition qui sont affichés sur le panneau avant de l'écran LCD pour chaque type de composant dans le châssis.

Tableau 49. Condition du CMC

Élément	Description
Exemple : CMC1, CMC2	Nom/Emplacement
Aucune erreur	Si aucune erreur ne s'est produite, le message « Aucune erreur » s'affiche à la place de messages d'erreur.
Version du micrologiciel	S'affiche uniquement sur le CMC actif. Indique En attente pour le CMC de secours.
IP4 <activée, désactivée>	Affiche la condition activée de l'IPv4 actuel uniquement sur un CMC actif.
Adresse IP4 : <adresse, en cours d'acquisition>	Ne s'affiche que si l'IPv4 est activée sur un CMC actif uniquement.
IP6 <activée, désactivée>	Affiche état actuel d'activation IPv6, uniquement pour le CMC actif.
Adresse locale IP6 : <adresse>	S'affiche uniquement si IPv6 est activé, uniquement sur le CMC actif.
Adresse globale IP6 : <adresse>	S'affiche uniquement si IPv6 est activé, uniquement sur le CMC actif.

Tableau 50. Condition du châssis/État de l'enceinte

Élément	Description
Nom défini par l'utilisateur	Exemple : « Système en rack Dell ». Valeur modifiable dans l'interface de ligne de commande (CLI) ou l'interface utilisateur graphique (GUI) Web CMC.
Messages d'erreur	Si aucune erreur ne s'est produite, le message « Aucune erreur » s'affiche ; sinon, les messages d'erreur sont répertoriés en premier, suivis des avertissements.
Numéro de modèle	Exemple « PowerEdgeM1000 »
Consommation énergétique	Consommation électrique en watts
Puissance maximale	Consommation électrique maximale en watts
Puissance minimale	Consommation électrique minimale en watts
Température ambiante	Température ambiante en degrés Celsius
Numéro de service	Le numéro de service attribué par l'usine.
Mode de redondance de CMC	Non redondant ou redondant
Mode de redondance de l'unité d'alimentation	Non redondant, redondant en CA - secteur ou redondant en CC

Tableau 51. Condition du ventilateur

Élément	Description
Nom/Emplacement	Exemple : Ventilateur1, Ventilateur2, etc.
Messages d'erreur	En l'absence d'erreurs, « Pas d'erreurs » est affiché ; sinon, les messages d'erreur sont répertoriés, les erreurs critiques en premier, puis les avertissements.
RPM	Vitesse actuelle du ventilateur en tr/min

Tableau 52. État PSU

Élément	Description
Nom/Emplacement	Exemple : Unité d'alimentation1, Unité d'alimentation2, etc.
Messages d'erreur	En l'absence d'erreurs, « Pas d'erreurs » est affiché ; sinon, les messages d'erreur sont répertoriés, les erreurs critiques en premier, puis les avertissements.
Condition	Hors ligne, en ligne ou veille
Puissance maximale	Puissance maximale que l'unité d'alimentation peut fournir au système

Tableau 53. Condition du module d'E/S

Élément	Description
Nom/Emplacement	Exemple : Module d'E/S A1, Module d'E/S B1.
Messages d'erreur	En l'absence d'erreurs, « Pas d'erreurs » est affiché ; sinon, les messages d'erreur sont répertoriés, les erreurs critiques en premier, puis les avertissements.
Condition	Éteint ou allumé
Modèle	Modèle du module d'E/S
Type de structure	Type de mise en réseau
Adresse IP	S'affiche uniquement si le module IOM est activé. Cette valeur est égale à zéro pour un IOM d'intercommunication.
Numéro de service	Le numéro de service attribué par l'usine.

Tableau 54. Condition d'iKVM

Élément	Description
Nom	iKVM
Aucune erreur	Si aucune erreur ne s'est produite, le message « Aucune erreur » s'affiche ; sinon, les messages d'erreur sont répertoriés. Les erreurs critiques sont affichées en premier, suivies des avertissements. Pour plus d'informations, voir « Messages d'erreur de l'écran LCD ».
Condition	Éteint ou allumé
Modèle/Fabricant	Une description du modèle iKVM.
Numéro de service	Le numéro de service attribué par l'usine.
Numéro de pièce	Le numéro de pièce détachée du fabricant.
Version du micrologiciel	Version du micrologiciel du module iKVM.
Version du matériel	Version du matériel du module iKVM.

REMARQUE : Ces informations sont mises à jour de manière dynamique.

