

Micrologiciel Dell Chassis Management Controller Version 3.1 Guide d'utilisation

[Présentation](#)

[Installation et configuration de CMC](#)

[Configuration de CMC pour utiliser des consoles de ligne de commande](#)

[Utilisation de l'interface de ligne de commande RACADM](#)

[Utilisation de l'interface Web de CMC](#)

[Utilisation de FlexAddress](#)

[Utilisation de FlexAddress Plus](#)

[Utilisation du service d'annuaire CMC](#)

[Gestion de l'alimentation](#)

[Utilisation du module iKVM](#)

[Gestion de la structure d'E/S](#)

[Dépannage et récupération](#)

[Diagnostics](#)

Remarques et précautions

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

 **PRÉCAUTION** : une PRÉCAUTION indique un risque d'endommagement du matériel ou de perte de données en cas de non-respect des instructions.

Les informations que contient cette publication sont sujettes à modification sans préavis.

© 2010 Dell Inc. Tous droits réservés.

La reproduction de ce document, de quelque manière que ce soit, sans l'autorisation écrite de Dell Inc. est strictement interdite. Marques utilisées dans ce texte : Dell™, le logo DELL, FlexAddress™, OpenManage™, PowerEdge™ et PowerConnect™ sont des marques de Dell Inc. Microsoft®, Active Directory®, Internet Explorer®, Windows®, Windows Server®, et Windows Vista® sont des marques ou des marques déposées de Microsoft Corporation aux États-Unis et dans d'autres pays. Red Hat® et Red Hat Enterprise Linux® sont des marques déposées de Red Hat, Inc. aux États-Unis et dans d'autres pays. Novell® est une marque déposée et SUSE™ est une marque de Novell Inc. aux États-Unis et dans d'autres pays. Intel® est une marque déposée d'Intel Corporation. UNIX® est une marque déposée de The Open Group aux États-Unis et dans d'autres pays. Avocent® est une marque commerciale de Avocent Corporation. OSCAR® est une marque déposée d'Avocent Corporation ou ses filiales.

Copyright 1998-2006 The OpenLDAP Foundation. Tous droits réservés. La redistribution et l'utilisation aux formats source et binaire, avec ou sans modification, ne sont permises que selon les termes de la licence publique OpenLDAP. Une copie de cette licence est disponible dans le fichier LICENSE qui se trouve dans le répertoire de haut niveau de la distribution ainsi qu'à l'adresse <http://www.OpenLDAP.org/license.html>. OpenLDAP est une marque déposée de The OpenLDAP Foundation. Il se peut que certains fichiers individuels et/ou progiciels fournis par des tiers soient sous copyright et qu'ils soient sujets à des restrictions supplémentaires. Ce produit est dérivé de la distribution LDAP v3.3 de l'Université du Michigan. Ce produit contient aussi des produits dérivés de sources publiques. Les informations sur OpenLDAP sont disponibles sur <http://www.openldap.org/>. Parties de Copyright 1998-2004 Kurt D. Zeilenga. Parties de Copyright 1998-2004 Net Boolean Incorporated. Parties de Copyright 2001-2004 IBM Corporation. Tous droits réservés. La redistribution et l'utilisation aux formats source et binaire, avec ou sans modification, ne sont permises que selon les termes de la licence publique OpenLDAP. Parties de Copyright 1999-2003 Howard Y.H. Chu. Parties de Copyright 1999-2003 Symas Corporation. Parties de Copyright 1998-2003 Hallvard B. Furuseth. Tous droits réservés. La redistribution et l'utilisation aux formats source et binaire, avec ou sans modification, sont permises tant que cet avis est conservé. Les noms des détenteurs de copyright ne peuvent pas être utilisés pour approuver ou promouvoir des produits dérivés de ce logiciel sans leur autorisation préalable par écrit. Ce logiciel est fourni « en l'état » sans garantie explicite ou tacite. Parties de Copyright (c) 1992-1996 Membres du conseil de l'Université du Michigan. Tous droits réservés. La redistribution et l'utilisation aux formats source et binaire sont permises tant que cet avis est conservé et que l'Université du Michigan à Ann Arbor reçoit les crédits qui lui sont dus. Le nom de l'université ne peut pas être utilisé pour approuver ou promouvoir des produits dérivés de ce logiciel sans son autorisation préalable par écrit. Ce logiciel est fourni « en l'état » sans garantie explicite ou tacite.

D'autres marques et noms commerciaux peuvent être utilisés dans ce document pour faire référence aux entités se réclamant de ces marques et de ces noms ou à leurs produits. Dell Inc. rejette tout intérêt propriétaire dans les marques et les noms commerciaux autres que les siens.

Décembre 2010

[Retour à la page Contenu](#)

Utilisation du service d'annuaire CMC

Micrologiciel Dell Chassis Management Controller Version 3.1 Guide d'utilisation

- [Utilisation de CMC avec Microsoft Active Directory](#)
- [Présentation d'Active Directory avec le schéma standard](#)
- [Présentation du schéma étendu](#)
- [Configuration de la connexion directe](#)
- [Configuration de l'authentification bifactorielle par carte à puce](#)
- [Utilisation de CMC avec un LDAP générique](#)

Un service de répertoire permet de maintenir une base de données commune rassemblant toutes les informations nécessaires au contrôle des utilisateurs réseau, des ordinateurs, des imprimantes, etc. Si votre entreprise utilise le logiciel Microsoft Active Directory ou LDAP Directory, vous pouvez configurer CMC pour utiliser l'authentification des utilisateurs basée sur répertoire.

Utilisation de CMC avec Microsoft Active Directory

 **REMARQUE** : l'utilisation d'Active Directory pour reconnaître les utilisateurs CMC est prise en charge par les systèmes d'exploitation Microsoft Windows 2000 et Windows Server 2003. Active Directory sur IPv6 est pris en charge uniquement sous Windows 2008.

Extensions de schéma Active Directory

Vous pouvez utiliser Active Directory pour définir l'accès utilisateur à CMC selon deux méthodes :

- 1 La solution de schéma standard qui utilise uniquement les objets de groupe Active Directory standard.
- 1 La solution de schéma étendu, qui utilise des objets Active Directory définis par Dell.

Schéma standard comparé au schéma étendu

Lorsque vous utilisez Active Directory pour configurer l'accès à CMC, vous devez choisir la solution de schéma étendu ou schéma standard.

Avec le schéma standard :

- 1 Aucune extension de schéma n'est nécessaire car le schéma standard utilise uniquement des objets Active Directory.
- 1 La configuration d'Active Directory est simple.

Avec le schéma étendu :

- 1 Tous les objets de contrôle d'accès sont maintenus dans Active Directory.
- 1 La configuration de l'accès utilisateur sur des contrôleurs CMC différents avec des niveaux de privilège différents permet une flexibilité maximale.

Présentation d'Active Directory avec le schéma standard

L'utilisation du schéma étendu pour l'intégration d'Active Directory requiert une configuration sur Active Directory et sur CMC.

Du côté d'Active Directory, un objet Groupe standard est utilisé comme groupe de rôles. Un utilisateur ayant accès à CMC sera membre du groupe de rôles.

Pour donner à cet utilisateur accès à une carte CMC spécifique, le nom du groupe de rôles et son nom de domaine doivent être configurés sur cette carte CMC. Contrairement à la solution du schéma étendu, le niveau des rôles et des privilèges est défini sur chaque carte CMC et non pas dans Active Directory. Vous pouvez configurer et définir un maximum de cinq groupes de rôles sur chaque contrôleur CMC. Le [Tableau 5-4.1](#) présente le niveau de privilège des groupes de rôles et le [Tableau 8-1](#) illustre les paramètres par défaut des groupes de rôles.

Figure 8-1. Configuration de CMC avec Active Directory et le schéma standard

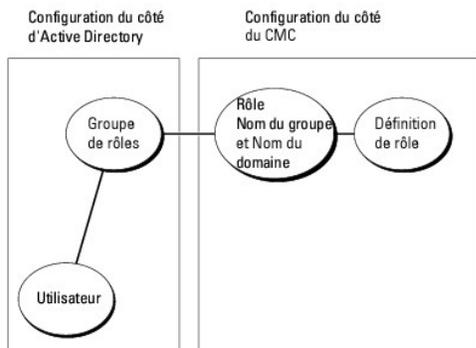


Tableau 8-1. Privilèges par défaut des groupes de rôles

Groupe de rôles	Niveau de privilège par défaut	Droits accordés	Masque binaire
1	None (Aucun)	<ul style="list-style-type: none"> 1 Ouverture de session utilisateur CMC 1 Administrateur de configuration du châssis 1 Administrateur de configuration des utilisateurs 1 Administrateur d'effacement des journaux 1 Administrateur de contrôle du châssis (contrôle de l'alimentation) 1 Super utilisateur 1 Server Administrator 1 Utilisateur de tests d'alertes 1 Utilisation de commande de débogage 1 Administrateur de structure A 1 Administrateur de structure B 1 Administrateur de structure C 	0x00000fff
2	None (Aucun)	<ul style="list-style-type: none"> 1 Ouverture de session utilisateur CMC 1 Administrateur d'effacement des journaux 1 Administrateur de contrôle du châssis (contrôle de l'alimentation) 1 Server Administrator 1 Utilisateur de tests d'alertes 1 Administrateur de structure A 1 Administrateur de structure B 1 Administrateur de structure C 	0x000000f9
3	None (Aucun)	Ouverture de session utilisateur CMC	0x00000001
4	None (Aucun)	Aucun droit attribué	0x00000000
5	None (Aucun)	Aucun droit attribué	0x00000000

REMARQUE : les valeurs de masque binaire sont utilisées uniquement lors de la définition du schéma standard avec RACADM.

REMARQUE : pour plus d'informations sur les privilèges utilisateur, voir [Types d'utilisateurs](#).

Il existe deux méthodes pour activer Active Directory avec le schéma standard :

- 1 Avec l'interface Web de CMC. Voir [Configuration de CMC avec Active Directory avec schéma standard et l'interface Web](#).
- 1 Avec l'outil CLI?RACADM. Voir [Configuration de CMC avec Active Directory avec schéma standard et RACADM](#).

Configuration du schéma standard d'Active Directory pour accéder à CMC

Vous devez suivre les étapes suivantes pour configurer Active Directory pour qu'un utilisateur Active Directory puisse accéder à CMC :

1. Sur un serveur Active Directory (contrôleur de domaine), ouvrez le snap-in Utilisateurs et ordinateurs Active Directory.
2. Créez un groupe ou sélectionnez un groupe existant. Le nom du groupe et le nom de ce domaine doivent être configurés sur CMC soit avec l'interface Web soit RACADM.

Pour plus d'informations, voir [Configuration de CMC avec Active Directory avec schéma standard et l'interface Web](#) ou [Configuration de CMC avec Active Directory avec schéma standard et RACADM](#).

- Ajoutez l'utilisateur Active Directory comme membre du groupe Active Directory pour qu'il puisse accéder à iDRAC6.

Configuration de CMC avec Active Directory avec schéma standard et l'interface Web

- Ouvrez une session sur l'interface Web de CMC.
- Sélectionnez **Châssis** dans l'arborescence du système.
- Cliquez sur **Authentification utilisateur** → **Services d'annuaire**. La page **Services d'annuaire** s'affiche.
- Sélectionnez le bouton radio en regard de Microsoft Active Directory (Schéma standard). La page **Configuration et gestion d'Active Directory** apparaît.
- Dans la section **Paramètres communs** :
 - Sélectionnez la case à cocher **Activer Active Directory**.
 - Tapez le **nom de domaine racine**.

 **REMARQUE** : le **nom de domaine racine** doit être un nom de domaine valide qui respecte la convention d'attribution des noms x.y, où x est une chaîne de 1 à 256 caractères ASCII non séparés par des espaces, et où y est un type de domaine valide tel que com, edu, gov, int, mil, net ou org.

 - Tapez le **Délai d'attente** en secondes. Le Délai d'attente est compris entre 15 et 300 secondes. Le Délai d'attente par défaut est 90 secondes
- Si vous voulez que l'appel dirigé recherche le contrôleur de domaine et le catalogue global, cochez la case **Chercher le serveur AD à rechercher (facultatif)**, puis :
 - Dans le champ de texte **Contrôleur de domaine**, tapez le nom du serveur sur lequel est installé le service Active Directory.
 - Dans le champ de texte **Catalogue global**, tapez l'emplacement du catalogue global sur le contrôleur de domaine d'Active Directory. Le catalogue global fournit une ressource pour rechercher une forêt Active Directory.
- Cliquez sur **Appliquer** pour enregistrer vos paramètres.

 **REMARQUE** : vous devez appliquer vos paramètres avant de passer à l'étape suivante. Si vous n'appliquez pas les paramètres, vous perdrez les paramètres entrés lorsque vous passerez à la page suivante.
- Dans la section **Paramètres du schéma standard**, cliquez sur un **Groupe de rôles**. La page **Configurer le groupe de rôles** s'affiche.
- Saisissez le **Nom du groupe**. Le nom du groupe identifie le groupe de rôles dans l'Active Directory associé à la carte CMC.
- Saisissez le **Domaine du groupe**. Le **Domaine du groupe** est le nom de domaine racine pleinement qualifié de la forêt.
- Sélectionnez les privilèges du groupe dans la page **Privilèges de groupes de rôles**.

Si vous modifiez des privilèges, le **privilège du groupe de rôles** (administrateur, utilisateur privilégié ou utilisateur invité) existant deviendra celui du groupe personnalisé ou du groupe de rôles approprié. Voir [Table 5-41](#).
- Cliquez sur **Appliquer** pour enregistrer les paramètres Groupe de rôles.
- Cliquez sur **Retour à la page Configuration**.
- Téléversez votre certificat signé par une autorité de certification racine de la forêt de domaines sur CMC. Dans la section **Gestion des certificats**, tapez le chemin d'accès du fichier du certificat ou naviguez vers le fichier du certificat. Cliquez sur le bouton **Téléverser** pour transférer le fichier vers CMC.

 **REMARQUE** : la valeur **Chemin du fichier** affiche le chemin de fichier relatif du certificat que vous téléversez. Vous devez taper le chemin de fichier absolu, y compris le chemin et le nom de fichier complets et l'extension du fichier.

Les certificats SSL des contrôleurs de domaine doivent être signés par le certificat signé par l'autorité de certification racine. Le certificat signé par l'autorité de certification racine doit être disponible sur la station de gestion accédant à CMC.
- Cliquez sur **Appliquer**. Le serveur Web de CMC redémarre automatiquement lorsque vous cliquez sur **Appliquer**.
- Fermez, puis ouvrez une session sur CMC pour terminer la configuration de la fonctionnalité Active Directory CMC.
- Sélectionnez **Châssis** dans l'arborescence du système.
- Cliquez sur l'onglet **Réseau**.

19. Cliquez sur le sous-onglet **Réseau**. La page **Configuration réseau** s'affiche.
20. Si **Utiliser DHCP (pour l'adresse IP du NIC)** est sélectionné sous **Paramètres réseau**, sélectionnez **Utiliser DHCP pour obtenir l'adresse du serveur DNS**.

Pour saisir manuellement l'adresse IP du serveur DNS, désélectionnez **Utiliser DHCP pour obtenir des adresses de serveur DNS** et tapez les adresses IP de serveur DNS principale et alternative.
21. Cliquez sur **Appliquer les modifications**.

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

Configuration de CMC avec Active Directory avec schéma standard et RACADM

Pour configurer la fonctionnalité Active Directory CMC avec le schéma standard à l'aide de l'interface de ligne de commande RACADM, utilisez les commandes suivantes :

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

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1

racadm config -g cfgActiveDirectory -o cfgADType 2

racadm config -g cfgActiveDirectory -o cfgADRacDomain <nom de domaine rac pleinement qualifié>

racadm config -g cfgStandardSchema -i <index> -o cfgSSADRoleGroupName <nom de domaine du groupe de rôles>

racadm config -g cfgStandardSchema -i <index> -o cfgSSADRoleGroupDomain <nom de domaine pleinement qualifié>

racadm config -g cfgStandardSchema -i <index> -o cfgSSADRoleGroupPrivilege <numéro du masque binaire pour des droits d'utilisateur spécifiques>

racadm sslcertupload -t 0x2 -f <certificat d'AC racine ADS>

racadm sslcertdownload -t 0x1 -f <certificat SSL du RAC>
```

 **REMARQUE** : pour connaître les valeurs de numéro du masque binaire, consultez le Tableau 3-1 du chapitre concernant les propriétés de la base de données du *Guide de référence Administrateur de Dell Chassis Management Controller*.

2. Spécifiez un serveur DNS à l'aide de l'une des options suivantes :

- 1 Si DHCP est activé sur CMC et que vous voulez utiliser l'adresse DNS obtenue automatiquement par le serveur DHCP, tapez la commande suivante :

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

- 1 Si le protocole DHCP est désactivé sur CMC ou que vous voulez entrer manuellement l'adresse IP DNS, tapez les commandes suivantes :

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

racadm config -g cfgLanNetworking -o cfgDNSServer1 <adresse IP de DNS principale>

racadm config -g cfgLanNetworking -o cfgDNSServer2 <adresse IP de DNS secondaire>
```

Présentation du schéma étendu

Il existe deux méthodes pour activer Active Directory avec le schéma étendu :

- 1 Utilisation de l'interface Web de CMC. Pour les instructions, voir [Configuration de CMC avec le schéma étendu d'Active Directory et l'interface Web](#).
- 1 Utilisation de l'interface de ligne de commande RACADM. Pour les instructions, voir [Configuration de CMC avec le schéma étendu d'Active Directory et RACADM](#).

Extensions de schéma Active Directory

Les données d'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 pouvant être ajoutées ou incluses dans la base de données.

La classe d'utilisateur est un exemple de classe qui est conservée dans la base de données. Les attributs de classe d'utilisateur peuvent inclure le prénom de l'utilisateur, son nom de famille, son numéro de téléphone, etc.

Vous pouvez étendre la base de données d'Active Directory en y ajoutant vos propres attributs et classes pour répondre aux besoins de l'environnement de votre entreprise. Dell a étendu ce schéma pour inclure les modifications nécessaires à la prise en charge de l'authentification et de l'autorisation de la gestion à distance.

Chaque attribut ou classe ajouté à un schéma Active Directory existant peut être défini par une référence unique. Pour maintenir des numéros uniques dans l'industrie, Microsoft conserve une base de données d'identifiants d'objets (OID) d'Active Directory. Pour étendre le schéma dans Active Directory de Microsoft, Dell a créé des OID uniques, des extensions de noms uniques et des numéros d'attributs liés de façon unique pour des attributs et classes spécifiques à Dell :

Extension de Dell : dell

OID de base de Dell : 1.2.840.113556.1.8000.1280

Plage de N° d'association RAC : 12070-2079

Présentation des extensions de schéma du RAC

Dell fournit un groupe de propriétés que vous pouvez configurer. Le schéma étendu par Dell inclut les propriétés Association, Périphérique et Privilège.

La propriété Association lie les utilisateurs ou les groupes à un ensemble spécifique de privilèges pour un ou plusieurs périphériques RAC. Ce modèle offre à l'administrateur un maximum de flexibilité sur les différentes combinaisons d'utilisateurs, de privilèges du RAC et de périphériques RAC sur le réseau, sans ajouter trop de complexité.

Présentation des objets Active Directory

Lorsque le réseau que vous voulez intégrer avec Active Directory pour l'authentification et l'autorisation comprend deux CMC, vous devez créer au moins un objet Association et un objet Périphérique RAC pour chaque contrôleur CMC. Vous pouvez créer plusieurs objets Association et chaque objet Association peut être lié à autant d'utilisateurs, groupes d'utilisateurs ou objets Périphérique RAC que nécessaire. Les utilisateurs et les objets Périphérique RAC peuvent être des membres de n'importe quel domaine dans l'entreprise.

Cependant, chaque objet Association ne peut être lié (ou ne peut lier les utilisateurs, les groupes d'utilisateurs ou les objets Périphérique RAC) qu'à un seul objet Privilège. Cet exemple permet à l'administrateur de contrôler les privilèges de chaque utilisateur sur des CMC spécifiques.

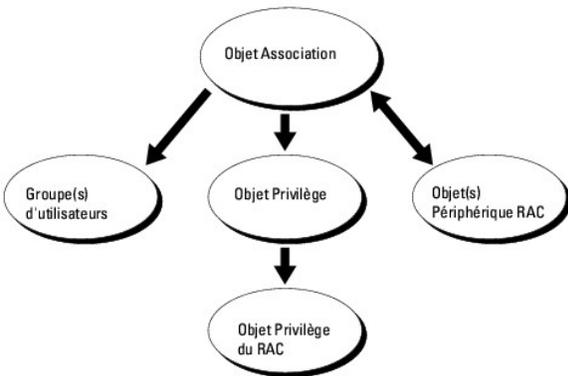
L'objet Périphérique RAC est le lien vers le micrologiciel du RAC permettant à Active Directory d'effectuer une requête d'authentification et d'autorisation. Lorsqu'un RAC est ajouté au réseau, l'administrateur doit configurer le RAC et son objet de périphérique avec son nom Active Directory pour que les utilisateurs puissent établir l'authentification et l'autorisation avec Active Directory. En outre, l'administrateur doit ajouter le RAC à au moins un objet Association pour que les utilisateurs puissent s'authentifier.

[Figure 8-2](#) illustre le fait que l'objet Association fournit la connexion nécessaire pour toute authentification et autorisation.

REMARQUE : l'objet Privilège RAC s'applique à DRAC 4, DRAC 5 et à CMC.

Vous pouvez créer autant d'objets Association que souhaité. Vous devez toutefois créer au moins un objet Association et avoir un objet Périphérique RAC pour chaque RAC (CMC) présent sur le réseau que vous voulez intégrer à Active Directory.

Figure 8-2. Configuration type pour les objets Active Directory

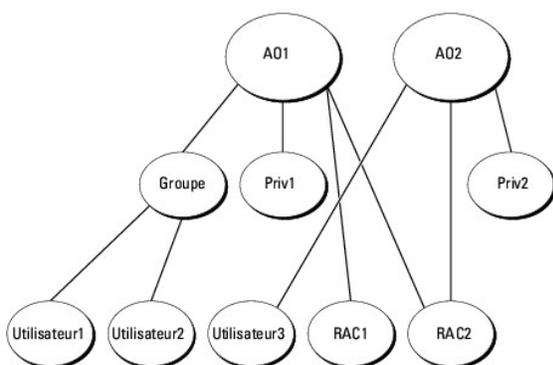


L'objet Association inclut autant d'utilisateurs et/ou de groupes que d'objets Périphérique RAC. Toutefois, l'objet Association ne peut inclure qu'un seul objet Privilège par objet Association. L'objet Association connecte les « Utilisateurs » qui ont des « Privilèges » sur les contrôleurs RAC (CMC).