Tableau 55. Condition du serveur

Élément	Description
Exemple : Serveur1, Serveur2.	Nom/Emplacement
Aucune erreur	Si aucune erreur ne s'est produite, le message « Aucune erreur » s'affiche ; sinon, les messages d'erreur sont répertoriés. Les erreurs critiques sont affichées en premier, suivies des avertissements. Pour plus d'informations, voir « Messages d'erreur de l'écran LCD ».

Nom du logement	Nom de logement du châssis. Par exemple, SLOT-01. **REMARQUE :** Ce tableau est configurable via l'interface de ligne de commande ou l'interface utilisateur graphique Web du CMC.
Nom	Nom du serveur, que l'utilisateur peut définir dans Dell OpenManage. Ce nom s'affiche uniquement si l'amorçage de l'iDRAC est terminé et si le serveur prend en charge cette fonctionnalité ; sinon, les messages d'amorçage de l'iDRAC s'affichent.
Numéro de modèle	S'affiche si iDRAC a fini de démarrer.
Numéro de service	S'affiche si iDRAC a fini de démarrer.
BIOS Version	Version micrologicielle du BIOS du serveur.
Dernier code POST	Affiche la dernière chaîne de messages du code POST du BIOS du serveur.
Version du micrologiciel iDRAC	S'affiche si iDRAC a fini de démarrer. **REMARQUE :** L'iDRAC version 1.01 est affiché sous la forme 1.1. Il n'existe aucun iDRAC version 1.10.
IP4 <activée, désactivée>	Affiche la condition activée de l'IPv4.
Adresse IP4 : <adresse, en cours d'acquisition>	S'affiche uniquement si l'IPv4 est activée.
IP6 <activée, désactivée>	S'affiche uniquement si l'iDRAC prend en charge IPv6. Affiche l'état actuel d'activation d'IPv6.
Adresse locale IP6 : <adresse>	S'affiche uniquement si l'iDRAC prend en charge IPv6 et si IPv6 est activée.
Adresse globale IP6 : <adresse>	S'affiche uniquement si l'iDRAC prend en charge IPv6 et si IPv6 est activée.
FlexAddress activée sur les structures	S'affiche uniquement si la fonction est installée. Répertorie les structures activées pour le serveur concerné (A, B ou C).

Les informations de la table 17-16 sont mises à jour de façon dynamique. Si le serveur ne prend pas en charge cette fonction, les informations suivantes ne s'affichent pas. Sinon, les options Server Administrator sont les suivantes :

- Option « Aucune » = Aucune chaîne ne doit être affichée sur l'écran LCD.
- Option « Par défaut » = Aucun effet.
- Option « Personnalisé » = Vous permet d'entrer un nom de chaîne pour le serveur.

Les informations s'affichent uniquement si l'amorçage de l'iDRAC est terminé. Pour plus d'informations sur cette fonctionnalité, voir le manuel « *RACADM Command Line Reference Guide for iDRAC7 and CMC* » (Guide de référence de l'interface de ligne de commande RACADM pour iDRAC7 et CMC).

18

Questions fréquemment posées

Cette section contient les questions courantes sur les éléments suivants :

- RACADM
- Gestion et restauration d'un système distant
- Active Directory
- FlexAddress et FlexAddressPlus
- iKVM
- IOM

RACADM

Après réinitialisation du CMC (avec la sous-commande RACADM racreset), lorsque vous entrez une commande, le message suivant s'affiche :

```
racadm <sous-commande> 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 les 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.

Messages d'erreur liés à CMC : problèmes empêchant le CMC de réaliser une opération. Le message peut également être « échec de la commande racadm ».

Tapez `racadm gettracelog` pour obtenir des informations de débogage.

Lorsque vous utilisez l'interface RACADM distante, 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 « Introuvable » s'affiche lorsque vous utilisez les commandes `$ logout` et `$ quit`.

Les commandes « logout » (déconnecter) et « quit » (quitter) ne sont pas prises en charge dans l'interface RACADM de CMC.

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.

CMC inclut 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 émis pour CMC ne correspond pas au nom d'hôte de 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 l'arborescence système, cliquez sur **Présentation du châssis**.
2. Cliquez sur l'onglet **Réseau**, puis sur **Réseau**.

   La page Configuration réseau s'affiche.
3. Sélectionnez l'option **Enregistrer CMC sur DNS**.
4. Entrez le nom du CMC dans le champ **Nom DNS CMC**.
5. Cliquez sur **Appliquer les changements**.

   Pour plus d'informations sur la génération de RSC et l'émission de certificats, voir « Obtention de certificats ».

   L'interface distante RACADM et les services Web ne sont plus disponibles lorsqu'une propriété est modifiée. Pourquoi ?

   Après la réinitialisation du Web Server CMC, il peut s'écouler une minute avant que les services RACADM à distance et l'interface Web ne redeviennent disponibles.

   Le Web Server CMC est réinitialisé dans les cas suivants :

   - Modification de la configuration réseau ou des propriétés de sécurité réseau avec 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.

   Mon serveur DNS n'enregistre pas mon CMC. Pourquoi ?

   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.

   CMC inclut 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 (CA) de confiance. Pour résoudre ce problème de sécurité, téléversez un certificat de serveur CMC émis par une autorité de certification de confiance (comme Thawte ou Verisign). Pour plus d'informations sur les certificats, voir « Obtention de certificats ».

   Pourquoi le message suivant s'affiche-t-il pour des raisons inconnues ?

   `Accès distant : échec de l'authentification SNMP`

   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 <nom de communauté>
```