En outre, vous pouvez configurer des objets Active Directory dans un domaine unique ou dans des domaines multiples. Par exemple, supposons que vous avez deux contrôleurs CMC (RAC1 et RAC2) et trois utilisateurs Active Directory existants (utilisateur1, utilisateur2 et utilisateur3). Vous voulez attribuer des privilèges d'administrateur à utilisateur1 et utilisateur2 sur les deux CMC et des privilèges d'ouverture de session à utilisateur3 sur la carte RAC2. La [Figure 8-3](#) montre illustre la configuration des objets Active Directory dans ce scénario.

Lorsque vous ajoutez des groupes universels à partir de domaines séparés, 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 ne fonctionnent pas avec les groupes universels d'autres domaines.

Figure 8-3. Configuration d'objets Active Directory dans un domaine unique



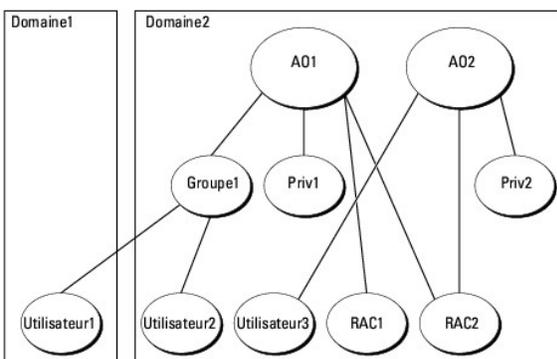
Pour configurer les objets pour le scénario de domaine unique :

1. Créez deux objets Association.
2. Créez deux objets Périphérique RAC, RAC1 et RAC2, pour représenter les deux CMC.
3. Créez deux objets Privilège, Priv1 et Priv2 ; Priv1 disposant de tous les privilèges (administrateur) et Priv2 disposant des privilèges d'ouverture de session.
4. Groupez Utilisateur1 et Utilisateur2 dans le Groupe1.
5. Ajoutez Groupe1 comme membre de l'objet Association 1 (A01), Priv1 comme objet Privilège dans A01, et RAC1 et RAC2 comme périphériques RAC dans A01.
6. Ajoutez Utilisateur3 comme membre de l'objet Association 2 (A02), Priv2 comme objet Privilège dans A02 et RAC2 comme périphérique RAC dans A02.

Pour des instructions détaillées, voir [Ajout d'utilisateurs CMC et de leurs privilèges à Active Directory](#).

La [Figure 8-4](#) fournit un exemple d'objets Active Directory dans de multiples domaines. Dans ce scénario, vous avez deux CMC (RAC1 et RAC2) et trois utilisateurs Active Directory existants (utilisateur1, utilisateur2 et utilisateur3). Utilisateur1 est dans le Domaine1 ; Utilisateur2 et Utilisateur3 sont dans le Domaine2. Dans ce scénario, configurez utilisateur1 et utilisateur2 avec les droits d'administrateur sur les deux CMC et configurez utilisateur3 avec les privilèges d'ouverture de session sur la carte RAC2.

Figure 8-4. Configuration des objets Active Directory dans des domaines multiples



Pour configurer les objets pour le scénario de domaine multiple :

1. Assurez-vous que la fonction de forêt de domaines est en mode Natif ou Windows 2003.
2. Créez deux objets Association, A01 (d'étendue universelle) et A02, dans n'importe quel domaine.

La [Figure 8-4](#) illustre les objets du 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. Groupez Utilisateur1 et Utilisateur2 dans le Groupe1. L'étendue de groupe de Groupe1 doit être Universel.
6. Ajoutez Groupe1 comme membre de l'objet Association 1 (A01), Priv1 comme objet Privilège dans A01, et RAC1 et RAC2 comme périphériques RAC dans A01.
7. Ajoutez Utilisateur3 comme membre de l'objet Association 2 (A02), Priv2 comme objet Privilège dans A02 et RAC2 comme périphérique RAC dans A02.

Configuration du schéma étendu d'Active Directory pour accéder à votre CMC

Avant d'utiliser Active Directory pour accéder à CMC, configurez le logiciel Active Directory et CMC :

1. Étendez le schéma Active Directory (voir [Extension du schéma Active Directory](#)).
2. Étendez le snap-in Utilisateurs et ordinateurs Active Directory (voir [Installation de l'extension Dell sur le snap-in Utilisateurs et ordinateurs Active Directory](#)).
3. Ajoutez des utilisateurs CMC et leurs privilèges à Active Directory (voir [Ajout d'utilisateurs CMC et de leurs privilèges à Active Directory](#)).
4. Activez SSL sur chaque contrôleur de domaine.
5. Configurez les propriétés Active Directory de CMC via l'interface Web CMC ou l'utilitaire RACADM (voir [Configuration de CMC avec le schéma étendu d'Active Directory et l'interface Web](#) ou [Configuration de CMC avec le schéma étendu d'Active Directory et RACADM](#)).

Extension du schéma Active Directory

En étendant votre schéma Active Directory, vous ajoutez une division opérationnelle Dell, des classes et des attributs de schéma, et des exemples d'objets Privilège et Association au schéma Active Directory. Pour étendre le schéma, vous devez avoir des privilèges d'administrateur de schéma pour le propriétaire de rôle FSMO contrôleur de schéma de la forêt de domaine.

Vous pouvez étendre votre schéma en utilisant une des méthodes suivantes :

1. l'utilitaire Dell Schema Extender ;
1. le fichier script LDIF.

Si vous utilisez le fichier script LDIF, la division opérationnelle Dell ne sera pas ajoutée au schéma.

Les fichiers LDIF et Dell Schema Extender sont situés sur votre DVD *Dell Systems Management Tools and Documentation* respectivement dans les répertoires suivants :

1. <lecteur de DVD>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\<type d'installation>\LDIF Files
1. <lecteur de DVD>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\<type d'installation>\Schema Extender

Pour utiliser les fichiers LDIF, consultez les instructions du fichier « Lisez-moi » qui se trouve dans le répertoire LDIF_Files. Pour obtenir des instructions sur l'utilisation de Dell Schema Extender pour étendre le schéma Active Directory, voir [Utilisation de Dell Schema Extender](#).

Vous pouvez copier et exécuter Schema Extender ou les fichiers LDIF depuis n'importe quel emplacement.

Utilisation de Dell Schema Extender



PRÉCAUTION : l'utilitaire Dell Schema Extender utilise le fichier SchemaExtenderOem.ini. Pour que l'utilitaire Dell Schema Extender fonctionne normalement, ne changez pas le nom de ce fichier.

1. Dans l'écran **Bienvenue**, cliquez sur **Suivant**.
2. Lisez et comprenez l'avertissement, 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 de schéma, utilisez la console de gestion de Microsoft (MMC) et le snap-in du schéma Active Directory pour vérifier ce qui suit :

- 1 Classes : voir du [Tableau 8-2](#) au [Tableau 8-7](#)
- 1 Attributs : voir le [Tableau 8-8](#)

Consultez votre documentation Microsoft pour des informations supplémentaires sur l'activation et l'utilisation du snap-in du schéma Active Directory MMC.

Tableau 8-2. Définitions de classe pour les classes ajoutées au schéma Active Directory

Nom de classe	Numéro d'identification d'objet (OID) attribué
dellRacDevice	1.2.840.113556.1.8000.1280.1.1.1.1
dellAssociationObject	1.2.840.113556.1.8000.1280.1.1.1.2
dellRACPrivileges	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 8-3. Classe dellRacDevice

OID	1.2.840.113556.1.8000.1280.1.1.1.1
Description	Représente le périphérique RAC de Dell. Le périphérique RAC doit être configuré comme dellRacDevice dans Active Directory. Cette configuration permet à CMC d'envoyer des requêtes de protocole LDAP (Lightweight Directory Access Protocol) à Active Directory.
Type de classe	Classe structurelle
SuperClasses	dellProduct
Attributs	dellSchemaVersion dellRacType

Tableau 8-4. Classe dellAssociationObject

OID	1.2.840.113556.1.8000.1280.1.1.1.2
Description	Représente l'objet Association de Dell. L'objet Association établit la connexion entre les utilisateurs et les périphériques.
Type de classe	Classe structurelle
SuperClasses	Groupe
Attributs	dellProductMembers dellPrivilegeMember

Tableau 8-5. Classe dellRAC4Privileges

OID	1.2.840.113556.1.8000.1280.1.1.1.3
Description	Définit les droits (privileges) d'autorisation pour le périphérique CMC.
Type de classe	Classe auxiliaire
SuperClasses	None (Aucune)
Attributs	dell sLoginUser dell sCardConfigAdmin dell sUserConfigAdmin dell sLogClearAdmin dell sServerResetUser dell sTestAlertUser dell sDebugCommandAdmin dellPermissionMask1 dellPermissionMask2

Tableau 8-6. Classe dellPrivileges

OID	1.2.840.113556.1.8000.1280.1.1.1.4
Description	Classe de conteneur pour les privilèges (droits d'autorisation) de Dell.
Type de classe	Classe structurelle
SuperClasses	Utilisateur
Attributs	dellRAC4Privileges

Tableau 8-7. Classe dellProduct

OID	1.2.840.113556.1.8000.1280.1.1.1.5
Description	Classe principale à partir de laquelle tous les produits Dell sont dérivés.
Type de classe	Classe structurelle
SuperClasses	Ordinateur
Attributs	dellAssociationMembers

Tableau 8-8. 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	FAUX
Nom unique : (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
Attribut : dellProductMembers	
Description : Liste des objets dellRacDevices appartenant à ce rôle. Cet attribut est le lien vers l'avant vers le lien vers l'arrière dellAssociationMembers.	
Numéro de lien : 12070	
OID : 1.2.840.113556.1.8000.1280.1.1.2.2	FAUX
Nom unique : (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
Attribut : dellIsCardConfigAdmin	
Description : VRAI si l'utilisateur a des droits de configuration de carte sur le périphérique.	
OID : 1.2.840.113556.1.8000.1280.1.1.2.4	VRAI
Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
Attribut : dellIsLoginUser	
Description : VRAI si l'utilisateur a des droits d'ouverture de session sur le périphérique.	
OID : 1.2.840.113556.1.8000.1280.1.1.2.3	VRAI
Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
Attribut : dellIsCardConfigAdmin	
Description : VRAI si l'utilisateur a des droits de configuration de carte sur le périphérique.	
OID : 1.2.840.113556.1.8000.1280.1.1.2.4	VRAI
Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
Attribut : dellIsUserConfigAdmin	
Description : VRAI si l'utilisateur a des droits d'administrateur et configuration des utilisateurs sur le périphérique.	
OID : 1.2.840.113556.1.8000.1280.1.1.2.5	VRAI
Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
Attribut : dellIsLogClearAdmin	
Description : VRAI si l'utilisateur a des droits d'administrateur et effacement des journaux sur le périphérique.	
OID : 1.2.840.113556.1.8000.1280.1.1.2.6	VRAI

Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
Attribut : dellIsServerResetUser	
Description : VRAI si l'utilisateur a des droits de réinitialisation de serveur sur le périphérique.	
OID : 1.2.840.113556.1.8000.1280.1.1.2.7	VRAI
Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
Attribut : dellIsTestAlertUser	
Description : VRAI si l'utilisateur a des droits d'utilisateur et test d'alertes sur le périphérique.	
OID : 1.2.840.113556.1.8000.1280.1.1.2.10	VRAI
Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
Attribut : dellIsDebugCommandAdmin	
Description : VRAI si l'utilisateur a des droits d'administrateur pour la commande de débogage sur le périphérique.	
OID : 1.2.840.113556.1.8000.1280.1.1.2.11	VRAI
Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	
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	VRAI
Case Ignore String(LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	
Attribut : dellRacType	
Description : cet attribut est le type de RAC actuel pour l'objet dellRacDevice et le lien vers l'arrière vers le lien vers l'avant dellAssociationObjectMembers.	
OID : 1.2.840.113556.1.8000.1280.1.1.2.13	VRAI
Case Ignore String(LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	
Attribut : dellAssociationMembers	
Description : liste des dellAssociationObjectMembers appartenant à ce produit. Cet attribut est le lien vers l'arrière vers l'attribut lié dellProductMembers.	
ID de lien : 12071	
OID : 1.2.840.113556.1.8000.1280.1.1.2.14	FAUX
Nom distingué (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
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 sur le snap-in Utilisateurs et ordinateurs Active Directory

Lorsque vous étendez le schéma dans Active Directory, vous devez également développer 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.

Lors de l'installation de Systems Management Software à l'aide du DVD *Dell Systems Management Tools and Documentation*, vous pouvez étendre le snap-in en sélectionnant l'option **Extension Dell sur le snap-in Utilisateurs et ordinateurs Active Directory** au cours de la procédure d'installation. Voir le *Guide d'installation de Dell OpenManage Server Administrator* et le *Guide d'installation du logiciel de la station de gestion de Dell OpenManage* pour des instructions supplémentaires sur l'installation du logiciel de gestion des systèmes.

Pour plus d'informations sur le snap-in Utilisateurs et ordinateurs Active Directory, voir la documentation Microsoft.

Installation du pack administrateur

Vous devez installer le pack administrateur sur tous les systèmes qui gèrent les objets CMC d'Active Directory. Si vous n'installez pas le pack administrateur, vous ne pouvez pas visualiser l'objet RAC Dell dans le conteneur.

Ouverture du snap-in Utilisateurs et ordinateurs Active Directory

Pour ouvrir le snap-in Utilisateurs et ordinateurs Active Directory :

1. Si vous avez ouvert une session sur le contrôleur de domaine, cliquez sur **Démarrer Outils d'administration** → **Utilisateurs et ordinateurs Active**

Directory.

Si vous n'avez pas ouvert une session sur le contrôleur de domaine, le pack administrateur Microsoft approprié doit être installé sur votre système local. Pour installer ce pack administrateur, cliquez sur **Démarrer**→ **Exécuter**, tapez MMC et appuyez sur <Entrée>.

Ceci ouvre la console de gestion Microsoft (MMC).

2. Dans la fenêtre **Console 1**, cliquez sur **Fichier** (ou sur **Console** sur les systèmes exécutant Windows 2000).
3. Cliquez sur **Ajouter/Supprimer un snap-in**.
4. Sélectionnez le snap-in **Utilisateurs et ordinateurs Active Directory**, puis cliquez sur **Ajouter**.
5. Cliquez sur **Fermer**, puis sur **OK**.

Ajout d'utilisateurs CMC et de leurs privilèges à Active Directory

Le snap-in Utilisateurs et ordinateurs Active Directory étendu par Dell vous permet d'ajouter des utilisateurs CMC et des privilèges en créant des objets RAC, Association et Privilège. Pour ajouter chaque type d'objet :

1. Créer un objet Périphérique RAC.
2. Créer un objet Privilège.
3. Créer un objet Association.
4. Ajouter des objets à un objet Association.

Création d'un objet Périphérique RAC

1. Dans la fenêtre **Racine de la console MMC**, cliquez avec le bouton droit de la souris sur un conteneur.
2. Sélectionnez **Nouveau**→ **Objet RAC Dell**.
La fenêtre **Nouvel objet** apparaît.
3. Tapez un nom pour le nouvel objet. Ce nom doit être identique au nom CMC saisi à l'étape 8a de [Configuration de CMC avec le schéma étendu d'Active Directory et l'interface Web](#).
4. Sélectionnez **Objet Périphérique RAC**.
5. Cliquez sur **OK**.

Création d'un objet Privilège

 **REMARQUE** : un objet Privilège doit être créé dans le même domaine que l'objet Association associé.

1. Dans la fenêtre **Racine de la console (MMC)**, cliquez avec le bouton droit de la souris sur un conteneur.
2. Sélectionnez **Nouveau**→ **Objet RAC Dell**.
La fenêtre **Nouvel objet** apparaît.
3. Tapez un nom pour le nouvel objet.
4. Sélectionnez **Objet Privilège**.
5. Cliquez sur **OK**.
6. Cliquez avec le bouton droit de la souris sur l'objet Privilège que vous avez créé et sélectionnez **Propriétés**.
7. Cliquez sur l'onglet **Privilèges RAC** et sélectionnez les privilèges que vous souhaitez attribuer à l'utilisateur. Pour plus d'informations sur les privilèges utilisateur CMC, voir [User Types](#).

Création d'un objet Association

L'objet Association est dérivé d'un groupe et doit contenir un type de groupe. L'étendue de l'association spécifie le type de groupe de sécurité pour l'objet Association. Quand vous créez un objet Association, vous devez choisir l'étendue de l'association qui s'applique au type d'objet que vous avez l'intention d'ajouter.

Par exemple, si vous sélectionnez **Universel**, les objets Association sont uniquement disponibles lorsque le domaine d'Active Directory fonctionne en mode natif ou supérieur.

1. Dans la fenêtre **Racine de la console** (MMC), cliquez avec le bouton droit de la souris sur un conteneur.
2. Sélectionnez **Nouveau** → **Objet RAC Dell**.
Cette action ouvre la fenêtre **Nouvel objet**.
3. Tapez un nom pour le nouvel objet.
4. Sélectionnez **Objet Association**.
5. Sélectionnez l'étendue de l'**objet Association**.
6. Cliquez sur **OK**.

Ajout d'objets à un objet Association

En utilisant la fenêtre **Propriétés de l'objet Association**, vous pouvez associer des utilisateurs, des groupes d'utilisateurs, des objets Privilège et des périphériques RAC ou des groupes de périphériques RAC. Si votre système s'exécute sous Windows 2000 ou supérieur, utilisez les groupes universels pour répartir sur des domaines vos utilisateurs ou vos objets RAC.

Vous pouvez ajouter des groupes d'utilisateurs et de périphériques RAC. La procédure de création de groupes associés à Dell et de groupes non associés à Dell est identique.

Ajout d'utilisateurs ou de 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. Tapez le nom de l'utilisateur ou du groupe d'utilisateurs et cliquez sur **OK**.

Cliquez sur l'onglet **Objet Privilège** pour ajouter l'objet Privilège à l'association qui définit les privilèges de l'utilisateur ou du groupe d'utilisateurs durant l'authentification auprès d'un périphérique RAC. Vous ne pouvez ajouter qu'un seul objet Privilège à un objet Association.

Ajout de privilèges

1. Sélectionnez l'onglet **Objet Privilège** et cliquez sur **Ajouter**.
2. Tapez le nom de l'objet Privilège et cliquez sur **OK**.

Cliquez sur l'onglet **Produits** pour ajouter un ou plusieurs périphériques RAC à l'association. Les périphériques associés spécifient les périphériques RAC connectés au réseau qui sont disponibles pour les utilisateurs ou les groupes d'utilisateurs définis. Vous pouvez ajouter plusieurs périphériques RAC à un 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. Tapez le nom du périphérique RAC ou du groupe de périphériques RAC et cliquez sur **OK**.
3. Dans la fenêtre **Propriétés**, cliquez sur **Appliquer**, puis sur **OK**.

Configuration de CMC avec le schéma étendu d'Active Directory et l'interface Web

1. Ouvrez une session sur l'interface Web de CMC.
2. Sélectionnez **Châssis** dans l'arborescence.
3. Cliquez sur **Authentification utilisateurs** → **Services d'annuaire**.

La page **Services d'annuaire** s'affiche.

4. Sélectionnez **Microsoft Active Directory (Schéma étendu)**.

5. Dans la section **Paramètres communs** :

- a. Assurez-vous d'avoir coché la case **Active Directory activé**.
- b. Tapez le **nom de domaine racine**.

 **REMARQUE** : le **nom de domaine racine** doit être un nom de domaine valide qui respecte la convention d'attribution des noms *x.y*, où *x* est une chaîne ASCII de 1 à 256 caractères sans espace, et où *y* est un type de domaine valide tel que *com*, *edu*, *gov*, *int*, *mil*, *net* ou *org*.

- c. Tapez le **Délai d'attente** en secondes. **Plage de configuration** : 15 à 300 secondes. **Par défaut** : 90 secondes

6. **Facultatif** : si vous voulez que l'appel dirigé recherche le contrôleur de domaine et le catalogue global, cochez la case **Chercher le serveur AD à rechercher (facultatif)**, puis :

- a. Dans le champ de texte **Contrôleur de domaine**, tapez le nom du serveur sur lequel est installé le service Active Directory.
- b. Dans le champ de texte **Catalogue global**, tapez l'emplacement du catalogue global sur le contrôleur de domaine d'Active Directory. Le catalogue global fournit une ressource pour rechercher une forêt Active Directory.

 **REMARQUE** : la définition de l'adresse IP 0.0.0.0 désactive la recherche d'un serveur par CMC.

 **REMARQUE** : vous pouvez spécifier une liste de serveurs de contrôleur de domaine ou de catalogue global séparés 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.

7. Dans la section **Paramètres du schéma étendu** :

- a. Tapez le **nom du dispositif CMC**. Le **nom CMC** identifie de manière unique la carte CMC dans Active Directory. Le **nom CMC** doit être identique au nom de domaine du nouvel objet CMC que vous avez créé dans votre contrôleur de domaine. Le **nom CMC** doit être une chaîne ASCII de 1 à 256 caractères sans espace.
- b. Tapez le **nom de domaine CMC** (exemple : *cmc.com*). Le **nom de domaine CMC** est le nom DNS (chaîne) du domaine sur lequel réside l'objet CMC d'Active Directory. Le nom doit être un nom de domaine valide sous la forme *x.y*, où *x* est une chaîne ASCII de 1 à 256 caractères sans espace entre les caractères, et où *y* est un type de domaine valide comme *com*, *edu*, *gov*, *int*, *mil*, *net* ou *org*.

8. Cliquez sur **Appliquer** pour enregistrer vos paramètres.

 **REMARQUE** : vous devez appliquer vos paramètres avant de passer à l'étape suivante, au cours de laquelle vous allez accéder à une autre page. Si vous n'appliquez pas les paramètres, vous perdrez les paramètres que vous avez saisis lorsque vous naviguerez vers la page suivante.

9. Dans la section **Gérer les certificats**, tapez le chemin du fichier du certificat dans le champ de texte, ou cliquez sur **Parcourir** pour sélectionner le fichier de certificat. Cliquez sur le bouton **Téléverser** pour transférer le fichier vers CMC.

 **REMARQUE** : la valeur **Chemin du fichier** affiche le chemin de fichier relatif du certificat que vous téléversez. Vous devez taper le chemin de fichier absolu, y compris le chemin et le nom de fichier complets et l'extension du fichier.

La validation du certificat SSL est requise par défaut. Il y a un nouveau paramètre dans le groupe **RACADM cfgActiveDirectory** et dans l'interface graphique pour désactiver la vérification du certificat.

PRÉCAUTION : la désactivation de ce certificat est dangereuse.

Pour activer la validation du certificat SSL (par défaut) :

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 1
```

Pour désactiver la validation du certificat SSL :

```
racadm config -g cfgActiveDirectory -o cfgADCertValidationEnable 0
```

Les certificats SSL du contrôleur de domaine doivent être signés par l'autorité de certification racine. Le certificat signé par l'autorité de certification racine doit être disponible sur la station de gestion accédant à CMC.

10. Cliquez sur **Appliquer**. Le serveur Web CMC redémarre automatiquement lorsque vous cliquez sur **Appliquer**.

11. Ouvrez à nouveau une session dans l'interface Web CMC.

12. Sélectionnez **Châssis** dans l'arborescence du système, cliquez sur l'onglet **Réseau**, puis cliquez sur le sous-onglet **Réseau**. La page **Configuration réseau** s'affiche.
13. Si **Utiliser DHCP (pour l'adresse IP de l'interface réseau CMC)** est activé (coché), effectuez l'une des opérations suivantes :
 - 1 Sélectionnez **Utiliser DHCP pour obtenir des adresses de serveur DNS** pour que le serveur DHCP puisse obtenir automatiquement les adresses du serveur DNS, ou
 - 1 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.
14. Cliquez sur **Appliquer les modifications**.

La configuration de la fonctionnalité Active Directory CMC avec schéma étendu est terminée.

Configuration de CMC avec le schéma étendu d'Active Directory et RACADM

Utilisez les commandes suivantes pour configurer la fonctionnalité Active Directory CMC avec le schéma étendu via l'outil d'interface de ligne de commande RACADM plutôt que via l'interface Web.

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

```
racadm config -g cfgActiveDirectory -o cfgADEnable 1

racadm config -g cfgActiveDirectory -o cfgADType 1

racadm config -g cfgActiveDirectory -o cfgADRacDomain <nom de domaine CMC pleinement qualifié>

racadm config -g cfgActiveDirectory -o cfgADRacDomain <nom de domaine rac pleinement qualifié>

racadm config -g cfgActiveDirectory -o cfgADRacName <nom de domaine CMC>

racadm sslcertupload -t 0x2 -f <certificat d'une autorité de certification racine ADS> -r

racadm sslcertdownload -t 0x1 -f <certificat SSL CMC>
```

 **REMARQUE** : vous pouvez utiliser cette commande via la RACADM distante uniquement. Pour plus d'informations sur le RACADM distant, voir [Accès à distance à RACADM](#).

Facultatif : Si vous voulez 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, tapez 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 ne correspond pas au nom du serveur spécifié. Ceci est particulièrement utile si vous êtes un administrateur CMC car cela vous permet de saisir un nom d'hôte et une adresse IP.

Après avoir activé l'option **Spécifier un serveur**, vous pouvez spécifier un serveur LDAP et un catalogue global avec les adresses IP ou les noms de domaine complets (FQDN) des serveurs. Les FQDN se composent des noms d'hôte et des noms de domaine des serveurs.

Pour spécifier un serveur LDAP, tapez :

```
racadm config -g cfgActiveDirectory -o cfgADDomainController <Adresse IP du contrôleur de domaine AD>
```

Pour spécifier un serveur de catalogue global, tapez :

```
racadm config -g cfgActiveDirectory -o cfgADGlobalCatalog <Adresse IP du catalogue global AD>
```

 **REMARQUE** : la définition de l'adresse IP 0.0.0.0 désactive la recherche d'un serveur par CMC.

 **REMARQUE** : vous pouvez spécifier une liste de serveurs LDAP ou de catalogue global séparés 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 :

- 1 Si DHCP est activé sur CMC et que vous voulez utiliser l'adresse DNS obtenue automatiquement par le serveur DHCP, tapez la commande suivante :

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

- 1 Si le protocole DHCP est désactivé sur CMC ou s'il est activé mais que vous voulez spécifier manuellement l'adresse IP DNS, tapez les commandes suivantes :

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

```
racadm config -g cfgLanNetworking -o cfgDNSServer1 <adresse IP de DNS principale>
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer2 <adresse IP de DNS secondaire>
```

La configuration de la fonctionnalité de schéma étendu est terminée.

Questions les plus fréquentes

Tableau 8-9. Utilisation de CMC avec Active Directory : questions les plus fréquentes

Question	Réponse
Puis-je ouvrir une session sur CMC en utilisant Active Directory sur plusieurs arborescences ?	Oui. L'algorithme de requête Active Directory de CMC prend en charge plusieurs arborescences d'une seule forêt.
L'ouverture d'une session sur CMC avec Active Directory est-elle possible en mode mixte (c'est-à-dire, avec les contrôleurs de domaine de la forêt s'exécutant sur des systèmes d'exploitation différents, comme Microsoft Windows 2000 ou Windows Server 2003) ?	Oui. En mode mixte, tous les objets utilisés par la procédure de requête CMC (notamment, l'utilisateur, l'objet Périphérique RAC et l'objet Association) doivent figurer 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 plusieurs environnements de domaine ?	Oui. Le niveau de la fonction de forêt de domaine doit être en mode natif ou Windows 2003. En outre, les groupes parmi l'objet Association, les objets Utilisateur RAC et les objets Périphérique RAC (y compris l'objet Association) doivent être des groupes universels.
Ces objets étendus par Dell (objets Association Dell, Périphérique RAC Dell et Privilège Dell) peuvent-ils appartenir à différents domaines ?	L'objet Association et l'objet Privilège doivent appartenir au même domaine. Le snap-in Utilisateurs et ordinateurs Active Directory étendu par Dell vous force à créer ces deux objets dans le même domaine. D'autres objets peuvent appartenir à différents domaines.
Y a-t-il des restrictions concernant la configuration SSL du contrôleur de domaine ?	Oui. Tous les certificats SSL pour les serveurs Active Directory de la forêt doivent être signés par le même certificat signé par l'autorité de certification racine car CMC vous permet uniquement de télécharger un seul certificat SSL signé par une autorité de certification de confiance.
J'ai créé un nouveau certificat de RAC et je l'ai téléversé ; depuis, l'interface Web ne se lance pas.	Si vous avez utilisé les services de certificats Microsoft pour générer le certificat RAC, vous avez peut-être choisi Certificat d'utilisateur par inadvertance au lieu de Certificat Web lorsque vous avez créé le certificat. Pour récupérer, générez une RSC, puis créez un nouveau certificat Web avec les services de certificats Microsoft et téléversez-le avec les commandes RACADM suivantes : <pre>racadm sslcsrgen [-g] [-f {nom de fichier}] racadm sslcertupload -t 1 -f {web_sslcert}</pre>
Que puis-je faire si je n'arrive pas à ouvrir une session sur CMC avec l'authentification Active Directory ? Comment puis-je résoudre ce problème ?	<ol style="list-style-type: none"> 1. Assurez-vous que vous utilisez le nom de domaine utilisateur correct pendant l'ouverture de session, et non le nom NetBIOS. 2. Si vous avez un compte utilisateur CMC local, ouvrez une session CMC à l'aide de vos références locales. <p>Une fois la session ouverte, effectuez les étapes suivantes :</p> <ol style="list-style-type: none"> a. Vérifiez que vous avez coché la case Activer Active Directory sur la page de configuration d'Active Directory de CMC. b. Vérifiez que le paramètre DNS est correct sur la page de configuration du réseau CMC. c. Vérifiez que vous avez téléversé le certificat Active Directory sur CMC à partir du certificat signé par l'autorité de certification racine d'Active Directory. d. Vérifiez les certificats SSL des contrôleurs de domaine pour vous assurer qu'ils n'ont pas expiré. e. Vérifiez que le nom CMC, le nom de domaine racine et le nom de domaine CMC correspondent à la configuration de votre environnement Active Directory. f. Assurez-vous que le mot de passe CMC contient 127 caractères au maximum. Tandis que CMC peut prendre en charge des mots de passe allant jusqu'à 256 caractères, Active Directory prend uniquement en charge les mots de passe d'un maximum de 127 caractères.

Configuration de la connexion directe

Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows 7 et Windows Server 2008 peuvent utiliser Kerberos, un protocole d'authentification réseau, comme méthode d'authentification permettant aux utilisateurs qui se sont connectés au domaine de se connecter automatiquement ou directement à des applications ultérieures telles qu'Exchange.

Dès la version 2.10, CMC peut utiliser Kerberos pour prendre en charge deux types supplémentaires de mécanismes d'ouverture de session : la connexion directe et l'ouverture de session par carte à puce. Pour l'ouverture de session par connexion directe, CMC utilise les informations d'identification du système

client, qui sont mises en mémoire cache par le système d'exploitation lorsque vous ouvrez une session avec un compte Active Directory valide.

 **REMARQUE** : la sélection d'une méthode d'ouverture de session ne définit pas les attributs de règles par rapport à d'autres interfaces d'ouverture de session, par exemple SSH. Vous devez également définir d'autres attributs de règles pour les autres interfaces d'ouverture de session. Si vous souhaitez désactiver toutes les autres interfaces d'ouverture de session, naviguez vers la page **Services** et désactivez toutes (ou certaines) interfaces d'ouverture de session.

Configuration système requise

Pour utiliser l'authentification Kerberos, votre réseau doit inclure les éléments suivants :

- 1 Serveur DNS
- 1 Serveur Microsoft Active Directory

 **REMARQUE** : si vous utilisez Active Directory sous Windows 2003, assurez-vous que les derniers service pack et les derniers correctifs sont bien installés sur le système client. Si vous utilisez Active Directory sous Windows 2008, vérifiez que vous avez bien installé SP1 avec les correctifs suivants :

Windows6.0-KB951191-x86.msu pour l'utilitaire KTPASS. Sans ce correctif, l'utilitaire génère des fichiers keytab *erronés*.
Windows6.0-KB957072-x86.msu pour utiliser les transactions GSS_API et SSL pendant une liaison LDAP.

- 1 Centre de distribution de clés Kerberos (fourni avec le logiciel du serveur Active Directory Server)
- 1 Serveur DHCP (recommandé)
- 1 La zone inverse du serveur DNS doit comporter une entrée pour le serveur Active Directory et pour CMC

Systemes clients

- 1 Pour l'ouverture de session par carte à puce uniquement, Microsoft Visual C++ 2005 redistribuable doit être installé sur le système client. Pour plus d'informations, voir www.microsoft.com/downloads/details.aspx?FamilyID=32BC1BEEA3F9-4C13-9C99-220B62A191EE&displaylang=en
- 1 Pour la connexion directe et l'ouverture de session par carte à puce, le système client doit faire partie du domaine Active Directory et du royaume Kerberos.

CMC

- 1 CMC doit comporter la version 2.10 du micrologiciel ou une version ultérieure
- 1 Chaque contrôleur CMC doit posséder un compte Active Directory
- 1 CMC doit faire partie du domaine Active Directory et du royaume Kerberos

Configuration des paramètres

Configuration requise

- 1 Le royaume Kerberos et le centre de distribution de clés (KDC) pour Active Directory (AD) ont été configurés (ksetup).
- 1 Une infrastructure NTP et DNS robuste pour éviter des problèmes relatifs à la dérive d'horloge et à la recherche inverse
- 1 Le groupe de rôles CMC avec schéma standard avec membres autorisés

Configuration d'Active Directory

Dans la boîte de dialogue **Propriétés CMC** sous la section des options **Comptes**, configurez les paramètres suivants :

- 1 **Le compte est fiable pour la délégation** : actuellement, CMC n'utilise pas les informations d'identification transférées qui sont créées lorsque cette option est sélectionnée. Vous pouvez ou non sélectionner cette option selon les besoins des autres services.
- 1 **Le compte est sensible et ne peut pas être délégué** : vous pouvez ou non sélectionner cette option selon les besoins des autres services.
- 1 **Types de cryptage DES de l'utilisateur Kerberos pour le compte** : sélectionnez cette option.
- 1 **Ne pas demander la pré-authentification Kerberos** : ne sélectionnez pas cette option.

Exécuter l'utilitaire ktpass (partie de Microsoft Windows) sur le contrôleur de domaine (serveur Active Directory) sur lequel vous souhaitez mapper CMC à un compte utilisateur dans Active Directory. Par exemple,

```
C:\>ktpass -princ HTTP/cmcname.domain_name.com@REALM_NAME.COM -mapuser dracname -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -pass * -out c:\krbkeytab
```

 **REMARQUE** : cmcname.domainname.com doit être en minuscules comme requis par RFC et le nom du ROYAUME (@REALM_NAME) doit être en majuscules. CMC prend en outre en charge le type de cryptographie DES-CBC-MD5 pour l'authentification Kerberos.

Cette procédure génère un fichier keytab que vous devez téléverser sur CMC.

 **REMARQUE** : le fichier keytab, qui contient une clé de cryptage, doit être conservé en lieu sûr. Pour plus d'informations sur l'utilitaire `ktpass`, consultez le site Web de Microsoft à l'adresse : technet2.microsoft.com/windowsserver/en/library/64042138-9a5a-4981-84e9-d576a8db0d051033.msp?mfr=true.

Configuration de CMC

 **REMARQUE** : les étapes de configuration décrites dans cette section s'appliquent uniquement à l'accès Web CMC.

Configurez CMC pour qu'il utilise le(s) groupe(s) de rôles avec schéma standard configuré(s) dans Active Directory. Pour plus d'informations, voir [Configuration du schéma standard d'Active Directory pour accéder à CMC](#).

Téléversement du fichier keytab Kerberos

Le fichier keytab Kerberos sert d'informations d'authentification de nom d'utilisateur et de mot de passe CMC auprès du centre de données Kerberos (KDC), qui à son tour autorise l'accès à Active Directory. Chaque contrôleur CMC du royaume Kerberos doit être enregistré auprès d'Active Directory et doit comporter un fichier keytab unique.

Pour téléverser le fichier keytab :

1. Accédez à l'onglet **Authentification utilisateur** → sous-onglet **Services d'annuaire**. Vérifiez que **Microsoft Active Directory Schéma standard** ou **étendu** est sélectionné. Si ce n'est pas le cas, sélectionnez votre préférence et cliquez sur **Appliquer**.
2. Cliquez sur **Parcourir** dans la section **Téléversement du fichier keytab Kerberos**, naviguez vers le dossier dans lequel vous avez enregistré le fichier keytab, puis cliquez sur **Téléverser**.

Lorsque le téléversement est terminé, une zone de message apparaît, indiquant la réussite ou l'échec du téléversement.

Activation de la connexion directe

1. Cliquez sur l'onglet **Sécurité réseau de Chassis Management Controller** → **Active Directory** → **Configurer Active Directory**.

La page **Configuration et gestion d'Active Directory** s'affiche.

2. Sur la page **Configuration et gestion d'Active Directory**, sélectionnez :
 - 1 Connexion directe : cette option vous permet d'ouvrir une session sur CMC à l'aide des informations d'identification mises en mémoire cache obtenues lorsque vous ouvrez une session sur Active Directory.

 **REMARQUE** : toutes les interfaces hors bande de la ligne de commande, y compris Secure Shell (SSH), Telnet, série et RACADM distant, restent inchangées pour cette option

3. Effectuez un défilement vers le bas de la page et cliquez sur **Appliquer**.

Vous pouvez tester Active Directory avec l'authentification Kerberos en utilisant la fonctionnalité de test des commandes de l'interface de ligne de commande.

```
testfeature -f adkrb -u <utilisateur>@<domaine>
```

où utilisateur correspond à un compte d'utilisateur Active Directory valide.

La réussite d'une commande indique que CMC est en mesure d'acquérir des références Kerberos et d'accéder au compte Active Directory de l'utilisateur. En cas d'échec de la commande, résolvez l'erreur et répétez la commande. Pour des informations supplémentaires, voir le *Guide de référence de la ligne de commande pour iDRAC6 et CMC* à l'adresse support.dell.com/manuals.

Configuration du navigateur pour l'ouverture de session par connexion directe

La connexion directe est prise en charge par les versions 6.0 et ultérieures d'Internet Explorer et par les versions 3.0 et ultérieures de Firefox.

 **REMARQUE** : les instructions suivantes s'appliquent uniquement si CMC utilise la connexion directe avec l'authentification Kerberos.

Internet Explorer

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 **Advanced** (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/utilisateurs de ce domaine.

Mozilla Firefox

1. Dans Firefox, saisissez **about:config** dans la barre d'adresses.

 **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**, tapez `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**.

Ouverture d'une session sur CMC avec la connexion directe

 **REMARQUE** : vous ne pouvez pas utiliser l'adresse IP pour ouvrir une session avec la connexion directe ou par carte à puce. Kerberos valide vos informations d'identification par rapport au nom de domaine pleinement qualifié (FQDN).

1. Ouvrez une session sur le système client avec votre compte réseau.
2. Accédez à la page Web de CMC via

`https://<nom_cmc.nom-domaine>`

Par exemple, `cmc-6G2WXP1.cmcad.lab`

où `cmc-6G2WXP1` correspond à `nom_cmc`

`cmcad.lab` à `nom-domaine`.

 **REMARQUE** : si vous avez changé le numéro de port HTTPS par défaut (port 80), accédez à la page Web CMC via `<nomcmc.nom-domaine:<numéro de port>`, où `nomcmc` correspond au nom d'hôte CMC de CMC, `nom-domaine` au nom du domaine et `numéro de port` au numéro de port HTTPS.

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

3. Cliquez sur **Ouvrir une session**.

CMC vous ouvre une session à l'aide des informations d'identification Kerberos qui ont été mises en mémoire cache par votre navigateur lorsque vous avez ouvert une session avec votre compte Active Directory valide. En cas d'échec de l'ouverture de session, le navigateur est redirigé vers la page d'ouverture de session 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.

Configuration de l'authentification bifactorielle par carte à puce

Les schémas d'authentification standard utilisent le nom d'utilisateur et le mot de passe pour authentifier les utilisateurs. Pour sa part, l'authentification bifactorielle offre un niveau de sécurité supérieur en demandant aux utilisateurs d'avoir un mot de passe ou un code PIN et une carte physique comprenant une clé privée ou un certificat numérique. Kerberos, un protocole d'authentification réseau, utilise ce mécanisme d'authentification bifactorielle qui permet aux systèmes de prouver leur authenticité. Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista et Windows Server 2008 utilisent Kerberos comme méthode d'authentification préférée. Dès la version 2.10, CMC peut utiliser Kerberos pour prendre en charge l'ouverture de session par carte à puce.

 **REMARQUE** : la sélection d'une méthode d'ouverture de session ne définit pas les attributs de règles par rapport à d'autres interfaces d'ouverture de session, par exemple SSH. Vous devez également définir d'autres attributs de règles pour les autres interfaces d'ouverture de session. Si vous souhaitez désactiver toutes les autres interfaces d'ouverture de session, naviguez vers la page **Services** et désactivez toutes (ou certaines) interfaces d'ouverture de session.

Configuration système requise

Les [Configurations requises](#) pour la carte à puce sont les mêmes que pour la connexion directe.

Configuration des paramètres

Les [Configurations requises](#) pour la carte à puce sont les mêmes que pour la connexion directe.

Configuration d'Active Directory

1. Configurez le royaume Kerberos et le centre de distribution de clés (KDC) pour Active Directory, s'ils ne sont pas déjà configurés (ksetup).

 **REMARQUE** : mettez en place une infrastructure NTP et DNS robuste pour éviter des problèmes relatifs à la dérive d'horloge et à la recherche inverse.

2. Créez des utilisateurs Active Directory pour chaque contrôleur CMC, configurés pour utiliser le cryptage DES Kerberos, mais non la préauthentification.
3. Enregistrez les utilisateurs CMC auprès du centre de distribution de clés avec Ktpass (ceci génère également une clé pour le téléversement sur CMC).

Configuration de CMC

 **REMARQUE** : les étapes de configuration décrites dans cette section s'appliquent uniquement à l'accès Web CMC.

Configurez CMC pour qu'il utilise le(s) groupe(s) de rôles avec schéma standard configuré(s) dans Active Directory. Pour plus d'informations, voir [Configuration du schéma standard d'Active Directory pour accéder à CMC](#).

Téléversement du fichier keytab Kerberos

Le fichier keytab Kerberos sert d'informations d'authentification de nom d'utilisateur et de mot de passe CMC auprès du centre de données Kerberos (KDC), qui à son tour autorise l'accès à Active Directory. Chaque contrôleur CMC du royaume Kerberos doit être enregistré auprès d'Active Directory et doit comporter un fichier keytab unique.

Pour téléverser le fichier keytab :

1. Accédez à l'onglet **Authentification utilisateur** → sous-onglet **Services d'annuaire**. Vérifiez que **Microsoft Active Directory Schéma standard** ou **étendu** est sélectionné. Si ce n'est pas le cas, sélectionnez votre préférence et cliquez sur **Appliquer**.
2. Cliquez sur **Parcourir** dans la section **Téléversement du fichier keytab Kerberos**, naviguez vers le dossier dans lequel vous avez enregistré le fichier keytab, puis cliquez sur **Téléverser**.

Lorsque le téléversement est terminé, une zone de message apparaît, indiquant la réussite ou l'échec du téléversement.

Activation de l'authentification par carte à puce

1. Accédez à l'onglet **Authentification utilisateur** → sous-onglet **Services d'annuaire**. Vérifiez que **Microsoft Active Directory Schéma standard** ou **étendu** est sélectionné.
2. Dans la section **Paramètres courants** :
 - 1 Carte à puce : cette option nécessite d'insérer une carte à puce dans le lecteur et de saisir le code PIN.

 **REMARQUE** : toutes les interfaces hors bande de la ligne de commande, y compris Secure Shell (SSH), Telnet, série et RACADM distant, restent inchangées pour cette option

3. Défilez vers le bas de la page et cliquez sur **Appliquer**.

Vous pouvez tester Active Directory avec l'authentification Kerberos en utilisant la fonctionnalité de test des commandes de l'interface de ligne de commande.

Entrez :