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.

Entrez un exemple qui illustre la tâche actuelle (facultatif).

Entrez les tâches que l'utilisateur doit réaliser après la tâche actuelle (facultatif).

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 à travers 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 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 pour la création du certificat.

Pour corriger le problème, générez une requête de signature de certificat (RSC), créez un nouveau certificat Web avec Services de certificats Microsoft, puis téléversez-le avec les commandes RACADM suivantes :

```
racadm sslcsrgen [-g] [-f {filename}]
racadm sslcertupload -t 1 -f {web_sslcert}
```

FlexAddress et FlexAddressPlus

Que se passe-t-il si une carte de fonction est retirée ?

Il ne se produit aucun changement visible si vous retirez une carte de fonction. Vous pouvez retirer les cartes de fonction pour les stocker, ou les laisser en place.

Que se passe-t-il si une carte de fonction utilisée dans un châssis est retirée et insérée dans un autre châssis ?

L'interface Web affiche le message d'erreur suivant :

```
Cette carte de fonction a été activée avec un autre châssis. Vous devez la
retirer avant d'accéder à la fonction FlexAddress.
Numéro de service du châssis actuel= XXXXXXXX
Numéro de service du châssis de la carte de fonction = YYYYYYYY
Une entrée sera ajoutée au journal CMC :
cmc <horodatage> : fonction 'FlexAddress@YYYYYYYY' non activée ; ID de châssis
='XXXXXXXX'
```

Que se passe-t-il si la carte de fonction est retirée et qu'une carte non FlexAddress est installée ?

Cette carte n'est ni activée, ni modifiée. La carte est ignorée par CMC. Dans ce cas, la commande **$racadm featurecard -s** renvoie le message suivant :

```
Aucune carte de fonction insérée
ERREUR : impossible d'ouvrir le fichier
```

Que se passe-t-il si une carte de fonction est liée à un châssis dont le numéro de service est reprogrammé ?

- Si la carte de fonction d'origine est présente sur le CMC actif, dans ce châssis ou dans un autre, l'interface Web affiche le message d'erreur suivant :

  ```
  Cette carte de fonction a été activée avec un autre châssis. Vous devez la
  retirer avant d'accéder à la fonction FlexAddress.
  Numéro de service actuel du châssis = XXXXXXXX
  Numéro de service de châssis de la carte de fonction = YYYYYYYY
  ```

  La carte de fonction originale ne peut plus être désactivée, dans ce châssis ou dans un autre, sauf si Dell Service reprogramme le numéro de châssis original d'un châssis et si le CMC où se trouve la carte de fonction d'origine est activé dans ce même châssis.
- La fonction FlexAddress reste activée dans le châssis initialement lié. La valeur de *liaison* de ce châssis est mise à jour pour refléter le nouveau numéro de service.

Est-ce qu'un message d'erreur s'affiche si deux cartes de fonction sont installées dans un système à CMC redondants ?

La carte de fonction du CMC actif est activée et installée dans le châssis. CMC ignore la deuxième carte.

Est-ce que la carte SD dispose d'un verrou de protection en écriture ?

Oui. Avant d'installer la carte SD dans le module CMC, vérifiez que son clapet de protection en écriture est en position déverrouillée. La fonction FlexAddress ne peut pas être activée si la carte SD est protégée en écriture. Dans ce cas, la commande **$racadm feature -s** renvoie le message suivant :

```
Aucune carte de fonction active dans le châssis. ERREUR : système de fichiers en
lecture seule.
```

Que se passe-t-il si aucune carte SD n'est présente dans le contrôleur CMC actif ?