```
testfeature -f adkrb -u <utilisateur>@<domaine>
```

où utilisateur correspond à un compte d'utilisateur Active Directory valide.

La réussite d'une commande indique que CMC est en mesure d'acquiescer des références Kerberos et d'accéder au compte Active Directory de l'utilisateur. En cas d'échec de la commande, résolvez l'erreur et répétez la commande. Pour plus d'informations, consultez la documentation de la commande RACADM testfeature.

Configuration du navigateur pour l'ouverture de session par carte à puce

Mozilla Firefox

CMC 2.10 ne prend pas en charge l'ouverture de session par carte à puce via le navigateur Firefox.

Internet Explorer

Assurez-vous que le navigateur Internet est bien configuré pour télécharger des plug-in Active-X.

Ouverture de session sur CMC avec la carte à puce

 **REMARQUE** : vous ne pouvez pas utiliser l'adresse IP pour ouvrir une session avec la connexion directe ou par carte à puce. Kerberos valide vos informations d'identification par rapport au nom de domaine pleinement qualifié (FQDN).

1. Ouvrez une session sur le système client avec votre compte réseau.

2. Accédez à la page Web de CMC via

`https://<nomcmc.nom-domaine>`

Par exemple, `cmc-6G2WXP1.cmcad.lab`

où `cmc-6G2WXP1` correspond à `nom_cmc`

`cmcad.lab` à `nom-domaine`.

 **REMARQUE** : si vous avez changé le numéro de port HTTPS par défaut (port 80), accédez à la page Web CMC via `<nomcmc.nom-domaine:<numéro de port>`, où `nomcmc` correspond au nom d'hôte CMC de CMC, `nom-domaine` au nom du domaine et `numéro de port` au numéro de port HTTPS.

La page **Connexion directe CMC** apparaît et vous invite à insérer la carte à puce.

3. Insérez la carte à puce dans le lecteur et cliquez sur **OK**.

La boîte de dialogue contextuelle **Code PIN** s'affiche.

4. Facultativement, sélectionnez un délai de session. Il s'agit de la durée pendant laquelle vous restez connecté sans activité. La valeur par défaut est définie comme le délai d'inactivité du service Web. Voir Configuration des services pour plus de détails.

5. Saisissez le code PIN, puis cliquez sur **OK**.

Résolution des problèmes liés à l'ouverture de session par carte à puce

Les astuces suivantes vous permettent de déboguer une carte à puce inaccessible :

Le plug-in ActiveX est incapable de détecter le lecteur de cartes à puce

Vérifiez que la carte à puce est bien prise en charge sur le système d'exploitation Microsoft Windows. Windows prend en charge un nombre limité de fournisseurs de services cryptographiques (CSP) de cartes à puce.

Astuce : en règle générale, pour vérifier si les CSP de carte à puce sont présentes sur un client donné, insérez la carte à puce dans le lecteur lorsque l'écran d'ouverture de session de Windows apparaît (Ctrl-Alt-Suppr) et vérifiez si Windows détecte bien la carte à puce et affiche la boîte de dialogue Code PIN.

Code NIP de la carte à puce incorrect

Vérifiez si la carte à puce a été bloquée suite à un nombre trop élevé de tentatives avec un code PIN incorrect. Dans ces cas, l'émetteur de la carte à puce dans l'organisation peut vous aider à obtenir une nouvelle carte à puce.

Impossible d'ouvrir une session sur CMC en tant qu'utilisateur Active Directory

Si vous ne parvenez pas à ouvrir une session sur CMC en tant qu'utilisateur Active Directory, essayez d'ouvrir une session sur CMC sans activer l'ouverture de session par carte à puce. Vous avez également la possibilité de désactiver l'ouverture de session par carte à puce via la RACADM locale à l'aide des commandes suivantes :

```
racadm config -g cfgActiveDirectory -o cfgADSCLEnable 0
```

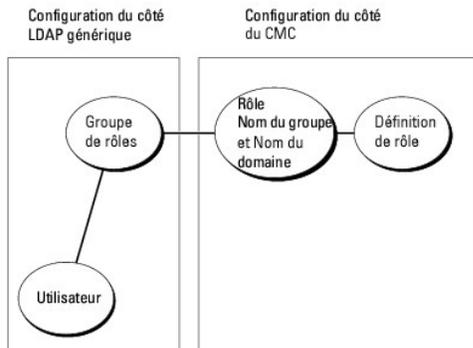
```
racadm config -g cfgActiveDirectory -o cfgADSSOEnable 0
```

Utilisation de CMC avec un LDAP générique

Un administrateur CMC peut désormais intégrer les connexions utilisateur du serveur LDAP au MCC. Cette intégration nécessite une configuration à la fois sur le serveur LDAP et CMC. Sur le serveur LDAP, un objet Groupe standard est utilisé comme groupe de rôles. Un utilisateur qui a accès à CMC devient un membre du groupe de rôles. Les privilèges sont encore stockés sur CMC pour une autorisation similaire lors de l'installation du schéma standard avec support Active Directory.

Pour permettre à l'utilisateur LDAP d'accéder à une carte CMC spécifique, le nom du groupe de rôles et son nom de domaine doivent être configurés sur la carte CMC spécifique. Vous pouvez configurer un maximum de cinq groupes de rôles dans chaque contrôleur CMC. Le [Tableau 5-41](#) présente le niveau de privilège des groupes de rôles et le [Tableau 8-1](#) illustre les paramètres par défaut des groupes de rôles.

Figure 8-5. Configuration de CMC avec un LDAP générique



Configuration de l'annuaire LDAP générique pour accéder à CMC

La mise en œuvre du LDAP générique de CMC fait appel à deux phases pour donner l'accès à un utilisateur. La phase 1 commence par l'authentification des utilisateurs, suivie de la phase 2 pour l'autorisation de l'utilisateur.

Authentification et autorisation des utilisateurs LDAP

Certains serveurs d'annuaire exigent une liaison avant que les recherches puissent être effectuées sur un serveur LDAP spécifique. Voici les étapes de l'authentification :

1. Effectuez éventuellement la liaison au service d'annuaire. Par défaut, la liaison est anonyme.
2. Recherchez l'utilisateur en fonction de son nom d'utilisateur. 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 considéré comme authentifié. La phase suivante concerne l'autorisation. CMC stocke un maximum de 5 groupes et leurs privilèges correspondants. Un utilisateur a la possibilité d'être ajouté à plusieurs groupes au sein du service d'annuaire. Si l'utilisateur est membre de plusieurs groupes, il obtient les privilèges de tous ses groupes.

Voici les étapes de l'autorisation :

1. Recherchez dans chaque groupe configuré le DN de l'utilisateur dans les attributs **member** ou **uniqueMember**. Ce champ peut être configuré par l'administrateur.
2. Pour chaque groupe dont l'utilisateur est membre, ajoutez les privilèges.

Configuration du service d'annuaire LDAP générique à l'aide de l'interface Web de CMC

Vous pouvez utiliser le service LDAP (Lightweight Directory Access Protocol) générique pour configurer votre logiciel afin qu'il fournisse l'accès à CMC. Le service LDAP vous permet d'ajouter et de contrôler les privilèges utilisateur CMC de vos utilisateurs existants.

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

Pour plus d'informations sur la configuration LDAP et la configuration du LDAP générique, voir [Utilisation de CMC avec un LDAP générique](#).

Pour voir et configurer le LDAP, suivez ces étapes :

1. Connectez-vous à l'interface Web.
2. Cliquez sur l'onglet **Authentification utilisateur**, puis cliquez sur le sous-onglet **Services d'annuaire**. La page **Services d'annuaire** s'affiche.
3. Cliquez sur le bouton radio associé au LDAP générique.
4. Configurez les options affichées et cliquez sur **Appliquer**.

Les options de configuration disponibles sont les suivantes :

Tableau 8-10. Paramètres communs

Paramètre	Description
LDAP générique activé	Active le service LDAP générique sur CMC.
Utilisez le nom unique (DN) pour rechercher l'appartenance au groupe.	Spécifie le nom unique (DN) de groupes LDAP dont les membres sont autorisés à accéder au dispositif.
Activer la validation de certificat SSL	Si activé, CMC utilise le certificat d'une autorité de certification pour valider le certificat du serveur LDAP pendant l'établissement de liaisons SSL.
Liaison de DN	Le nom unique d'un utilisateur utilisé pour établir la liaison au serveur lors de la recherche du nom unique de l'utilisateur d'ouverture de session. S'il n'est pas fourni, une liaison anonyme est utilisée.
Le mot de passe	Mot de passe de liaison à utiliser conjointement avec le nom unique de liaison. Le mot de passe de liaison contient des données sensibles et doit être protégé de manière appropriée.
Nom unique de base à rechercher	Nom unique de la branche du répertoire à partir duquel toutes les recherches doivent débiter.
Attribut de l'identifiant de l'utilisateur	Spécifie l'attribut à rechercher. S'il n'est pas configuré, uid est utilisé par défaut. Il est recommandé qu'il soit unique dans le DN de base choisi, faute de quoi un filtre de recherche doit être configuré pour assurer l'unicité de l'utilisateur d'ouverture de session. Si le DN d'utilisateur ne peut pas être identifié par la recherche de la combinaison de l'attribut et du filtre de recherche, la connexion échoue avec une erreur.
Attribut de l'appartenance au groupe.	Spécifie l'attribut LDAP qui est utilisé pour vérifier l'appartenance au groupe. Il doit s'agir d'un attribut de la classe de groupe. S'il n'est pas spécifié, les attributs member et uniquemember sont utilisés.
Filtre de recherche	Indique un filtre de recherche LDAP valide. Ceci est utilisé si l'attribut d'utilisateur ne parvient pas à identifier de manière unique l'utilisateur d'ouverture de session dans le nom unique de base choisi. S'il n'est pas spécifié, la valeur est définie par défaut sur (objectClass=*), qui recherche tous les objets de l'arborescence. La longueur maximale de cette propriété est de 1 024 caractères.
Délai de réseau (secondes)	Définit le délai en secondes après lequel une session LDAP inactive est automatiquement fermée.
Délai de recherche (secondes)	Définit le délai en secondes après lequel une recherche est automatiquement fermée.

Sélection de vos serveurs LDAP

Vous pouvez configurer le serveur pour une utilisation avec le LDAP générique de deux façons. Les serveurs statiques permettent à l'administrateur de mettre un nom de domaine pleinement qualifié ou une adresse IP dans le champ. Par ailleurs, une liste de serveurs LDAP peut être récupérée en recherchant leur enregistrement SRV dans le DNS.

Les éléments suivants sont les propriétés de la section Serveurs LDAP :

- 1 Utiliser les serveurs LDAP statiques : lorsque vous sélectionnez cette option, le service LDAP utilise les serveurs spécifiés avec le numéro de port fourni (voir les détails ci-dessous).

 **REMARQUE** : vous devez sélectionner Statique ou DNS.

- 1 Adresse de serveur LDAP : précisez le nom de domaine pleinement qualifié ou l'adresse IP du serveur LDAP. Pour spécifier plusieurs serveurs LDAP redondants qui desservent le même domaine, fournissez la liste de tous les serveurs séparés par des virgules. CMC tente de se connecter à chaque serveur l'un après l'autre jusqu'à ce qu'une connexion soit établie.

- 1 Port de serveur LDAP : port de LDAP sur SSL, par défaut 636 s'il n'est pas configuré. Le port non SSL n'est pas pris en charge dans la version 3.0 de CMC puisque le mot de passe ne peut pas être transporté sans SSL.
- 1 Utiliser le DNS pour trouver des serveurs LDAP : lorsque vous sélectionnez cette option, LDAP utilise le domaine de la recherche et le nom du service via DNS. Vous devez sélectionner Statique ou 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.

Gestion des paramètres de groupe LDAP

Le tableau qui figure dans la section Paramètres du groupe répertorie les groupes de rôles et affiche les noms, domaines et privilèges associés pour les groupes de rôles qui sont déjà configurés.

- 1 Pour configurer un nouveau groupe de rôles, cliquez sur un nom de groupe de rôles qui n'a pas de nom, de domaine et de privilège dans la liste.
- 1 Pour modifier les paramètres d'un groupe de rôles existant, cliquez sur le nom de groupe de rôles.

Lorsque vous cliquez sur un nom de groupe de rôles, la page **Configurer le groupe de rôles** s'affiche. L'aide relative à cette page est disponible via le lien **Aide** en haut à droite de la page.

Gestion des certificats de sécurité LDAP

Cette section affiche les propriétés du certificat LDAP récemment téléversé sur CMC. Si vous avez téléchargé un certificat, utilisez ces informations pour vérifier que le certificat est valide et n'a pas expiré.

 **REMARQUE** : par défaut, CMC ne dispose pas d'un certificat de serveur délivré par une autorité de certification pour Active Directory. Vous devez téléverser un certificat de serveur valide, signé par une autorité de certification.

Les propriétés suivantes sont affichées pour le certificat :

- 1 Numéro de série : numéro de série du certificat.
- 1 Informations sur le sujet : sujet du certificat (nom de la personne ou de l'entreprise certifiée).
- 1 Renseignements sur l'émetteur : émetteur du certificat (nom de l'autorité de certification).
- 1 Valable à partir de : la date de début du certificat.
- 1 Valable jusqu'à : la date d'expiration du certificat.

Utilisez les commandes ci-dessous pour télécharger et envoyer ce certificat :

- 1 **Téléverser** : lance le processus de téléversement du certificat. Ce certificat, qui vous est délivré par votre serveur LDAP, permet d'accéder à CMC.
- 1 **Télécharger** : lance le processus de téléchargement. Vous êtes invité à choisir un emplacement pour enregistrer le fichier. Lorsque vous sélectionnez cette option et cliquez sur **Suivant**, la boîte de dialogue **Téléchargement de fichier** apparaît. Utilisez cette boîte de dialogue pour spécifier l'emplacement réservé au certificat de serveur sur votre station de gestion ou réseau partagé.

Configuration du service de répertoire LDAP générique avec la RACADM

 **REMARQUE** : cette fonction prend en charge IPv4 et IPv6.

Il existe beaucoup d'options pour configurer les connexions LDAP. Dans la plupart des cas, certaines options peuvent être utilisées avec leurs paramètres par défaut.

 **REMARQUE** : il est vivement recommandé d'utiliser la commande `'racadm testfeature -f LDAP'` pour tester les paramètres LDAP lors des configurations initiales. Cette fonction prend en charge IPv4 et IPv6.

Les modifications des propriétés requises comprennent l'activation des connexions LDAP, la configuration du nom de domaine pleinement qualifié ou de l'adresse IP du serveur, et la configuration du DN de base du serveur LDAP.

```
1 $ racadm config -g cfgLDAP -o cfgLDAPEnable 1
1 $ racadm config -g cfgLDAP -o cfgLDAPServer 192.168.0.1
1 $ racadm config -g cfgLDAP -o cfgLDAPBaseDN dc=company,dc=com
```

CMC peut être configuré pour interroger un serveur DNS à la recherche d'enregistrements SRV. Si la propriété `cfgLDAPSrvLookupEnable` est activée, la propriété `cfgLDAPServer` est ignorée. La requête suivante est utilisée pour rechercher 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`.

Utilisation

Pour vous connecter à CMC à l'aide d'un utilisateur LDAP, utilisez le nom d'utilisateur à l'invite de connexion et le mot de passe de l'utilisateur à l'invite de mot de passe. Si un utilisateur LDAP ne peut pas être identifié pour une raison quelconque, CMC tente d'utiliser une connexion locale avec les mêmes nom d'utilisateur et mot de passe. Ceci permet une connexion si la connectivité réseau est interrompue ou si le serveur LDAP n'est pas accessible.

Obtention d'aide

Le journal de suivi de CMC contient des informations expliquant pourquoi un utilisateur ne parvient pas à se connecter. Pour trier les pannes de connexions LDAP, il est recommandé d'utiliser la commande `racadm testfeature -f LDAP` avec le débogage activé.

[Retour à la page Contenu](#)

[Retour à la page Contenu](#)

Diagnostics

Micrologiciel Dell Chassis Management Controller Version 3.1 Guide d'utilisation

- [Utilisation de l'interface de l'écran LCD](#)
- [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 sur la condition du serveur et du module de l'écran LCD](#)

L'écran LCD vous permet de diagnostiquer des problèmes concernant un serveur ou un module dans le châssis. En cas de problème ou de défaillance avec le châssis ou un serveur ou un autre module dans le châssis, l'indicateur d'état de l'écran LCD clignote en orange. Dans le menu principal, une icône avec un arrière-plan orange s'affiche en regard de l'élément de menu (Serveur ou Enceinte) qui permet d'accéder au serveur ou au module défectueux.

En suivant les icônes orange jusque dans le système de menus de l'écran LCD, vous pouvez afficher l'écran Condition et les messages d'erreur concernant l'élément présentant le problème.

Les messages d'erreur de l'écran LCD peuvent être supprimés en supprimant le module ou le serveur au centre du problème. Dans le cas d'erreurs de serveur, utilisez l'interface Web iDRAC ou l'interface de ligne de commande pour effacer le journal SEL (System Event Log - Journal des événements système) afin de supprimer les erreurs de serveur de l'écran LCD.

Utilisation de l'interface de l'écran LCD

Utilisez l'écran LCD pour procéder à la configuration et aux diagnostics et pour obtenir des informations sur la condition du châssis et son contenu.

Navigation sur l'écran LCD

Utilisez les boutons à droite de l'écran LCD pour vous servir de l'écran LCD. Les boutons flèches haut, bas, gauche et droite permettent de changer les éléments de menu ou les icônes sélectionnés à l'écran. L'élément sélectionné est indiqué avec un arrière-plan ou un bord bleu clair.

Le bouton central active l'élément sélectionné.

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 13-1](#) permettent de naviguer entre les écrans LCD :

Tableau 13-1. Icônes de navigation de l'écran LCD

Icône normale	Icône en surbrillance	Nom et description de l'icône
		Précédent. Mettez en surbrillance le bouton central et appuyez dessus pour retourner à l'écran précédent.
		Accepter/Oui. Mettez en surbrillance le bouton central et appuyez dessus pour accepter une modification et retourner à l'écran précédent.
		Ignorer/Suivant. Mettez le bouton central en surbrillance et appuyez dessus pour ignorer les modifications apportées et accéder à l'écran suivant.
		Non. Mettez en surbrillance le bouton central et appuyez dessus pour répondre « Non » à une question.
 OU		Pivoter. Mettez le bouton central en surbrillance et appuyez dessus pour alterner entre les affichages graphiques avant et arrière du châssis. REMARQUE : l'arrière-plan orange indique que la vue opposée comporte des erreurs.

		
		<p>Identification de composant. Fait clignoter la LED bleue sur un composant.</p> <p>REMARQUE : un rectangle bleu clignotant entoure cette icône lorsque l'Identification de composant est activée.</p>

Menu principal

Vous pouvez naviguer vers l'un des écrans suivants depuis le menu **principal** :

- 1 **Menu Configuration de l'écran LCD** : sélectionne la langue à utiliser et l'écran LCD qui s'affiche lorsque personne n'utilise l'écran LCD.
- 1 **Serveur** : affiche des informations sur la condition des serveurs.
- 1 **Enceinte** : affiche des informations sur la condition du châssis.

1. Utilisez les boutons flèche haut et bas pour mettre un élément en surbrillance.
2. Appuyez sur le bouton central pour activer votre sélection.

Écran LCD Setup Menu (Menu Configuration du module LCD)

Le menu **Configuration de l'écran LCD** affiche un menu d'éléments pouvant être configurés :

- 1 **Configuration de la langue** : choisissez la langue que vous souhaitez utiliser pour le texte et les messages de l'écran LCD.
- 1 **Écran par défaut** : choisissez l'écran qui s'affiche en l'absence d'activité sur l'écran LCD.

1. Utilisez les boutons flèche haut et bas pour mettre un élément en surbrillance dans le menu ou mettez en surbrillance l'icône **Précédent** si vous souhaitez retourner au menu **principal**.
2. Appuyez sur le bouton central pour activer votre sélection.

Écran de configuration de la langue

L'écran **Configuration de la langue** vous permet de sélectionner la langue utilisée pour les messages de l'écran LCD. La langue active est mise en surbrillance avec un arrière-plan 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** apparaît en surbrillance.
3. Appuyez sur le bouton central pour confirmer la modification. Le menu **Configuration de l'écran LCD** est affiché.

Écran par défaut

L'**écran par défaut** vous permet de changer l'écran affiché par l'écran LCD en l'absence d'activité sur le panneau. L'écran par défaut est le **menu principal**. Vous pouvez choisir parmi les écrans suivants à afficher :

- 1 **Menu Main** (Principal)
- 1 **Condition du serveur** (affichage graphique avant du châssis)
- 1 **Condition du module** (affichage graphique arrière du châssis)
- 1 **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 **Condition du serveur graphique** affiche des icônes pour chaque serveur installé dans le châssis et indique la condition d'intégrité générale de chaque serveur. L'intégrité du serveur est indiquée par la couleur de l'icône du serveur :

- 1 Gris : le serveur est hors tension sans erreurs
- 1 Vert : le serveur est sous tension sans erreurs
- 1 Jaune : le serveur a une ou plusieurs erreurs non critiques
- 1 Rouge : le serveur a une ou plusieurs erreurs critiques
- 1 Noir : le serveur n'est pas présent

Un rectangle bleu clair clignotant autour d'une icône de serveur indique que le serveur est mis en surbrillance.

Pour afficher l'écran **Condition du module graphique** :

1. Mettez en surbrillance l'icône **Rotation**.
2. Appuyez sur le bouton central.

Pour afficher l'écran de condition d'un serveur :

1. Utilisez les boutons flèche pour mettre en surbrillance le serveur souhaité.
2. Appuyez sur le bouton central. L'écran **Condition du serveur** s'affiche.

Pour retourner au menu principal :

1. Utilisez les boutons flèche pour mettre en surbrillance l'icône **Précédent**.
2. Appuyez sur le bouton central.

Écran Condition du module graphique

L'écran **Condition du module graphique** 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 indiquée par la couleur de chaque icône de module, comme suit :

- 1 Gris : le module est hors tension ou sous tension en veille sans erreurs
- 1 Vert : le module est sous tension sans erreurs
- 1 Jaune : le module a une ou plusieurs erreurs non critiques
- 1 Rouge : le serveur a une ou plusieurs erreurs critiques
- 1 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 **Condition du serveur graphique** :

1. Mettez en surbrillance l'icône **Rotation**.
2. Appuyez sur le bouton central.

Pour afficher l'écran de condition d'un module :

1. Utilisez les boutons flèche haut, bas, gauche et droite pour mettre le module souhaité en surbrillance.
2. Appuyez sur le bouton central. L'écran **Condition du module** s'affiche.

Pour retourner au **menu principal** :

1. Utilisez les boutons fléchés pour mettre en surbrillance l'icône **Précédent**.
2. Appuyez sur le bouton central. Le **menu principal** s'affiche.

Écran du menu Enceinte

Cet écran vous permet de naviguer vers les écrans suivants :

- 1 Écran Condition du module
- 1 Écran Condition de l'enceinte
- 1 Écran **Résumé IP**
- 1 **Menu Main (Principal)**

1. Utilisez les boutons de navigation pour mettre en surbrillance l'élément souhaité. (Mettez en surbrillance l'icône **Précédent** pour retourner au **menu principal**.)
2. Appuyez sur le bouton central. L'écran sélectionné apparaît.

Écran Condition du module

L'écran **Condition du module** affiche des informations et des messages d'erreur sur un module. Voir [Informations sur la condition du serveur et du module de l'écran LCD](#) et [Messages d'erreur de l'écran LCD](#) pour les messages qui peuvent s'afficher sur cet écran.

Utilisez les touches fléchées haut et bas pour faire défiler 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 du module graphique**.

Écran Condition de l'enceinte

L'écran **Condition de l'enceinte** affiche des messages d'information et d'erreur concernant l'enceinte. Voir [Messages d'erreur de l'écran LCD](#) pour les messages qui peuvent s'afficher sur cet écran.

Utilisez les touches fléchées haut et bas pour faire défiler 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 boutons flèche haut et bas pour faire défiler la liste. Utilisez les boutons flèche 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 permet de diagnostiquer des problèmes concernant un serveur ou un module dans le châssis. En cas de problème ou de défaillance avec le châssis ou un serveur ou un autre module dans le châssis, l'indicateur d'état de l'écran LCD clignote en orange. Dans le **menu principal**, une icône clignotante avec un arrière-plan orange s'affiche en regard de l'élément de menu (Serveur ou Enceinte) qui permet d'accéder au serveur ou au module défectueux.

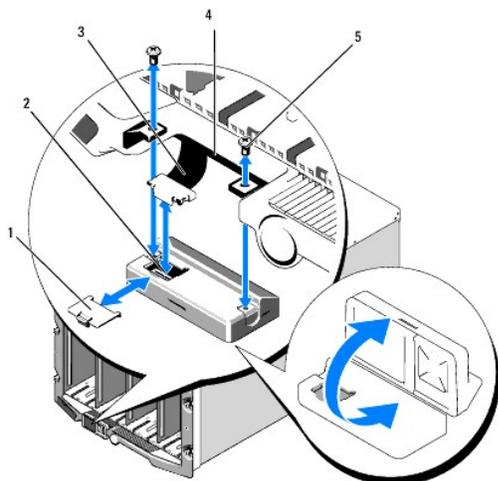
En suivant les icônes orange clignotantes jusque dans le système de menus de l'écran LCD, vous pouvez afficher l'écran **Condition** et les messages d'erreur concernant l'élément présentant le problème.

Les messages d'erreur apparaissant sur l'écran LCD peuvent être supprimés en supprimant le module ou le serveur à l'origine du problème ou en effaçant le journal du matériel du module ou du serveur. En ce qui concerne les erreurs liées au serveur, utilisez l'interface Web ou l'interface de ligne de commande d'iDRAC pour effacer le journal des événements système (journal SEL) du serveur. Quant aux erreurs concernant le châssis, utilisez l'interface Web ou l'interface de ligne de commande de CMC pour effacer le journal du matériel.

Dépannage du matériel LCD

Si vous rencontrez des problèmes avec l'écran LCD lors de votre utilisation de CMC, vérifiez 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 13-1. Retrait et installation du module LCD



1	cache de protection des câbles	2	module LCD
3	câble ruban	4	charnières (2)
5	vis (2)		

Tableau 13-2. Éléments de dépannage matériel LCD

Symptôme	Problème	Action de récupération
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 du LCD.	Vérifiez que le CMC démarre, puis réinitialisez-le à l'aide de l'interface graphique ou des commandes de l'utilitaire RACADM.
Message d'alerte de l'écran CMC ne répond pas et la LED reste orange fixe ou est 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 de l'interface graphique ou des commandes de l'utilitaire RACADM. Cherchez un message indiquant : Communication avec le contrôleur LCD impossible. 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 encore, le module LCD est défectueux.	Consultez le journal du matériel à l'aide de l'interface graphique ou des commandes de l'utilitaire RACADM. Recherchez des messages du type : <ul style="list-style-type: none"> 1 Le câble du module LCD n'est pas branché ou n'est pas branché correctement. 1 Le câble du panneau de configuration n'est pas branché, ou n'est pas branché correctement. Réinstallez les câbles.
Message de l'écran LCD CMC introuvable	Aucun CMC n'est présent dans le châssis	Insérer 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* s'affichant sur l'écran LCD présentent un format similaire à celui du journal des événements système (journal SEL) affiché sur l'interface de ligne de commande ou l'interface Web. Ce format est le suivant :

```
<Gravité> <Nom du capteur> : capteur <Type de capteur> pour <Entité>, <Description de l'événement>
```

Les tableaux présentés dans la section concernant les erreurs répertorient les messages d'erreur et d'avertissement qui apparaissent sur les divers écrans de l'écran LCD et la cause possible du message. Le texte figurant entre crochets fléchés (< >) indique que le texte peut varier.

Les *Informations sur la condition* qui apparaissent sur l'écran LCD incluent des informations descriptives sur les modules dans le châssis. Les tableaux qui figurent dans cette section décrivent les informations affichées pour chaque composant.

Messages d'erreur de l'écran LCD

Tableau 13-3. Écrans Condition de CMC

Sévérité	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	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	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.
Avertissement	Détection d'un 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 13-4. Écran Condition de l'enceinte/du châssis

Sévérité	Message	Cause
Critique	Le ventilateur <numéro> est retiré.	Ce ventilateur est nécessaire pour refroidir correctement l'enceinte/le châssis.
Avertissement	La redondance du bloc d'alimentation est dégradée.	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	La redondance du bloc d'alimentation est perdue.	Une ou plusieurs unités d'alimentation sont défaillantes ou ont été retirées, et le système n'est plus redondant.
Critique	Les blocs d'alimentation ne sont pas redondants. Les ressources sont insuffisantes pour maintenir un fonctionnement normal.	Une ou plusieurs unités d'alimentation sont défaillantes ou ont été retirées, et le système n'est pas suffisamment alimenté pour maintenir ses opérations normales. Les serveurs pourraient se mettre hors tension.
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.	CMC plus redondant. Cela se produit si le CMC en attente est retiré.
Critique	La journalisation de toutes les erreurs est désactivée.	Le châssis/enceinte ne peut pas journaliser tous les événements. Ceci indique généralement que le panneau de configuration ou le câble de ce dernier a rencontré un problème.
Avertissement	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	Le journal est presque plein..	Le journal des événements du châssis est plein à 75 %.

Tableau 13-5. Écrans Condition du ventilateur

Sévérité	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	Les rotations par minute du ventilateur <numéro> sont en dessus du seuil critique minimal.	La vitesse du ventilateur spécifié est trop haute. Ceci est généralement le résultat d'un pale de ventilateur cassée.

Tableau 13-6. Écrans Condition du module d'E/S

Sévérité	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'un échec dans le module d'E/S <numéro>.	Le module d'E/S est défaillant. La même erreur peut également se produire si le module d'E/S est déclenché thermiquement.

Tableau 13-7. Écran Condition de l'IKVM

Sévérité	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 KVM local n'est pas opérationnel et est mis hors tension.	Échec RIP série ou échec de la puce de l'hôte USB.

Tableau 13-8. Écrans Condition de l'unité d'alimentation

Sévérité	Message	Cause
Critique	Échec du bloc d'alimentation <numéro>.	L'unité d'alimentation est défaillante.
Critique	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	Le bloc d'alimentation <numéro> fonctionne à 110 volts et pourrait entraîner un court-circuit.	Le bloc d'alimentation est branché sur un source de 110 volt.

Tableau 13-9. Écran Condition du serveur

Sévérité	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 se refroidit.
Avertissement	La température ambiante de la carte système est supérieure au seuil d'avertissement maximal.	La température du serveur se réchauffe.
Critique	La température ambiante de la carte système est supérieure au seuil critique maximal.	La température du serveur est trop chaude.
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	Le niveau de charge de 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 dépasse la plage autorisée.	
Critique	La tension <nom du capteur de tension> de la carte mezzanine <numéro> dépasse la plage autorisée.	
Critique	La tension <nom du capteur de tension> du stockage dépasse la plage autorisée.	
Critique	Erreur interne de l'UC <numéro> (IERR).	Panne de l'UC.
Critique	Événement de déclenchement thermique de l'UC <numéro> (surchauffe).	UC surchauffée.
Critique	Configuration de l'UC <numéro> non pris en charge..	Type de processeur incorrect ou dans un emplacement erroné.
Critique	L'UC <numéro> est absente.	L'UC requise est manquante ou est absente.
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	Condition de la carte Mezz C<numéro de logement> : capteur de carte d'extension de la carte Mezz C<numéro de logement>, l'erreur d'installation a été confirmée	Carte mezzanine incorrecte installée pour la structure d'E/S
Critique	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	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	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	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 mise hors tension.
Critique	Le registre d'horloge de la surveillance a exécuté un cycle d'alimentation sur 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 cycle d'alimentation.
Critique	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 corrigible sur un périphérique mémoire de l'emplacement <emplacement>.	
Avertissement	Le taux d'erreur de la mémoire permanente corrigible a augmenté pour un périphérique mémoire de l'emplacement <emplacement>.	Les erreurs corrigibles de l'ECC atteignent un taux critique.
Critique	Détection d'erreurs multi-bits sur un périphérique mémoire de l'emplacement <emplacement>.	Une erreur ECC non corrigible a été détectée.
Critique	Détection d'une interruption non masquable (NMI) lors d'une vérification d'un canal d'E/S sur un composant du périphérique <numéro> de fonction <numéro> du bus <numéro>.	Une interruption critique est générée dans le canal d'E/S.
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	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 périphérique <numéro> de fonction <numéro> du bus <numéro>.	Erreur PCI détectée par un périphérique.
Critique	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 corrigible 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	La journalisation de toutes les erreurs est désactivée.	
Irrécupérable	Détection d'une erreur de protocole de l'UC.	Le protocole du processeur est passé à l'état irrécupérable.
Irrécupérable	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 de l'UC.	Le Machine Check du processeur est passé à l'état irrécupérable.
Critique	Perte de la redondance de la mémoire.	
Critique	Détection d'une erreur fatale du bus sur un composant du périphérique <numéro> de fonction <numéro> du bus <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 périphérique <numéro> de fonction <numéro> du bus <numéro>.	Une erreur de puce a été détectée.
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	Échec de la prise en charge du réglage de liaison ou de l'adresse flex 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	Échec d'obtention de données de réglage de liaison ou de l'adresse flex depuis iDRAC.	

 **REMARQUE** : pour des informations supplémentaires sur des messages LCD du serveur, voir le « Guide d'utilisation du serveur ».

Informations sur la condition du serveur et du module de l'écran LCD

Les tableaux qui figurent 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 13-10. Condition 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	Ne s'affiche que sur un CMC actif. Affiche De secours 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 la condition activée de l'IPv6 actuel uniquement sur un CMC actif.
Adresse locale IP6 : <adresse>	Ne s'affiche que si l'IPv6 est activée sur un CMC actif uniquement.
Adresse globale IP6 : <adresse>	Ne s'affiche que si l'IPv6 est activée sur un CMC actif uniquement.

Tableau 13-11. Condition du châssis/de l'enceinte

Élément	Description
Nom défini par l'utilisateur	Exemple : « Système de rack Dell ». Définissable via l'interface de ligne de commande ou l'interface utilisateur Web de CMC
Messages d'erreur	Si aucune erreur ne s'est produite, le message Aucune erreur s'affiche ; sinon, des messages d'erreur sont répertoriés, puis des avertissements.
Numéro de modèle	Exemple « PowerEdgeM1000 »
Consommation électrique	Consommation électrique en watts
Puissance maximale	Consommation électrique maximale en watts
Consommation électrique 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 13-12. 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 13-13. Condition de l'unité d'alimentation

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 13-14. Condition du module d'E/S

Élément	Description
Nom/Emplacement	Exemple : Module d'E/S A1, Module d'E/S B1. 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	Éteint ou allumé
Modèle	Modèle du module d'E/S
Type de structure	Type de mise en réseau
adresse IP	Apparaît uniquement si le module d'E/S est allumé. Cette valeur est zéro dans le cas d'un module d'E/S de type transfert des données.
Numéro de service	Le numéro de service attribué par l'usine.

Tableau 13-15. Condition iKVM

Élément	Description
Nom	iKVM

Aucune erreur	Si aucune erreur ne s'est produite, le message Aucune erreur s'affiche ; sinon, des messages d'erreur sont répertoriés. Les erreurs critiques sont répertoriées en premier, puis les avertissements. Pour plus d'informations, voir Messages d'erreur de l'écran LCD .
Condition	Éteint ou allumé
Modèle/Fabriquant	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 logiciel du module iKVM.
Ces informations sont mises à jour de manière dynamique.	

Tableau 13-16. 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, des messages d'erreur sont répertoriés. Les erreurs critiques sont répertoriées en premier, puis les avertissements. Pour plus d'informations, voir Messages d'erreur de l'écran LCD .
Nom de logement	Nom du logement du châssis. Par exemple, SLOT-01. REMARQUE : ce tableau est configurable via l'interface de ligne de commande ou l'interface utilisateur Web du CMC.
Nom	Nom du serveur, définissable par l'utilisateur via Dell OpenManage. Le nom s'affiche uniquement une fois que l'iDRAC a fini de démarrer et si le serveur prend cette fonctionnalité en charge. Sinon, des messages indiquant de l'iDRAC est en cours de démarrage 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 du BIOS)	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 : la version iDRAC 1.01 s'affiche en tant que 1.1. Il n'existe aucune version iDRAC 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 la condition activée de l'IPv6.
Adresse locale IP6 : <adresse>	S'affiche uniquement si l'iDRAC prend en charge IPv6 et si IPv6 est activée.
Adresse globale IP6 : <adresse>	S'affiche uniquement si l'iDRAC prend en charge IPv6 et si IPv6 est activée.
FlexAddress activée sur les structures	S'affiche uniquement si la fonctionnalité est installée. Répertorie les structures activées sur ce serveur (c'est-à-dire, A, B, C).

Les informations du [Tableau 13-16](#) sont mises à jour de manière dynamique. Si le serveur ne prend pas en charge cette fonctionnalité, les informations suivantes ne s'affichent pas. Sinon, les options de Server Administrator sont les suivantes :

- 1 Option « Aucune » = Aucune chaîne ne doit être affichée sur l'écran LCD.
- 1 Option « Par défaut » = Aucun effet.
- 1 Option « Personnalisé » = Vous permet d'entrer un nom de chaîne pour le serveur.

Les informations ne s'affichent que si l'iDRAC a fini de démarrer. Pour des informations supplémentaires sur cette fonctionnalité, voir le « *Guide de référence de ligne de commande pour iDRAC6 et CMC* »

[Retour à la page Contenu](#)

[Retour à la page Contenu](#)

Configuration de CMC pour utiliser des consoles de ligne de commande

Micrologiciel Dell Chassis Management Controller Version 3.1 Guide d'utilisation

- [Fonctionnalités de la console de ligne de commande de CMC](#)
- [Utilisation d'une console série, Telnet ou SSH](#)
- [Utilisation d'une console Telnet avec CMC](#)
- [Utilisation de SSH avec CMC](#)
- [Configuration du logiciel d'émulation de terminal](#)
- [Connexion aux serveurs ou aux modules d'E/S à l'aide de la commande Connect](#)

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 de manière à pouvoir effectuer des actions de gestion de systèmes via la console. Pour plus d'informations sur l'utilisation des commandes RACADM dans CMC via la console de ligne de commande, voir [Utilisation de l'interface de ligne de commande RACADM](#).

Fonctionnalités de la console de ligne de commande de CMC

CMC prend en charge les fonctions de console série, Telnet et SSH suivantes :

- 1 Une connexion de client série et un maximum de quatre connexions de clients Telnet simultanées.
- 1 Un maximum de quatre connexions de clients Secure Shell (SSH) simultanées.
- 1 Prise en charge des commandes RACADM.
- 1 Commande **connect** intégrée de connexion à la console série des serveurs et des modules d'E/S ; également disponible sous la forme **racadm connect**.
- 1 Modification et historique de la ligne de commande.
- 1 Contrôle du délai d'expiration de la session sur toutes les interfaces de console.

Utilisation d'une console série, Telnet ou SSH

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

Tableau 3-1. Commandes de la ligne de commande CMC

Commande	Description
racadm	Les commandes RACADM commencent par le mot-clé racadm et sont suivies d'une sous-commande, comme getconfig , serveraction ou getsensorinfo . Voir Utilisation de l'interface de ligne de commande RACADM pour en savoir plus sur l'utilisation de RACADM.
connect	Se connecte à la console série d'un serveur ou d'un module d'E/S. Voir Connexion aux serveurs ou aux modules d'E/S à l'aide de la commande Connect pour obtenir de l'aide sur l'utilisation de la commande connect . REMARQUE : la commande racadm connect peut également être utilisée.
exit, logout et quit	Ces commandes exécutent toutes la même action : elles mettent fin à la session en cours et retournent à une invite d'ouverture de session.

Utilisation d'une console Telnet avec CMC

Un maximum de quatre systèmes client Telnet et quatre clients SSH peuvent se connecter à la fois.

Si votre station de gestion exécute Windows XP ou Windows 2003, un problème peut surgir au niveau des caractères lors d'une session Telnet sur CMC. Ce problème peut prendre la forme d'une ouverture de session figée, la touche Retour ne répondant pas et l'invite de mot de passe n'apparaissant pas.

Pour résoudre ce problème, téléchargez le correctif 824810 sur le site Web du support de Microsoft à l'adresse support.microsoft.com. Consultez l'article 824810 de la Base de connaissances de Microsoft pour plus d'informations.

Utilisation de SSH avec CMC

SSH est une session de ligne de commande qui intègre les mêmes fonctions qu'une session Telnet, mais avec la négociation et le cryptage de session afin d'améliorer la sécurité. CMC prend en charge la version 2 de SSH avec authentification par mot de passe. SSH est activé sur le contrôleur CMC par défaut.

 **REMARQUE** : CMC ne prend pas en charge la version 1 de SSH.

Lorsqu'une erreur se produit lors de la procédure d'ouverture de session, le client SSH publie un message d'erreur. Le texte du message dépend du client et n'est pas contrôlé par le contrôleur CMC. Consultez les messages RACLog pour déterminer la cause de la panne.

 **REMARQUE** : `OpenSSH` doit être exécuté à partir d'un émulateur de terminal VT100 ou ANSI sous Windows. Vous pouvez aussi exécuter `OpenSSH` à l'aide de `PuTTY.exe`. L'exécution d'`OpenSSH` à partir d'une invite de commande Windows n'offre pas une fonctionnalité complète (quelques touches ne répondent pas et aucun graphique n'est affiché). Pour Linux, exécutez les services de clients SSH pour vous connecter à CMC avec n'importe quel environnement.

Quatre sessions SSH simultanées sont prises en charge à la fois. Le délai d'expiration de la session est contrôlé par la propriété `cfgSsnMgt.SshIdleTimeout` (reportez-vous au chapitre Propriétés de la base de données du *Guide de référence de la ligne de commande pour iDRAC6 et CMC*) ou depuis la page **Gestion des services** dans l'interface Web (voir [Configuration des services](#)).

CMC prend également en charge l'authentification par clé publique (PKA) sur SSH. Cette méthode d'authentification améliore l'automatisation des scripts SSH en évitant d'intégrer ou de demander l'ID utilisateur/le mot de passe. Pour plus d'informations, voir [Utilisation de RACADM pour configurer l'authentification par clé publique sur SSH](#).

Activation de SSH sur CMC

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

Pour des instructions sur l'activation des connexions SSH sur CMC à l'aide de RACADM, consultez la section relative à la commande `config` et la section Propriétés de la base de données `cfgSerial` du *Guide de référence la ligne de commande pour iDRAC6 et CMC*. Pour des instructions sur l'activation des connexions SSH sur CMC à l'aide de l'interface Web, voir [Configuration des services](#).

Modification du port SSH

Pour modifier le port SSH, utilisez la commande suivante :

```
racadm config -g cfgRacTuning -o cfgRacTuneSshPort <numéro de port>
```

Pour des informations supplémentaires sur les propriétés `cfgSerialSshEnable` et `cfgRacTuneSshPort`, voir le chapitre Propriétés de la base de données du *Guide de référence de la ligne de commande pour iDRAC6 et CMC*.

La mise en œuvre SSH CMC prend en charge plusieurs schémas de cryptographie, tel qu'illustré dans le [Tableau 3-2](#).

Tableau 3-2. Schémas de cryptographie

Type de schéma	Schéma
Cryptographie asymétrique	Spécification de bits (aléatoire) Diffie-Hellman DSA/DSS 512-1024 par NIST
Cryptographie symétrique	<ul style="list-style-type: none">1 AES256-CBC1 RIJNDael256-CBC1 AES192-CBC1 RIJNDael192-CBC1 AES128-CBC1 RIJNDael128-CBC1 BLOWFISH-128-CBC1 3DES-192-CBC1 ARCFOUR-128
Intégrité du message	<ul style="list-style-type: none">1 HMAC-SHA1-1601 HMAC-SHA1-961 HMAC-MD5-1281 HMAC-MD5-96
Authentification	Le mot de passe

Activation de la connexion du panneau avant à iKVM

Pour des informations et des instructions sur l'utilisation des ports du panneau avant de l'iKVM, voir [Activation ou désactivation du panneau avant](#).

Configuration du logiciel d'émulation de terminal

CMC prend en charge une console texte série d'une station de gestion exécutant l'un des types de logiciel d'émulation de terminal suivants :

- 1 Linux Minicom
- 1 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. Les étapes suivantes s'appliquent pour configurer Minicom version 2.0. Les autres versions de Minicom peuvent être légèrement différentes, mais elles requièrent les mêmes paramètres de base. Suivez les informations de [Paramètres de Minicom requis](#) pour configurer les autres versions de Minicom.

Configuration de Minicom version 2.0

 **REMARQUE** : pour optimiser les résultats, définissez la propriété `cfgSerialConsoleColumns` pour qu'elle corresponde au nombre de colonnes. Rappel : l'invite utilise deux caractères. Par exemple, pour une fenêtre de terminal de 80 colonnes, tapez :