La commande **$racadm featurecard -s** renvoie le message suivant :

```
Aucune carte de fonction insérée.
```

Que devient la fonction FlexAddress si le BIOS du serveur est mis à jour de la version 1.xx vers la version 2.xx ?

Vous devez éteindre le module de serveur avant de pouvoir l'utiliser avec FlexAddress. Une fois la mise à jour du BIOS du serveur terminée, le module de serveur ne reçoit aucune adresse attribuée par le châssis tant que vous n'avez pas réalisé un cycle d'alimentation.

Que se passe-t-il si un châssis doté d'un seul contrôleur CMC est mis à niveau vers une version du micrologiciel antérieure à la version 1.10 ?

- La fonction FlexAddress et sa configuration sont supprimées du châssis.
- La carte de fonction utilisée pour activer la fonction dans ce châssis reste inchangée et reste liée au châssis. Lors de la mise à niveau ultérieure du micrologiciel CMC de ce châssis vers la version 1.10 ou supérieure, vous

réactivez la fonction FlexAddress en réinsérant la carte de fonction d'origine (si nécessaire), en réinitialisant le CMC (si la carte de fonction a été insérée avant la fin de la mise à niveau du micrologiciel) et en reconfigurant la fonction.

Que se passe-t-il si une unité CMC est remplacée par une autre dotée d'un micrologiciel de version antérieure à 1.10 dans un châssis comportant des modules CMC redondants ?

Dans un châssis comportant des modules CMC redondants, si vous remplacez un CMC par un autre dont la version de micrologiciel est antérieure à la version 1.10, vous devez appliquer la procédure suivante pour que la fonction FlexAddress et sa configuration actuelle ne soient PAS supprimées :

- Assurez-vous que la version du micrologiciel CMC actif est toujours la version 1.10 ou une version ultérieure.
- Retirez le contrôleur CMC de secours et insérez un nouveau contrôleur CMC à son emplacement.
- À partir du CMC actif, mettez à niveau le micrologiciel du CMC de secours vers la version 1.10 ou supérieure.

REMARQUE : Si le micrologiciel du CMC de secours n'est pas mis à niveau vers la version 1.10 ou supérieure, et si un basculement se produit, la fonction FlexAddress n'est pas configurée. Vous devez réactiver la fonction et la reconfigurer.

Comment restaurer une carte SD si cette carte n'était pas dans le châssis lorsque la commande de désactivation a été exécutée dans FlexAddress ?

Le problème, c'est qu'il est impossible d'utiliser la carte SD pour installer FlexAddress sur un autre châssis si cette carte n'était pas dans le CMC lors de la désactivation de FlexAddress. Pour que la carte fonctionne à nouveau, insérez-la de nouveau dans un CMC du châssis auquel elle est liée, réinstallez FlexAddress, puis désactivez à nouveau FlexAddress.

La carte SD est correctement installée et toutes les mises à jour de micrologiciel/logiciel ont été réalisées. La fonction FlexAddress est active, mais l'écran de déploiement de serveur n'affiche aucune option pour déployer cette fonction. Que se passe-t-il ?

Il s'agit d'un problème de cache du navigateur. Fermez le navigateur, puis relancez-le.

Que devient FlexAddress si je dois réinitialiser la configuration de mon châssis avec la commande RACADM `racresetcfg` ?

La fonction FlexAddress est quand même activée et prête à l'emploi. Par défaut, toutes les structures et tous les logements sont sélectionnés.

REMARQUE : Il est vivement recommandé d'éteindre le châssis avant d'émettre la commande RACADM `racresetcfg`.

Après que j'ai désactivé uniquement la fonction FlexAddressPlus (FlexAddress est toujours activé), la commande `racadm setflexaddr` échoue sur le CMC (encore actif). Pourquoi ?

Si le CMC est activé par la suite, alors que la carte de fonction FlexAddressPlus est toujours sans son logement, la fonction FlexAddressPlus est réactivée et les modifications de configuration de logement/structure flexaddress peuvent se poursuivre.

iKVM

Le message « L'utilisateur a été désactivé par le contrôle CMC » apparaît sur le moniteur connecté au panneau avant. Pourquoi ?

La connexion au panneau avant a été désactivée par CMC. Réactivez-la avec l'interface Web CMC ou avec RACADM.

Pour activer le panneau avant avec l'interface Web CMC, accédez à l'onglet **iKVM** → **Configuration**, sélectionnez l'option **USB/Vidéo du panneau avant activé**, puis cliquez sur **Appliquer** pour enregistrer le paramètre.