```
racadm config -g cfgSerial -o cfgSerialConsoleColumns 80.
```

1. Si vous n'avez pas de fichier de configuration Minicom, passez à l'étape suivante.

Si vous avez un fichier de configuration Minicom, tapez `minicom <nom du fichier de configuration Minicom>` et passez à l'[étape 13](#).

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>, définissez **Contrôle du débit du matériel** sur `Oui` et définissez **Contrôle du débit du logiciel** sur `Non`.

Pour quitter le menu **Configuration du port série**, appuyez sur <Entrée>.

7. Sélectionnez **Modem et numérotation** et appuyez sur <Entrée>.

8. Dans le menu **Configuration du modem et numérotation**, appuyez sur <Retour> pour effacer les paramètres `init`, `reset`, `connect` et `hangup` de sorte qu'ils soient vides, puis appuyez sur <Entrée> pour enregistrer chaque valeur vide.

9. Lorsque tous les champs indiqués sont effacés, appuyez sur <Entrée> pour quitter le menu **Configuration de la numérotation du modem et des paramètres**.

10. Sélectionnez **Enregistrer la configuration sous config_name** et appuyez sur <Entrée>.

11. Sélectionnez **Quitter Minicom** et appuyez sur <Entrée>.

12. À l'invite shell de commande, tapez `minicom <nom du fichier de configuration Minicom>`.

13. Appuyez sur <Ctrl+a>, <x>, <Entrée> pour quitter Minicom.

Assurez-vous que la fenêtre Minicom affiche une invite de connexion. Lorsque l'invite de connexion apparaît, votre connexion est établie. Vous êtes maintenant prêt à vous connecter et à accéder à l'interface de ligne de commande CMC.

Paramètres de Minicom requis

Utilisez [Tableau 3-3](#) pour configurer une version quelconque de Minicom.

Tableau 3-3. Paramètres de Minicom

Description du paramètre	Paramètre requis
B/s/Par/Bits	115200 8N1
Contrôle du débit matériel	Oui
Contrôle du débit logiciel	Non
Émulation de terminal	ANSI
Paramètres de la numérotation du modem et des paramètres	Effacez les paramètres <code>init</code> , <code>reset</code> , <code>connect</code> et <code>hangup</code> pour qu'ils soient vides

Connexion aux serveurs ou aux modules d'E/S à l'aide de la commande Connect

CMC peut établir une connexion pour rediriger la console série du serveur ou des modules d'E/S. Pour les serveurs, la redirection de la console série peut être effectuée de plusieurs façons :

- 1 À l'aide de la ligne de commande CMC et de la commande `connect` ou `racadm connect`. Pour des informations sur le paramètre `connect`, voir la commande `racadm connect` du *Guide de référence de la ligne de commande pour iDRAC6 et CMC*.
- 1 À l'aide de la fonctionnalité de redirection de la console série de l'interface Web iDRAC.
- 1 À l'aide de la fonctionnalité Serial Over LAN (SOL) iDRAC.

En revanche, pour les consoles série/Telnet/SSH, CMC prend en charge la commande `connect` pour établir une connexion série vers le serveur ou les modules d'E/S. La console série du serveur contient à la fois les écrans d'amorçage et de configuration du BIOS, ainsi que la console série du système d'exploitation. Pour les modules d'E/S, la console série du commutateur est disponible.

PRÉCAUTION : lorsqu'elle est exécutée depuis la console série de CMC, l'option `connect -b` reste connectée jusqu'à la réinitialisation de CMC. Cette connexion constitue un risque potentiel de sécurité.

REMARQUE : la commande `connect` fournit l'option `-b` (binaire). L'option `-b` transmet des données binaires brutes et `cfgSerialConsoleQuitKey` n'est pas utilisé. De plus, lors de la connexion à un serveur avec la console série CMC, les transitions dans le signal DTR (par exemple, si le câble série est retiré pour connecter un débogueur) n'entraînent pas une fermeture de session.

REMARQUE : si un module d'E/S ne prend pas en charge la redirection de console, la commande `connect` affiche une console vide. Dans ce cas, pour retourner à la console CMC, tapez la séquence Échap. La séquence Échap de la console par défaut 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 une étiquette de module d'E/S a1, a2, b1, b2, c1 et c2.

Les modules d'E/S sont étiquetés A1, A2, B1, B2, C1 et C2. (Voir la [Figure 11-1](#) pour une illustration du placement des modules d'E/S dans le châssis.) Lorsque vous référez les modules d'E/S dans la commande `connect`, ils sont adressés à des commutateurs, comme présenté dans le [Tableau 3-4](#).

Tableau 3-4. Adressage des modules d'E/S aux commutateurs

Nom des modules d'E/S	Commutateur
A1	switch-a1
A2	switch-a2
B1	switch-b1
B2	switch-b2
C1	switch-c1
C2	switch-c2

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 vous connecter à une console série du serveur géré, utilisez la commande `connect server-n`, où *-n* est le numéro d'emplacement du serveur ; vous pouvez également utiliser la commande `racadm connect server-n`. Lorsque vous vous connectez à un serveur à l'aide de l'option `-b`, une communication binaire est très probablement établie et le caractère d'échappement est désactivé. Si iDRAC n'est pas disponible, le message d'erreur `Pas de route vers l'hôte` apparaît.

La commande `connect server-n` permet à l'utilisateur d'accéder au port série du serveur. Une fois cette connexion établie, l'utilisateur est en mesure de voir la redirection de console du serveur via le port série de CMC qui inclut à la fois la console série du BIOS et la console série du système d'exploitation.

REMARQUE : pour afficher les écrans d'amorçage du BIOS, la redirection série doit être activée dans la configuration BIOS des serveurs. Vous devez également définir la fenêtre d'émulateur de terminal sur 80x25. Sinon, l'écran est flou.

REMARQUE : toutes les touches ne fonctionnent pas dans les écrans de configuration du BIOS ; par conséquent, vous devez spécifier des séquences d'échappement appropriées pour `CTRL+ALT+SUPPR`, ainsi que d'autres séquences d'échappement. L'écran de redirection initial affiche les séquences d'échappement nécessaires.

Configuration du BIOS du serveur géré pour la redirection de console série

Il est nécessaire de se connecter au serveur géré à l'aide d'iKVM (voir [Gestion de serveurs avec iKVM](#)) ou d'établir une session VKVM depuis l'interface utilisateur Web iDRAC (voir le *Guide d'utilisation d'iDRAC* à l'adresse support.dell.com/manuals), et d'effectuer les étapes suivantes :

Par défaut, la communication série dans le BIOS est désactivée. Pour rediriger les données de la console texte hôte vers les communications série sur le réseau local, vous devez activer la redirection de console via COM1. Pour modifier le paramètre du BIOS :

1. Démarrez le serveur géré.
2. Appuyez sur `<F2>` pour accéder à l'utilitaire de configuration du BIOS pendant le POST.

3. Effectuez un défilement vers le bas jusqu'à **Communication série** et appuyez sur <Entrée>. Dans la boîte de dialogue contextuelle, la liste des communications série affiche les options suivantes :

- 1 off
- 1 activé sans redirection de console
- 1 activé avec redirection de console via COM1

Utilisez les touches fléchées pour naviguer entre ces options.

4. Assurez-vous que l'option '**Activé avec redirection de console via COM1**' est activée.
5. Activez la **Redirection après démarrage** (la valeur par défaut est **Désactivée**). Cette option active la redirection de console du BIOS à chaque redémarrage.
6. Enregistrez les modifications et quittez.
7. Le serveur géré redémarre.

Configuration de Windows pour la redirection de console série

Aucune configuration n'est nécessaire pour les serveurs exécutant les versions de Microsoft Windows Server à partir de Windows Server 2003. Windows reçoit des informations du BIOS et active la console d'administration spéciale (SAC) un COM1.

Configuration de Linux pour la redirection de console série du serveur pendant le démarrage

Les étapes suivantes sont spécifiques au chargeur GRUB (GRand Unified Bootloader) de Linux. Vous devrez faire des changements du même type 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` de la manière suivante :

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 :

```
kernel..... console=ttyS1,57600
```

3. Si le fichier `/etc/grub.conf` contient une instruction `splashimage`, transformez-la en commentaire.

L'exemple suivant illustre les modifications décrites dans cette procédure.

```
# grub.conf généré par anaconda
#
# Notez que vous n'avez pas besoin de réexécuter le grub après avoir apporté des modifications
# à ce fichier
# AVIS : vous n'avez pas de partition /d'amorçage. Cela signifie que
# tous les chemins du noyau et initrd sont relatifs à /, par exemple
# root (hd0,0)
# kernel /boot/vmlinuz-version ro root=/dev/sdal
# initrd /boot/initrd-version.img
#
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz

serial --unit=1 --speed=57600
terminal --timeout=10 serial

title Red Hat Linux Advanced Server (2.4.9-e.3smp)
root (hd0,0)
kernel /boot/vmlinuz-2.4.9-e.3smp ro root=/dev/sdal hda=ide-scsi console=ttyS0 console=ttyS1,57600
initrd /boot/initrd-2.4.9-e.3smp.img
title Red Hat Linux Advanced Server-up (2.4.9-e.3)
root (hd0,00)
kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sdal
initrd /boot/initrd-2.4.9-e.3.img
```

Lors de l'édition du fichier `/etc/grub.conf`, respectez les consignes suivantes :

- Désactivez l'interface graphique de GRUB et utilisez l'interface texte. Dans le cas contraire, l'écran de GRUB ne s'affiche pas sur la redirection de console. Pour désactiver l'interface utilisateur, commentez la ligne commençant 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 décrit comment le processus INIT
# doit configurer le système sur 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 : interrompre (Ne définissez PAS initdefault sur ce niveau)
# 1 : Mode d'utilisateur unique
# 2 - Multi-utilisateurs, sans NFS (Identique à 3, si vous
#    ne disposez pas de mise en réseau)
# 3 : Mode multi-utilisateurs intégral
# 4 : inutilisé
# 5 : X11
# 6 : redémarrer (Ne définissez PAS initdefault sur ce niveau)
#
id:3:initdefault:

# Initialisation du système.
si::sysinit:/etc/rc.d/rc.sysinit

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

# Éléments à exécuter à chaque niveau d'exécution.
ud::once:/sbin/update

# Interrompre CTRL-ALT-SUPPR
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

# Lorsque notre onduleur nous indique une coupure d'alimentation, nous supposons qu'il ne nous reste que quelques
# minutes avant que tout s'arrête. Programmez un arrêt pendant 2 minutes à compter de maintenant.
# Ceci part bien évidemment du principe que vous avez installé une source d'alimentation et que votre
# onduleur est connecté et fonctionne correctement.
pf::powerfail:/sbin/shutdown -f -h +2 "Coupure d'alimentation ; arrêt du système"
# Si l'alimentation a été rétablie avant l'exécution de la procédure d'arrêt, annulez-la.
pr:12345:powerokwait:/sbin/shutdown -c "Alimentation rétablie ; arrêt annulé"

# Exécutez gettys aux 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 au niveau d'exécution 5
# xdm est désormais un service séparé
x:5:respawn:/etc/X11/prefdm -nodaemon
```

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

- Ajoutez une nouvelle ligne avec le nom du tty série de COM2 :

```
ttyS1
```

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

vc/1
vc/2
vc/3
vc/4
vc/5
vc/6
vc/7
vc/8
vc/9
vc/10
vc/11
tty1
tty2
tty3
tty4
tty5
tty6
tty7
tty8
tty9
tty10
tty11
ttyS1

[Retour à la page Contenu](#)

[Retour à la page Contenu](#)

Utilisation de FlexAddress Plus

Micrologiciel Dell Chassis Management Controller Version 3.1 Guide d'utilisation

- [Activation de FlexAddress Plus](#)
- [FlexAddress comparé à FlexAddress Plus](#)
- [Allocation d'adresse MAC, schéma 1 et schéma 2](#)

FlexAddress Plus est une nouvelle fonctionnalité ajoutée à la carte de fonction version 2.0. Il s'agit d'une mise à niveau depuis la fonctionnalité FlexAddress version 1.0. FlexAddress Plus contient davantage d'adresses MAC que la fonctionnalité FlexAddress. Ces deux fonctionnalités permettent au châssis d'attribuer les adresses WWN/MAC (World Wide Name/Media Access Control) aux périphériques Fibre Channel et Ethernet. Les adresses WWN/MAC attribuées par le châssis sont globalement uniques et spécifiques à un logement de serveur.

Activation de FlexAddress Plus

La fonctionnalité FlexAddress Plus est offerte sur la carte Secure Digital (SD), tout comme la fonctionnalité FlexAddress.

 **REMARQUE** : la carte SD libellée FlexAddress ne contient que la fonctionnalité FlexAddress, et la carte libellée FlexAddress Plus contient FlexAddress et FlexAddress Plus. Pour activer la fonctionnalité, la carte doit être insérée dans le module CMC.

Certains serveurs, tels que PowerEdge M710HD, peuvent avoir besoin plus d'adresses MAC que FA ne peut en procurer à CMC, selon leur configuration. Pour ces serveurs, une mise à niveau vers FA+ permet d'optimiser pleinement la configuration WWN/MAC. Veuillez contacter Dell pour obtenir de l'assistance concernant la fonctionnalité FlexAddress Plus.

Les mises à jour logicielles suivantes sont requises pour activer la fonctionnalité FlexAddress Plus : serveur BIOS, serveur iDRAC et micrologiciel CMC. Si ces mises à jour ne sont pas appliquées, seule la fonctionnalité FlexAddress est disponible.

Tableau 7-1. Mises à jour requises pour Flexaddress Plus

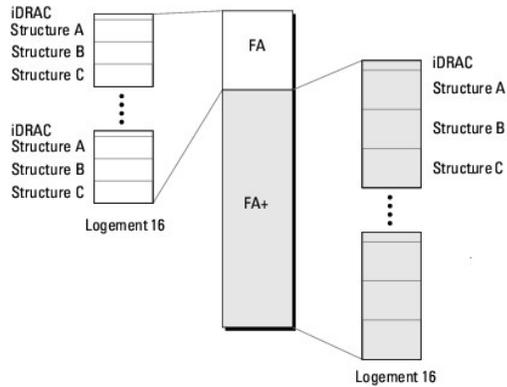
Composant	Version minimale requise
BIOS du module serveur	PowerEdge M710hd
iDRAC	Version 3.0 ou une version ultérieure
CMC	Version 3.0 ou une version ultérieure

FlexAddress comparé à FlexAddress Plus

FlexAddress a 208 adresses réparties dans 16 logements de serveur, chacun étant alloué à 13 MAC. FlexAddress a 2 928 adresses réparties dans 16 logements de serveur, chacun étant alloué à 183 MAC. Le tableau ci-dessous indique la disposition des adresses MAC dans les deux fonctionnalités.

	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 7-1. Fonctionnalité FlexAddress (FA) comparée à la fonctionnalité FlexPlusAddress (FA+)



Allocation d'adresse MAC, schéma 1 et schéma 2

Pour la rétrocompatibilité avec FA, les adresses dans FA + sont divisées en deux groupes : le premier groupe compte 208 adresses et le second groupe 2 928 adresses. Dans le premier groupe, 13 MAC sont alloués par logement (16 logements au total) comme avec FA. Dans le second groupe, 183 MAC sont alloués par logement.

L'attribution des 13 adresses MAC du premier groupe pour chaque serveur est divisée comme suit : un pour iDRAC et quatre pour chaque structure (A, B et C). Au sein de chaque structure (A, B et C), deux adresses sont allouées au port 1 et deux adresses sont allouées au port 2. Voici le résultat :

- 1 1 MAC pour la gestion iDRAC
- 1 4 MAC pour la structure A (deux MAC pour le port 1, deux MAC pour le port 2)
- 1 4 MAC pour la structure B (deux MAC pour le port 1, deux MAC pour le port 2)
- 1 4 MAC pour la structure C (deux MAC pour le port 1, deux MAC pour le port 2)

Pour référence, cette allocation d'adresse MAC est appelée schéma 1.

L'allocation des 183 adresses MAC pour le deuxième groupe de chaque serveur est également divisée en trois pour iDRAC, 60 pour chaque structure (A, B et C). Au sein de chaque structure, 30 adresses sont allouées au port 1 et 30 adresses sont allouées au port 2. Voici le résultat :

- 1 3 MAC pour la gestion iDRAC
- 1 60 MAC pour la structure A (30 MAC pour le port 1, 30 MAC pour le port 2)
- 1 60 MAC pour la structure B (30 MAC pour le port 1, 30 MAC pour le port 2)
- 1 60 MAC pour la structure C (30 MAC pour le port 1, 30 MAC pour le port 2)

Pour référence, cette allocation d'adresse MAC est appelée schéma 2.

Pour l'allocation des adresses MAC, la méthode la plus courante consiste à allouer des adresses MAC par structure depuis le schéma 1 au départ. Si une structure nécessite plus d'adresses que celles fournies par le schéma 1, deux MAC supplémentaires par structure sont alloués depuis le schéma 2.

Quand un châssis est activé uniquement avec FA et qu'il a un serveur avec une configuration réseau qui nécessite plus d'adresses que celles fournies par le schéma 1, les adresses supplémentaires ne sont pas disponibles. Le statut affiché est *Non installé*.

Si FA est activé sur un châssis, FA n'a pas besoin d'être désactivé afin d'ajouter FA +.

Dans ce cas, les allocations d'adresses MAC sont appliquées comme suit :

- 1 Les adresses MAC du schéma 1 sont attribuées depuis FA de la carte 1.0. Il n'y a aucun changement dans la précédente configuration WWN/MAC
- 1 Les adresses MAC supplémentaires du schéma 2 sont allouées depuis les adresses du schéma 2 de FA +.

Exemple d'allocation d'adresse MAC

En supposant que l'adresse de départ des MAC dans FA est 00:FA:AE:58:59:2B, l'adresse de départ des MAC dans le schéma 2 de FA+ est 00:FB:AE:58:59:FB. Le serveur est dans le logement 1, la configuration réseau pour le serveur est :

- 1 1 MAC pour iDRAC
- 1 8 MAC pour la structure A
- 1 4 MAC pour la structure B
- 1 4 MAC pour la structure C

Puisque la structure A a besoin de quatre adresses MAC de plus qu'avec le schéma 1, les 4 premières adresses MAC sont attribuées depuis le FA basé sur le

schéma 1 avec deux MA pour le port 1 et deux MAC pour le port 2. Les quatre autres adresses MAC sont attribuées depuis FA + basé sur le schéma 2, avec deux MAC pour le port 1 et deux MAC pour le port 2. L'allocation des adresses MAC pour iDRAC pour les structures B et C est de FA basé sur le schéma 1.

L'adresse de départ de la structure A port 1 depuis FA+ est 00:23:AE:58:59:FE, parce que les 3 premières MAC sont réservées à iDRAC. Ainsi, les adresses MAC attribuées au châssis sont :

iDRAC	00:FA:AE:58:59:2B (depuis FA)
Structure A port 1 :	00:FA:AE:58:59:2C(depuis FA) 00:FA:AE:58:59:2D (depuis FA) 00:FB:AE:58:59:FE (depuis FA+) 00:FB:AE:58:59:FF (depuis FA+)
Structure A port 2 :	00:FA:AE:58:59:2E (depuis FA) 00:FA:AE:58:59:2F (depuis FA) 00:FB:AE:58:5A:00 (depuis FA+) 00:FB:AE:58:5A:01 (depuis FA+)
Structure B port 1 :	00:FA:AE:58:59:30 (depuis FA) 00:FA:AE:58:59:31 (depuis FA)
Structure B port 2 :	00:FA:AE:58:59:32 (depuis FA) 00:FA:AE:58:59:33 (depuis FA)
Structure C port 1 :	00:FA:AE:58:59:34 (depuis FA) 00:FA:AE:58:59:35 (depuis FA)
Structure C port 2 :	00:FA:AE:58:59:36 (depuis FA) 00:FA:AE:58:59:37 (depuis FA)

Quand un châssis est sans précédent FA (n'ayant jamais été activé ou ayant été activé puis désactivé) avec un serveur dont la configuration réseau nécessite plus d'adresses qu'avec le schéma 1, l'allocation du schéma 1 acquiert des adresses depuis le schéma 1 de FA et l'allocation du schéma 2 acquiert des adresses depuis le schéma 2 de FA+.

En utilisant le même exemple, les adresses MAC attribuées au châssis du même serveur dans ce scénario sont les suivantes :

iDRAC	00:FB:AE:58:59:2B (FA)
Structure A port 1 :	00:FB:AE:58:59:2C (FA) 00:FB:AE:58:59:2D (FA) 00:FB:AE:58:59:FE (FA+) 00:FB:AE:58:59:FF (FA+)
Structure A port 2 :	00:FB:AE:58:59:2E (FA) 00:FB:AE:58:59:2F (FA) 00:FB:AE:58:5A:00 (FA+) 00:FB:AE:58:5A:01 (FA+)
Structure B port 1 :	00:FB:AE:58:59:30 (FA) 00:FB:AE:58:59:31 (FA)
Structure B port 2 :	00:FB:AE:58:59:32 (FA) 00:FB:AE:58:59:33 (FA)
Structure C port 1 :	00:FB:AE:58:59:34 (FA) 00:FB:AE:58:59:35 (FA)
Structure C port 2 :	00:FB:AE:58:59:36 (FA) 00:FB:AE:58:59:37 (FA)

[Retour à la page Contenu](#)

Utilisation de FlexAddress

Micrologiciel Dell Chassis Management Controller Version 3.1 Guide d'utilisation

- [Activation de FlexAddress](#)
- [Désactivation de FlexAddress](#)
- [Configuration de FlexAddress à l'aide de la CLI](#)
- [Consultation de l'état de FlexAddress à l'aide de la CLI](#)
- [Configuration de FlexAddress via l'interface utilisateur](#)
- [Dépannage de FlexAddress](#)
- [Messages des commandes](#)
- [CONTRAT DE LICENCE DES LOGICIELS DELL 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.

Chaque module serveur se voit attribuer des ID WWN et/ou MAC uniques lors de la fabrication. Avant FlexAddress, si vous deviez remplacer un module de serveur par un autre, les identifiants WWN/MAC changeaient et il fallait alors reconfigurer les outils de gestion réseau Ethernet et les ressources du SAN pour prendre en compte le nouveau module de serveur.

FlexAddress permet à CMC d'attribuer des identifiants WWN/MAC à un logement particulier et de *remplacer* les identifiants d'usine. Les identifiants WWN/MAC des logements sont conservés lors du remplacement du module de serveur. Grâce à cette fonctionnalité, il n'est plus nécessaire de reconfigurer les outils de gestion réseau Ethernet et les ressources du SAN lors de l'ajout d'un nouveau module de serveur.