Pour activer le panneau avant à l'aide de RACADM, ouvrez une console texte série/Telnet/SSH vers CMC, ouvrez une session et entrez :

```
racadm config -g cfgKVMInfo -o cfgKVMAccesToCMCEnable 1
```

L'accès au panneau arrière ne fonctionne pas. Pourquoi ?

Le paramètre du panneau avant est activé par CMC et un moniteur est connecté au panneau avant.

Le système autorise une seule connexion à la fois. La connexion au panneau avant est prioritaire sur l'interface de console analogique (ACI) et sur le panneau arrière. Pour plus d'informations sur l'ordre de priorité des connexions, voir « Priorités de connexion d'iKVM ».

Le message « L'utilisateur a été désactivé car plusieurs couches ont été affectées à un autre appareil » apparaît sur le moniteur connecté au panneau arrière. Pourquoi ?

Un câble réseau est connecté au connecteur du port ACI d'iKVM et à un appareil KVM secondaire.

Le système autorise une seule connexion à la fois. La connexion multicouche de l'interface de console analogique (ACI) est prioritaire sur la connexion au panneau arrière. L'ordre de priorité des connexions est le suivant : panneau avant, ACI, puis panneau arrière.

La LED orange du module iKVM clignote. Pourquoi ?

Trois causes sont possibles :

- **Il existe un problème de l'iKVM**, qui nécessite une reprogrammation du module iKVM. Pour corriger le problème, suivez les instructions de mise à jour du micrologiciel iKVM.
- **L'iKVM reprogramme l'interface de console CMC.** Dans ce cas, la console CMC est temporairement indisponible et est représentée par un point jaune dans l'interface OSCAR. Le processus prend environ 15 minutes.
- **Le micrologiciel iKVM a détecté une erreur matérielle.** Pour plus d'informations, affichez l'état du module iKVM.

Plusieurs couches ont été affectées à l'iKVM via le port ACI lié à un commutateur KVM externe, mais aucune entrée de connexion ACI n'est disponible.

Tous les états sont marqués d'un point jaune dans l'interface OSCAR.

La connexion au panneau avant est activée et un écran est connecté. Comme le panneau avant est prioritaire sur toutes les autres connexions iKVM, les connecteurs ACI et ceux du panneau arrière sont désactivés.

Pour activer la connexion au port ACI, vous devez d'abord désactiver l'accès au panneau avant ou supprimer l'écran connecté à ce panneau. Les entrées OSCAR du commutateur KVM externe deviennent actives et accessibles.

Pour désactiver le panneau avant avec l'interface Web CMC, accédez à l'onglet **iKVM → Configuration**, sélectionnez l'option **USB/Vidéo du panneau avant activé**, puis cliquez sur Appliquer.

Pour activer le panneau avant à l'aide de RACADM, ouvrez une console texte série/Telnet/SSH vers CMC, ouvrez une session et entrez :

racadm config -g cfgKVMInfo -o cfgKVMFrontPanelEnable 0

Dans le menu OSCAR, la connexion Dell CMC porte un X rouge et il est impossible de se connecter au CMC. Pourquoi ?

Deux causes sont possibles :

- **La console Dell CMC a été désactivée.** Dans ce cas, activez-la avec l'interface Web CMC ou avec RACADM.
- **Le CMC n'est pas disponible parce qu'il est en cours d'initialisation, de basculement vers le CMC de secours ou de reprogrammation.** Dans ce cas, attendez simplement la fin de l'initialisation du CMC.

Le nom de logement d'un serveur est marqué « Initialisation » dans OSCAR et je ne peux pas le sélectionner. Pourquoi ?

Le serveur s'initialise ou le contrôleur iDRAC sur ce serveur n'a pas pu s'initialiser.

Initialement, attendez 60 secondes. Si le serveur est toujours en cours d'initialisation, le nom de logement s'affiche dès l'initialisation terminée et le serveur peut être sélectionné.

Si, après 60 secondes, OSCAR indique encore que le logement s'initialise, retirez le serveur, puis réinsérez-le dans le châssis. Cette action permet à l'iDRAC de se réinitialiser.

IOM

Après un changement de configuration, le CMC affiche parfois l'adresse IP 0.0.0.0.

Cliquez sur l'icône Actualiser pour voir 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.

Pour plus d'informations sur les paramètres réseau des modules d'E/S (IOM), reportez-vous au document « *Dell PowerConnect M6220 Switch Important Information* » (Informations importantes sur le commutateur Dell PowerConnect M6220) et au livre blanc « *Dell PowerConnect 6220 Series Port Aggregator* » (Agrégation de ports Dell PowerConnect série 6220).