De plus, le *remplacement* s'effectue uniquement lorsqu'un module de serveur est inséré dans un châssis pour lequel la fonctionnalité FlexAddress est activée, aucune modification permanente n'est apportée au module de serveur. Si vous déplacez un module de serveur dans un châssis qui ne prend pas en charge FlexAddress, les identifiants WWN/MAC d'usine sont utilisés.

Avant d'installer FlexAddress, vous pouvez déterminer la plage d'adresses MAC contenue dans une carte de fonctionnalité FlexAddress en insérant la carte SD dans un lecteur de cartes mémoire USB et en consultant le fichier `pwwn_mac.xml`. Ce fichier XML de la carte SD n'est pas crypté et contient une balise XML `mac_start` qui représente la première adresse MAC hexadécimale utilisée pour cette plage d'adresses MAC unique. Le marqueur `mac_count` représente le nombre total d'adresses MAC allouées par la carte SD. La plage totale d'adresses MAC allouées peut être déterminée par l'opération suivante :

```
<mac_start> + 0xCF (208 - 1) = mac_end
```

où 208 correspond à `mac_count` et la formule est
`<mac_start> + <mac_count> - 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 éviter d'en modifier le contenu accidentellement. Vous devez *déverrouiller* la carte SD avant de l'insérer dans le module CMC.

Activation de FlexAddress

FlexAddress est livrée sur une carte Secure Digital (SD) qui doit être insérée dans CMC pour activer la fonctionnalité. Pour activer la fonctionnalité FlexAddress, des mises à jour logicielles peuvent être requises ; **si vous n'activez pas FlexAddress, ces mises à jour ne sont pas requises**. Les mises à jour, répertoriées dans le tableau ci-dessous, comprennent les BIOS des modules de serveur, les BIOS ou micrologiciels des cartes porteuses d'E/S et les micrologiciels CMC. Vous devez appliquer ces mises à jour avant d'activer FlexAddress. Si ces mises à jour ne sont pas appliquées, la fonctionnalité FlexAddress peut ne pas fonctionner 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 ultérieure pour les systèmes PowerEdge xx0x Version 2.10 ou ultérieure 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 un déploiement correct de la fonctionnalité 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 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.

Consultez le document *Spécifications techniques de la carte Secure Digital (SD) de Chassis Management Controller (CMC)* pour installer la carte SD.

 **REMARQUE** : la carte SD dispose d'une fonctionnalité FlexAddress. Les données contenues dans la carte SD sont cryptées et ne peuvent en aucune façon être dupliquées ou modifiées afin de garantir que le système et ses fonctions restent opérationnels.

 **REMARQUE** : vous ne pouvez utiliser la carte SD que sur un seul châssis à la fois. Si vous avez plusieurs châssis, vous devez acheter d'autres cartes SD.

L'activation de la fonctionnalité FlexAddress est automatique au redémarrage de CMC une fois que la carte de fonctionnalité SD est installée ; cette activation lie la fonctionnalité au châssis actuel. Si la carte SD est installée sur le contrôleur CMC redondant, l'activation de la fonctionnalité FlexAddress n'a lieu que lorsque le CMC redondant devient actif. Consultez le document *Spécifications techniques de la carte Secure Digital (SD) de Chassis Management Controller (CMC)* pour plus d'informations sur l'activation du contrôleur CMC de secours.

Lorsque CMC a redémarré, vérifiez l'activation en suivant les instructions de la section suivante, [Vérification de l'activation de FlexAddress](#).

Vérification de l'activation de FlexAddress

Vous pouvez utiliser des commandes de l'utilitaire RACADM pour vérifier l'activation de la carte de fonctionnalité SD et l'activation FlexAddress.

Utilisez la commande de l'utilitaire RACADM suivante pour vérifier la carte de fonctionnalité SD et son état :

```
racadm featurecard -s
```

Tableau 6-1. Messages d'état renvoyés par la commande featurecard -s

Message d'état	Actions
Aucune carte de fonction insérée.	Vérifiez que la carte SD est correctement insérée dans le contrôleur CMC. Dans une configuration CMC redondante, assurez-vous que CMC sur lequel est installée la carte de fonctionnalité SD est le contrôleur CMC actif, et non celui 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 ou les fonction(s) suivante(s) FlexAddress : La carte de fonction est liée à un autre châssis, svctag = ABC1234, SD card SN = 01122334455	Retirez la carte SD, localisez et installez la carte SD du châssis actuel.
La carte de fonction insérée est valide et contient la fonctionnalité FlexAddress suivante : la carte de fonction n'est pas liée à ce châssis.	Cette carte de fonctionnalité SD peut être déplacée dans un autre châssis ou réactivée dans le châssis actuel. Pour la réactiver dans le châssis actuel, entrez racadm racreset jusqu'à ce que le module CMC dans lequel la carte de fonctionnalité 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 d'état suivant :

```
Fonction = FlexAddress
```

Date d'activation = 8 avril 2008 - 10:39:40

Fonction installée depuis le numéro de carte SD = 01122334455

Si aucune fonctionnalité n'est active sur le châssis, la commande renvoie le message :

```
racadm feature -s
```

Aucune fonction active sur le châssis.

Les cartes de fonction Dell peuvent contenir plusieurs fonctions. Une fois que toutes les fonctions figurant sur une carte de fonction Dell ont été activées sur un châssis, les autres fonctions pouvant être incluses sur cette carte Dell ne peuvent pas être activées sur un châssis différent. Dans ce cas, la commande -s de la fonction racadm affiche le message suivant pour les fonctions concernées :

ERREUR : une ou plusieurs caractéristiques de la carte SD sont actives sur un autre châssis.

Pour des informations supplémentaires sur les commandes RACADM, voir les sections de commandes **fonction** et **carte de fonction** du *Guide de référence de ligne de commande pour iDRAC6 et CMC*.

Désactivation de FlexAddress

Il est possible de désactiver la fonctionnalité FlexAddress et de rétablir la carte SD à l'état précédant l'installation à l'aide d'une commande RACADM. Il n'existe aucune fonctionnalité de désactivation dans l'interface Web. La désactivation rétablit l'état d'origine de la carte SD : elle peut alors être installée et activée sur un autre châssis.

 **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 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.

Désactivation de FlexAddress

Utilisez la commande RACADM suivante pour désactiver la fonctionnalité FlexAddress et restaurer la carte SD :

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

Si la désactivation réussit, la commande renvoie le message d'état suivant :

La désactivation de la fonctionnalité FlexAddress sur le châssis a réussi.

Si le châssis n'a pas été mis hors tension 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 des informations supplémentaires sur la commande, voir la section de commande **fonction** du *Guide de référence de ligne de commande pour iDRAC6 et CMC*.

Configuration de FlexAddress à l'aide de la CLI

 **REMARQUE** : vous devez activer les deux (le logement et la structure) pour que l'adresse MAC assignée par le châssis soit poussée vers iDRAC.

 **REMARQUE** : vous pouvez également consulter la condition de FlexAddress à l'aide de l'interface utilisateur graphique. Pour plus d'informations, voir [FlexAddress](#).

Vous pouvez utiliser l'interface de ligne de commande pour activer ou désactiver FlexAddress structure par structure. Vous pouvez également activer/désactiver cette fonctionnalité logement par logement. Une fois que vous avez activé cette fonctionnalité par structure, vous pouvez sélectionner les logements à activer. Par exemple, si seule la structure A est activée, FlexAddress est activée uniquement sur la structure A des logements activés. Toutes les autres structures utilisent les identifiants WWN/MAC d'usine sur le serveur. Pour que cette fonctionnalité fonctionne, la structure doit être activée et le serveur doit être mis hors tension.

FlexAddress est activée sur les logements activés de toutes les structures qui sont activées. Par exemple, il n'est pas possible d'activer les structures A et B et d'activer FlexAddress pour le logement 1 de la structure A, mais pas de la structure B.

Utilisez la commande de l'utilitaire RACADM suivante pour activer ou désactiver les structures :

```
racadm setflexaddr [-f <nom de la structure> <état>]
```

<Nom de la structure> = A, B, C ou iDRAC

<état> = 0 ou 1

Où 0 est désactivé et 1 activé.

Utilisez la commande de l'utilitaire RACADM suivante pour activer ou désactiver des logements :

```
racadm setflexaddr [-i <N° logement> <état>]
```

<N° logement> compris entre 1 et 16

<état> = 0 ou 1

Où 0 est désactivé et 1 activé.

Pour des informations supplémentaires sur la commande, voir la section de commande `setflexaddr` du *Guide de référence de ligne de commande pour iDRAC6 et CMC*.

Configuration complémentaire de FlexAddress pour Linux

Lorsque vous passez d'un ID MAC attribué par le serveur à un ID MAC attribué par le châssis sur un système d'exploitation basé sur Linux, il peut être nécessaire d'effectuer des étapes de configuration supplémentaires :

- 1 SUSE Linux Enterprise Server 9 et 10 : vous devez exécuter YAST (Yet another Setup Tool) sur votre système Linux pour configurer vos périphériques réseau, puis redémarrer les services réseau.
- 1 Red Hat Enterprise Linux 4 (RHEL) et RHEL 5 : exécutez Kudzu, un utilitaire permettant de détecter et de configurer le matériel ajouté/modifié sur le système. Kudzu comprend le menu de découverte du matériel ; il détecte les modifications des adresses MAC lors du retrait et de l'ajout de matériel.

Consultation de l'état de FlexAddress à l'aide de la CLI

Vous pouvez utiliser l'interface de ligne de commande pour consulter les informations d'état de FlexAddress. Vous pouvez consulter les informations relatives à la condition pour l'ensemble du châssis ou un logement particulier. Les informations affichées incluent :

- 1 Configuration des structures
- 1 FlexAddress activée/désactivée
- 1 Numéro et nom du logement
- 1 Adresses attribuées par le châssis et le serveur
- 1 Adresses en cours d'utilisation

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 <N° logement>]
```

<N° logement> compris entre 1 et 16

Voir [Configuration de FlexAddress à l'aide de la CLI](#) pour des détails supplémentaires sur la configuration de FlexAddress. Pour des informations supplémentaires sur la commande, voir la section de commande `getflexaddr` du *Guide de référence de ligne de commande pour iDRAC6 et CMC*.

Configuration de FlexAddress via l'interface utilisateur

Réveil sur LAN avec FlexAddress

Lorsque la fonctionnalité FlexAddress est déployée pour la première fois, il est nécessaire de mettre le module serveur hors tension, puis de le remettre sous tension pour que la fonctionnalité FlexAddress soit prise en compte. FlexAddress est programmée par le BIOS du module serveur sur les périphériques Ethernet. Pour que le BIOS du module serveur programme l'adresse, il faut qu'il soit opérationnel, ce qui nécessite la mise sous tension du module serveur. Une fois que les séquences de mise hors tension et de mise sous tension ont été exécutées, les ID MAC attribués par le châssis sont disponibles pour la fonction Réveil sur LAN (WOL).

Dépannage de FlexAddress

Cette section contient des informations de dépannage pour FlexAddress.

1. Que se passe-t-il si une carte de fonction est retirée ?

Rien. Les cartes de fonction peuvent être retirées et stockées ou laissées en place.

2. 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 une erreur qui indique :

Cette carte de fonction a été activée sur un autre châssis. Elle doit être retirée avant d'accéder à la fonctionnalité 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> : fonctionnalité 'FlexAddress@XXXXXXX' non activée ; ID châssis='YYYYYYY'
```

3. Que se passe-t-il si la carte de fonction est retirée et qu'une carte non FlexAddress est installée ?

Aucune activation ou modification de la carte n'a lieu. CMC ignore la carte. Dans ce cas, la commande **\$racadm featurecard -s** renvoie le message suivant :

Aucune carte de fonction insérée

ERREUR : impossible d'ouvrir le fichier

4. Que se passe-t-il si une carte de fonction est liée à un châssis dont le numéro de service est reprogrammé ?

- 1 Si la carte de fonction d'origine figure dans le contrôleur CMC actif sur ce châssis ou sur un autre châssis, l'interface Web affiche une erreur indiquant ce qui suit :

Cette carte de fonction a été activée sur un autre châssis. Elle doit être retirée avant d'accéder à la fonctionnalité FlexAddress

Numéro de service du châssis actuel= XXXXXXXX

Numéro de service du châssis de la carte de fonction = YYYYYYYY

La carte de fonction d'origine ne peut plus être désactivée sur ce châssis ou sur un autre châssis, à moins que l'assistance Dell ne reprogramme le numéro de service du châssis d'origine dans un châssis et que le contrôleur CMC sur lequel est installée la carte de fonction d'origine devienne actif sur ce châssis.

- 1 La fonctionnalité FlexAddress reste activée sur le châssis initialement lié. La fonctionnalité de *liaison de ce châssis* est mise à jour pour refléter le nouveau numéro de service.

5. Vais-je recevoir un message d'erreur si deux cartes de fonction sont installées sur mon système CMC redondant ?

La carte de fonction du contrôleur CMC actif est active et installée dans le châssis. CMC ignore la deuxième carte.

6. Est-ce que la carte SD dispose d'un verrou de protection en écriture ?

Oui. Avant d'installer la carte SD dans le contrôleur CMC, vérifiez que le loquet de protection en écriture est en position « déverrouillée ». La fonctionnalité FlexAddress ne peut être activée si la carte SD est protégée en écriture. Dans ce cas, la commande **\$racadm feature -s** renvoie le message suivant :

Aucune fonction active sur le châssis. ERREUR : système de fichiers en lecture seule

7. 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.

8. Qu'advient-il de la fonctionnalité FlexAddress si le BIOS du serveur est mis à jour d'une version 1.xx à une version 2.xx ?

Le module de serveur doit être mis hors tension avant de pouvoir être utilisé avec FlexAddress. Une fois la mise à jour du BIOS du serveur terminée, le module de serveur n'obtient pas d'adresses attribuées par le châssis avant la mise hors tension, puis la mise sous tension du serveur.

9. 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 ?

- 1 La fonctionnalité FlexAddress et sa configuration sont supprimées du châssis.
- 1 La carte de fonctionnalité utilisée pour activer la fonctionnalité sur ce châssis est inchangée et reste liée au châssis. Lorsque le micrologiciel CMC du châssis est mis à niveau par la suite à la version 1.10 ou ultérieure, la fonctionnalité FlexAddress est réactivée par réinsertion de la carte de fonction d'origine (le cas échéant), en réinitialisant CMC (si la carte de fonction a été insérée à la fin de la mise à niveau du micrologiciel) et en reconfigurant la fonctionnalité.

10. 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 contrôleur CMC par un autre dont la version de micrologiciel est antérieure à la version 1.10, vous devez suivre la procédure suivante pour que la fonctionnalité et la configuration FlexAddress actuelles ne soient PAS supprimées.

- a. Assurez-vous que la version du micrologiciel CMC actif est toujours la version 1.10 ou une version ultérieure.
- b. Retirez le contrôleur CMC de secours et insérez un nouveau contrôleur CMC à son emplacement.
- c. À partir de CMC actif, mettez à niveau le micrologiciel CMC de secours vers la version 1.10 ou une version ultérieure.

 **REMARQUE** : si vous ne mettez pas à jour le micrologiciel CMC de secours vers la version 1.10 ou une version ultérieure et qu'un basculement se produit, la fonctionnalité FlexAddress n'est pas configurée et vous devez alors réactiver et reconfigurer la fonctionnalité.

11. La carte SD ne se trouvait pas dans le châssis lorsque j'ai exécuté la commande de désactivation sur FlexAddress. Comment puis-je récupérer la carte SD maintenant ?

Le problème est que la carte SD ne peut pas être utilisée pour installer FlexAddress sur un autre châssis si elle ne se trouvait pas dans CMC lorsque FlexAddress a été désactivée. Pour restaurer l'usage de la carte, réinsérez-la dans un contrôleur CMC dans le châssis à laquelle elle est liée, réinstallez FlexAddress, puis désactivez à nouveau FlexAddress.

12. La carte SD est installée correctement et toutes les mises à jour de micrologiciel/logicielles sont installées. FlexAddress semble active, mais aucune option de l'écran de déploiement du serveur ne me permet de déployer cette fonctionnalité. Qu'est-ce qui ne fonctionne pas ?

Ils 'agit d'un problème de cache du navigateur. Fermez le navigateur, puis relancez-le.

13. Qu'advient-il de FlexAddress si je dois réinitialiser la configuration de mon châssis avec la commande RACADM `racresetcfg` ?

La fonctionnalité FlexAddress restera activée et prête à l'utilisation. Toutes les structures et tous les logements seront sélectionnés comme structures et logements par défaut.

 **REMARQUE** : il est vivement recommandé de mettre le châssis hors tension avant d'émettre la commande RACADM `racresetcfg`.

Messages des commandes

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

Tableau 6-2. Sortie et commandes FlexAddress

Problème	Commande	Sortie
La carte SD du contrôleur CMC actif est liée à un autre numéro de service.	<code>\$racadm featurecard -s</code>	La carte de fonction insérée est valide et contient la ou les fonction(s) suivante(s) FlexAddress : la carte de fonction est liée à un autre châssis, numéro de service = J310TF1 numéro de série de la carte SD =0188BFFE03A
La carte SD du contrôleur CMC actif est liée au même numéro de service.	<code>\$racadm featurecard -s</code>	La carte de fonction insérée est valide et contient la ou les fonction(s) suivante(s) 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.	<code>\$racadm featurecard -s</code>	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)	<code>\$racadm setflexaddr [-f <nom de la structure> <état du logement>] OU</code> <code>\$racadm setflexaddr [-i <n° logement> <état du logement>]</code>	ERREUR : la fonctionnalité Flexaddress n'est pas active sur le châssis
L'utilisateur invité tente de définir FlexAddress sur des logements/des structures.	<code>\$racadm setflexaddr [-f <nom de la structure> <état du logement>]</code> <code>\$racadm setflexaddr [-i <n° logement> <état du logement>]</code>	ERREUR : privilèges utilisateur insuffisants pour effectuer cette opération
Désactivation de la fonctionnalité FlexAddress alors que le châssis est sous tension	<code>\$racadm feature -d -c flexaddress</code>	ERREUR : impossible de désactiver la fonction car le châssis est SOUS TENSION
L'utilisateur invité essaie de désactiver la fonctionnalité sur le châssis	<code>\$racadm feature -d -c flexaddress</code>	ERREUR : privilèges utilisateur insuffisants pour effectuer cette opération
Modification des paramètres FlexAddress de logement/structure pendant que les modules de serveur sont sous tension.	<code>\$racadm setflexaddr -i 1 1</code>	ERREUR : impossible d'exécuter l'opération demandée car elle affecte le serveur SOUS TENSION

CONTRAT DE LICENCE DES LOGICIELS DELL FlexAddress

Le présent document constitue un contrat liant l'utilisateur du Logiciel à Dell Products, L.P. ou Dell Global B.V. (« Dell »). Ce contrat s'applique à tous les

logiciels distribués avec le produit Dell, pour lesquels il n'existe aucun contrat de licence distinct vous liant avec l'éditeur ou le propriétaire du logiciel (collectivement ci-après, le « Logiciel »). Ce contrat ne concerne pas la vente du Logiciel ou de toute autre propriété intellectuelle. Tous les droits concernant la propriété intellectuelle du Logiciel sont détenus par l'éditeur ou le propriétaire du Logiciel. Tous les droits non expressément accordés dans le présent contrat sont réservés par l'éditeur ou le propriétaire du Logiciel. En ouvrant l'emballage contenant le Logiciel, en installant ou en téléchargeant le Logiciel, ou en utilisant le Logiciel préchargé ou intégré à votre produit, vous acceptez d'être lié par les termes du présent Contrat. Si vous refusez ces conditions, retournez rapidement tous les éléments composant le Logiciel (disques, documentations et emballage), et désinstallez le Logiciel préchargé ou intégré au produit.

Vous ne pouvez utiliser le Logiciel que sur un ordinateur à la fois. Si vous disposez de plusieurs licences pour le Logiciel, vous pouvez en utiliser autant d'exemplaires que vous avez de licences. Le terme « Utiliser » désigne le chargement dans la mémoire temporaire ou permanente de l'ordinateur. L'installation sur un serveur de réseau à des fins de distribution sur d'autres postes de travail n'est pas considérée comme une « Utilisation » si, et seulement si, vous disposez d'une licence distincte pour chaque ordinateur sur lequel le Logiciel est distribué. Vous devez vous assurer que le nombre de personnes utilisant le Logiciel installé sur un serveur de réseau n'excède pas le nombre de licences que vous possédez. Si le nombre d'utilisateurs du Logiciel installé sur un serveur de réseau excède votre nombre de licences, vous devez vous procurer une licence additionnelle pour chacun des utilisateurs en surnombre avant d'autoriser ceux-ci à utiliser le Logiciel. Si vous êtes une entreprise cliente de Dell ou une société affiliée de Dell, vous autorisez Dell, ou tout agent sélectionné par Dell, le droit de contrôler votre utilisation du Logiciel aux heures normales de bureau, et vous acceptez de collaborer avec Dell dans le cadre de cet audit. Vous acceptez de fournir à Dell toutes les données pouvant raisonnablement être considérées comme ayant un rapport avec votre utilisation du Logiciel. Le contrôle sera limité à la vérification de votre respect des dispositions du présent contrat.

Ce Logiciel est protégé par la loi relative au droit d'auteur et par les conventions internationales. Vous êtes autorisé à créer une seule copie du Logiciel à des fins de sauvegarde ou d'archivage, ou à le transférer sur un seul disque dur, à la condition que vous conserviez l'original uniquement à des fins de sauvegarde ou d'archivage. Vous n'êtes pas autorisé à prêter ni à louer le Logiciel ni à copier les documents imprimés fournis avec celui-ci. Vous êtes autorisé à transférer à titre permanent le Logiciel et tous ses composants dans le cadre de la vente ou du transfert du produit Dell, à condition que vous n'en conserviez aucun exemplaire, que vous transfériez la totalité du Logiciel (y compris tous ses composants, les supports et la documentation imprimée), et que le bénéficiaire du transfert accepte les termes du présent contrat. Tout transfert doit inclure la mise à jour la plus récente ainsi que toutes les versions précédentes. Vous n'êtes pas autorisé à reconstituer la logique du Logiciel, à le décompiler ou à le désassembler. Si le kit fourni avec l'ordinateur contient des disques compacts et/ou des disquettes 3 pouces $\frac{1}{2}$ ou 5 pouces $\frac{3}{4}$, vous ne pouvez utiliser que les disques du format approprié pour l'ordinateur. Vous n'êtes pas autorisé à utiliser les disques sur un autre ordinateur ou réseau ni à les louer, les prêter ou les transférer à un autre utilisateur, sauf si l'opération s'effectue en conformité avec les dispositions du présent contrat.

GARANTIE LIMITÉE

Dell garantit que les disques du Logiciel sont exempts de tout défaut matériel et de fabrication dans des conditions normales d'utilisation, pour une période de 90 (quatre-vingt dix) jours à compter de leur date de réception. Cette garantie limitée ne s'applique qu'à vous et n'est pas transférable. Toute garantie implicite est limitée à une période de 90 (quatre-vingt dix) jours à compter de la date à laquelle vous avez reçu le Logiciel. Certaines législations n'autorisent pas la limitation des garanties implicites, auquel cas, la limitation ci-dessus ne vous sera pas applicable. La responsabilité totale de Dell et de ses fournisseurs, et le seul recours dont vous disposez, sont limités soit (a) au remboursement du montant payé pour le Logiciel ou (b) au remplacement de tout disque non conforme aux dispositions de la présente garantie et ayant été renvoyé à Dell accompagné d'un numéro d'autorisation de retour, les coûts et risques afférents étant de votre responsabilité. Cette garantie ne s'appliquera pas en cas de dommage au disque causé par une utilisation incorrecte, un accident, un acte de vandalisme, ou en cas de modifications ou d'opérations de maintenance non effectuées par Dell. Tout disque fourni en remplacement du disque d'origine est garanti pour la durée la plus longue entre (a) le nombre de jours restants par rapport à la garantie d'origine ou (b) un délai de 30 (trente) jours.

Dell ne garantit PAS le fonctionnement ininterrompu ou sans erreur du Logiciel, NI son adéquation à vos besoins. Le fait d'avoir choisi ce Logiciel pour obtenir les résultats attendus, son utilisation et les résultats obtenus sont de votre seule et unique responsabilité.

EN SON NOM PROPRE ET CELUI DE SES FOURNISSEURS, DELL DÉCLINE TOUTE AUTRE GARANTIE OU CONDITION EXPRESSE OU IMPLICITE, INCLUANT SANS RESTRICTION LES GARANTIES ET CONDITIONS IMPLICITES DE QUALITÉ OU D'ADAPTABILITÉ À UN USAGE PARTICULIER, RELATIVES AU LOGICIEL ET AUX DOCUMENTS FOURNIS AVEC CELUI-CI. Cette garantie limitée vous donne des droits légaux spécifiques, auxquels peuvent s'ajouter d'autres droits, qui varient selon la juridiction.

DELL ET SES FOURNISSEURS NE SONT EN AUCUN CAS RESPONSABLES DES DOMMAGES QUELS QU'ILS SOIENT, Y COMPRIS, MAIS SANS S'Y LIMITER, LA PERTE DE BÉNÉFICES, L'INTERRUPTION D'ACTIVITÉ, LA PERTE D'INFORMATIONS COMMERCIALES, OU TOUTE AUTRE PERTE FINANCIÈRE, DÉCOULANT DE L'UTILISATION DU LOGICIEL OU DE L'INCAPACITÉ À UTILISER LE LOGICIEL, MÊME SI DELL OU SON REVENDUEUR ONT ÉTÉ INFORMÉS DE LA POSSIBILITÉ DE TELS DOMMAGES. Certaines législations n'autorisent pas la limitation ou l'exclusion de responsabilité pour des préjudices accessoires ou indirects, auquel cas l'exclusion ou la limitation qui précède ne vous sera pas applicable.

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 LIBRE EST DISTRIBUÉ DANS L'ESPOIR QU'IL SERA UTILISÉ, MAIS IL EST FOURNI « EN L'ÉTAT », SANS AUCUNE GARANTIE DE QUELQUE NATURE QUE CE SOIT, EXPRESSE OU IMPLICITE, Y COMPRIS, MAIS SANS S'Y LIMITER, LES GARANTIES IMPLICITES DE COMMERCIALITÉ ET DE LA CONFORMITÉ À UNE UTILISATION PARTICULIÈRE. EN AUCUN CAS, DELL, LES TITULAIRES DES DROITS D'AUTEUR OU TOUTE PARTIE AYANT CONTRIBUÉ À CE LOGICIEL NE POURRONT ÊTRE TENUS POUR RESPONSABLES DES DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, SPÉCIAUX, EXEMPLAIRES OU CONSÉCUTIFS (Y COMPRIS MAIS SANS S'Y LIMITER, LA MISE À DISPOSITION DE BIENS OU DE SERVICES DE SUBSTITUTION, LA PERTE DE BÉNÉFICES, REVENUS, DONNÉES OU UTILITÉ OU L'INTERRUPTION D'UNE ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA RESPONSABILITÉ (CONTRACTUELLE, RESPONSABILITÉ STRICTE OU DÉLIT CIVIL (Y COMPRIS LA NÉGLIGENCE OU TOUTE AUTRE CAUSE)), RÉSULTANT DE L'UTILISATION DU LOGICIEL, ET CE MÊME SI DELL, LES TITULAIRES DES DROITS D'AUTEUR OU TOUTE PARTIE AYANT CONTRIBUÉ À CE LOGICIEL ONT ÉTÉ INFORMÉS DE LA POSSIBILITÉ DE TELS DOMMAGES.

DROITS LIMITÉS PAR LE GOUVERNEMENT DES ÉTATS-UNIS

Le Logiciel est un « article de commerce », tel que défini par l'article 48 C.F.R. 2.101 (Oct. 1995), consistant en un « logiciel d'ordinateur du commerce » et une « documentation de logiciel d'ordinateur du commerce », termes devant être compris dans leur acception utilisée à l'article 48 C.F.R. 12.212. En accord avec les articles 48 C.F.R. 12.212 et 48 C.F.R. 227.7202-1 à 227.7202-4, tous les utilisateurs du gouvernement américain acquièrent le Logiciel et la documentation dans la limite des droits énoncés par les présentes. Fournisseur/Éditeur du logiciel: Dell Products, L.P., One Dell Way, Round Rock, Texas 78682.

CONSIGNES GÉNÉRALES

Ce contrat est valide jusqu'à expiration. Il sera résilié uniquement conformément aux conditions décrites ci-dessus, ou en cas de non-respect par l'utilisateur de l'une quelconque des clauses décrites. Une fois ce contrat arrivé à expiration, vous acceptez que le Logiciel et tout matériel l'accompagnant, ainsi que toutes les copies de ces éléments, doivent être détruits. Ce contrat est régi par les lois de l'état du Texas. Les dispositions du présent contrat sont juridiquement indépendantes les unes des autres. Le fait que l'une de ces dispositions se révèle non applicable n'altère en rien le caractère légal et obligatoire des autres dispositions, termes ou conditions du présent contrat. Le présent contrat lie également les successeurs et ayant-droits de l'utilisateur. Les parties renoncent expressément à tout droit de jugement par un jury des éventuels litiges liés au Logiciel ou au présent contrat. Cette dérogation n'étant pas valide dans certaines juridictions, il est possible qu'elle ne s'applique pas dans votre cas. Vous reconnaissez avoir lu et compris le présent contrat et en acceptez les termes et confirmez qu'il constitue le seul accord complet et exclusif entre vous et Dell concernant le Logiciel.

[Retour à la page Contenu](#)

[Retour à la page Contenu](#)

Utilisation du module iKVM

Micrologiciel Dell Chassis Management Controller Version 3.1 Guide d'utilisation

- [Présentation](#)
 - [Interfaces de connexion physique](#)
 - [Utilisation d'OSCAR](#)
 - [Gestion de serveurs avec iKVM](#)
 - [Gestion d'iKVM depuis CMC](#)
 - [Dépannage](#)
-

Présentation

Le module KVM d'accès local destiné à votre châssis de serveur Dell M1000e est appelé Avocent Integrated KVM Switch Module, ou iKVM. iKVM est un commutateur clavier, vidéo et souris analogique qui se branche sur votre châssis. Ce module de châssis enfichable à chaud en option offre un accès clavier, souris et vidéo local aux serveurs du châssis et à la ligne de commande du contrôleur CMC actif.

Interface utilisateur d'iKVM

iKVM utilise l'interface graphique utilisateur OSCAR (On Screen Configuration and Reporting/génération de rapports et configuration à l'écran), activée par un raccourci clavier. OSCAR vous permet de sélectionner un des serveurs ou la ligne de commande Dell CMC auquel vous souhaitez accéder avec le clavier, l'affichage et la souris locaux.

Une seule session iKVM par châssis est autorisée.

Sécurité

L'interface utilisateur OSCAR vous permet de protéger votre système avec un mot de passe d'économiseur d'écran. Après un temps défini par l'utilisateur, le mode économiseur d'écran s'active et l'accès est interdit jusqu'à ce que le mot de passe approprié soit saisi pour réactiver OSCAR.

Balayage

OSCAR vous permet de sélectionner une liste de serveurs qui sont affichés dans l'ordre sélectionné lorsque OSCAR est en mode de balayage.

Identification des serveurs

CMC attribue des noms de logements à tous les serveurs du châssis. Bien que vous puissiez attribuer des noms aux serveurs à l'aide de l'interface OSCAR depuis une connexion à plusieurs couches, les noms attribués par CMC sont prioritaires et tous les nouveaux noms que vous attribuez aux serveurs à l'aide d'OSCAR sont écrasés.

CMC identifie un logement en lui attribuant un nom unique. Pour changer les noms des logements à l'aide de l'interface Web CMC, voir [Modification du nom d'un logement](#). Pour changer le nom d'un logement avec RACADM, consultez la section `setslotname` dans le *Guide de référence de la ligne de commande pour iDRAC6 et CMC*.

Vidéo

Les connexions vidéo d'iKVM prennent en charge les résolutions d'affichage vidéo comprises entre 640 x 480 à 60 Hz et 1280 x 1024 à 60 Hz.

Plug and Play

iKVM prend en charge Plug and Play du canal d'affichage des données (DDC), qui automatise la configuration du moniteur vidéo, et est conforme à la norme VESA DDC2B.

Évolutif FLASH

Vous pouvez mettre à jour le micrologiciel iKVM à l'aide de l'interface Web de CMC ou de la commande `fwupdate` RACADM. Pour plus d'informations, voir [Gestion d'iKVM depuis CMC](#).

Interfaces de connexion physique

Vous pouvez vous connecter à un serveur ou à la console de l'interface de ligne de commande de CMC via iKVM depuis le panneau avant du châssis, une interface de console analogique (ACI) et le panneau arrière du châssis.

 **REMARQUE** : les ports du panneau de configuration avant du châssis sont conçus spécifiquement pour iKVM, qui en option. Si vous ne possédez pas iKVM, vous ne pouvez pas utiliser les ports du panneau de configuration avant.

Priorités de connexion d'iKVM

Une seule connexion iKVM est disponible à la fois. iKVM attribue un ordre de priorité à chaque type de connexion afin qu'en présence de plusieurs connexions, une seule connexion soit disponible tandis 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 les connexions d'iKVM sont situées sur le panneau avant et sur l'ACI, la connexion du panneau avant reste active tandis que la connexion de l'ACI est désactivée. En cas de connexions de l'ACI et du panneau arrière, la connexion de l'ACI devient prioritaire.

Affectation de plusieurs couches via la connexion de l'ACI

iKVM autorise les connexions auxquelles sont affectées plusieurs couches avec les serveurs et la console de ligne de commande CMC d'iKVM, soit en local via un port Remote Console Switch, soit à distance via le logiciel Dell RCS. Module iKVM prend en charge les connexions de l'ACI depuis les produits suivants :

- 1 180AS, 2160AS, 2161DS*, 2161DS-2 ou 4161DS Dell Remote Console Switches
- 1 Système de commutation Avocent AutoView
- 1 Système de commutation Avocent DSR
- 1 Système de commutation Avocent AMX

* Ne prend pas en charge la connexion de la console Dell CMC.

 **REMARQUE** : iKVM prend également en charge une connexion de l'ACI vers les Dell 180ES et 2160ES, mais l'affectation de plusieurs couches ne se fait pas de façon transparente. Cette connexion exige un SIP USB vers PS2.

Utilisation d'OSCAR

Cette section offre une présentation de l'interface OSCAR.

Notions de base sur la navigation

Tableau 10-1. Navigation dans OSCAR avec le clavier et la souris

Touche ou séquence de touches	Résultat
1 <Impr. écran>-<Impr. écran>	N'importe laquelle de ces séquences de touches peut ouvrir OSCAR en fonction de vos paramètres Invoquer OSCAR . Vous pouvez activer deux, trois ou l'intégralité de ces séquences de touches en cochant des cases dans la section Invoquer OSCAR de la boîte de dialogue Menu principal , puis en cliquant sur OK .
1 <Maj>-<Maj>	
1 <Alt>-<Alt>	
1 <Ctrl>-<Ctrl>	
<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 le bouton OK , puis retourne à la boîte de dialogue précédente.
<Entrée>	Termine une opération de commutateur dans la boîte de dialogue Menu principal et quitte OSCAR.
Simple clic, <Entrée>	Dans une zone de texte, sélectionne le texte à modifier et permet à la touche fléchée gauche et à la touche fléchée droite de déplacer le curseur. Appuyez à nouveau sur <Entrée> pour quitter le mode de modification.
<Impr. écran>, <Retour>	Revient à la sélection précédente en l'absence d'autres séquences de touches.
<Impr. écran>, <Alt>+<O>	Déconnecte immédiatement un utilisateur d'un serveur ; aucun serveur n'est sélectionné. L'indicateur de condition affiche Disponible. (Cette action s'applique uniquement au =<O> du clavier et non à celui 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 Num>	Désactivé. Pour changer la casse, utilisez la touche <Maj>.

Configuration de l'OSCAR

Tableau 10-2. Fonctions du menu Configuration d'OSCAR

Fonctionnalité	Rôle
Menu	Change la liste des serveurs soit numériquement par logement, soit alphabétiquement par nom.
Sécurité	<ul style="list-style-type: none"> 1 Définit un mot de passe pour restreindre l'accès aux serveurs. 1 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.
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.

Pour accéder à la boîte de dialogue **Configuration** :

1. Appuyez sur la touche <Impr écran> pour lancer l'interface OSCAR. La boîte de dialogue **Menu principal** s'affiche.
2. Cliquez sur **Configuration**. La boîte de dialogue **Configuration** apparaît.

Modification du comportement d'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 accéder à la boîte de dialogue **Menu** :

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.

Pour choisir l'ordre d'affichage par défaut des serveurs dans la boîte de dialogue **Menu principal** :

1. Sélectionnez **Nom** pour afficher les serveurs par nom, dans l'ordre alphabétique.

ou

Sélectionnez **Logement** pour afficher les serveurs par numéro de logement.

2. Cliquez sur **OK**.

Pour attribuer une ou plusieurs séquences de touches pour l'activation de l'OSCAR :

1. Sélectionnez une séquence de touches dans le menu **Invoquer OSCAR**.
2. Cliquez sur **OK**.

La touche par défaut d'invocation de l'OSCAR est <Impr. écran>.

Pour définir un temps de retard d'affichage de l'écran pour OSCAR :

1. Entrez le nombre de secondes (de 0 à 9) pour retarder l'affichage de l'OSCAR après avoir appuyé sur <Impr. écran>. Entrez <0> pour lancer OSCAR immédiatement.
2. Cliquez sur **OK**.

Le paramétrage d'un temps de retard d'affichage de l'OSCAR vous permet de terminer une commutation logicielle. Pour procéder à une commutation logicielle, voir [Commutation logicielle](#).

Contrôle de l'indicateur de condition

L'indicateur de condition s'affiche sur votre bureau de travail 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 changer la couleur, l'opacité, le temps d'affichage et l'emplacement de l'indicateur sur le bureau.

Tableau 10-3. Indicateurs de condition d'OSCAR

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 accéder à la boîte de dialogue **Indicateur** :

1. Appuyez sur <Impr. écran>. La boîte de dialogue **Menu principal** s'affiche.
2. Cliquez sur **Configuration**, puis sur **Indicateur**. La boîte de dialogue **Indicateur** apparaît.

Pour spécifier le mode d'affichage de l'indicateur de condition :

1. 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.

2. Sélectionnez une couleur d'indicateur dans la section **Couleur d'affichage**. Les options disponibles sont le noir, le rouge, le bleu et le violet.
3. Dans **Mode d'affichage**, sélectionnez **Opaque** pour obtenir un indicateur de couleur opaque ou **Transparent** pour voir le bureau à travers l'indicateur.
4. Pour positionner l'indicateur de condition sur le bureau :
 - a. Cliquez sur **Définir la position**. L'**indicateur de définition de position** apparaît.
 - b. Cliquez avec le bouton gauche sur la barre de titre et faites-la glisser vers l'emplacement souhaité sur le bureau.
 - c. Cliquez avec le bouton droit pour retourner à la boîte de dialogue **Indicateur**.

 **REMARQUE** : les modifications apportées à la position de l'indicateur ne sont pas enregistrées tant que vous ne cliquez pas sur **OK** dans la boîte de dialogue **Indicateur**.

5. Cliquez sur **OK** pour enregistrer les paramètres.

Pour quitter sans enregistrer les modifications, cliquez sur .

Gestion de serveurs avec iKVM

iKVM est une matrice de commutateur analogique prenant en charge jusqu'à 16 serveurs. Le commutateur iKVM utilise l'interface utilisateur OSCAR pour sélectionner et configurer vos serveurs. iKVM inclut en outre une entrée système pour établir une connexion de console de ligne de commande CMC avec CMC.

Compatibilité des périphériques et prise en charge

iKVM est compatible avec les périphériques suivants :

- 1 Claviers USB PC standard avec dispositions QWERTY, QWERTZ, AZERTY et Japonais 109.
- 1 Moniteurs VGA avec prise en charge DDC.
- 1 Périphériques de pointage USB standard.
- 1 Concentrateurs USB 1.1 auto-alimentés connectés au port USB local sur iKVM.
- 1 Concentrateurs USB 2.0 alimentés connectés à la console du panneau avant du châssis Dell M1000e.

 **REMARQUE** : vous pouvez utiliser plusieurs claviers et plusieurs souris sur le port USB local d'iKVM. iKVM rassemble les signaux d'entrée. Si des signaux d'entrée simultanés sont émis par plusieurs claviers ou souris USB, des résultats imprévisibles peuvent se produire.

 **REMARQUE** : les connexions USB sont destinées uniquement aux claviers, souris et concentrateurs USB pris en charge. iKVM ne prend pas en charge les données transmises par d'autres périphériques USB.

Affichage et sélection de serveurs

Utilisez la boîte de dialogue **Menu principal** de l'OSCAR pour afficher, configurer et gérer des serveurs via iKVM. Vous pouvez afficher vos serveurs par nom ou par logement. ce dernier correspondant au numéro du logement occupé par le serveur dans le châssis. Ce numéro est indiqué dans la colonne **Logement**.

 **REMARQUE** : la ligne de commande Dell CMC occupe le logement 17. La sélection de ce logement permet d'afficher la ligne de commande CMC, à partir de laquelle vous pouvez exécuter les commandes RACADM ou vous connecter à la console série du serveur ou des modules d'E/S.

 **REMARQUE** : le nom des serveurs et les numéros de logements sont attribués par le contrôleur CMC.

Pour accéder à la boîte de dialogue **Menu principal**, procédez comme suit :

Appuyez sur la touche <Impr écran> pour lancer l'interface OSCAR. La boîte de dialogue **Menu principal** s'affiche.

ou

Si un mot de passe est défini, la boîte de dialogue **Mot de passe** s'affiche. Entrez votre mot de passe et cliquez sur **OK**. La boîte de dialogue **Menu principal** s'affiche.

Pour plus d'informations sur la définition d'un mot de passe, voir [Paramétrage de la sécurité de la console](#).

 **REMARQUE** : quatre options sont disponibles pour invoquer OSCAR. Vous pouvez activer une, plusieurs ou l'intégralité de ces séquences de touches en cochant des cases dans la section **Invoquer OSCAR** de la boîte de dialogue **Menu principal**, puis en cliquant sur **OK**.

Affichage de la condition de vos serveurs

La condition des serveurs dans votre châssis est indiquée dans les colonnes de droite de la boîte de dialogue **Menu principal**. Le tableau suivant décrit les symboles de condition.

Tableau 10-4. Symboles de condition de l'interface OSCAR

Symboles	Description
	(Point vert.) Le serveur est en ligne.
	(X rouge.) Le serveur est hors ligne ou absent du châssis.
	(Point jaune.) Le serveur n'est pas disponible.
	(A ou B vert.) Le canal utilisateur indiqué par la lettre (A=panneau arrière, B=panneau avant) accède au serveur.

Sélection des serveurs

Utilisez la boîte de dialogue **Menu principal** pour sélectionner des serveurs. Lorsque vous sélectionnez un serveur, iKVM reconfigure le clavier et la souris sur les paramètres appropriés pour ce serveur.

- 1 Pour sélectionner des serveurs :

Double-cliquez sur le nom de serveur ou le numéro de logement.

ou

Si l'ordre d'affichage de votre liste de serveurs est défini par logement (à savoir, le bouton **Logement** est enfoncé), tapez le numéro de logement et appuyez sur <Entrée>.

ou

Si l'ordre d'affichage de votre liste de serveurs est défini par nom (à savoir, le bouton **Nom** est enfoncé), tapez les premiers caractères du nom du serveur, établissez-le comme nom unique et appuyez à deux reprises sur <Entrée>.

- 1 Pour sélectionner le serveur précédent :

Appuyez sur <Impr. écran>, puis sur <Retour>. Cette combinaison de touches alterne entre les connexions précédentes et actuelles.

- 1 Pour déconnecter l'utilisateur d'un serveur :

Appuyez sur <Impr. écran> pour accéder à OSCAR, puis cliquez sur **Déconnecter**.

ou

Appuyez sur <Impr. écran>, puis sur <Alt><0>. L'état devient disponible, sans serveur sélectionné. L'indicateur de condition sur votre bureau, s'il est actif, affiche Disponible. Voir [Contrôle de l'indicateur de condition](#).

Commutation logicielle

La commutation logicielle consiste à commuter entre les serveurs à l'aide d'une séquence de touches rapides. Pour basculer vers un serveur de cette manière, appuyez sur <Impr. écran>, puis tapez les premiers caractères de son nom ou de son numéro. Si vous avez défini précédemment un **temps de retard** (le nombre de secondes avant l'affichage de la boîte de dialogue **Menu principal** une fois que <Impr. écran> a été enfoncé) et que vous appuyez sur les séquences de touches avant que ce temps ne soit écoulé, l'interface OSCAR ne s'affiche pas.

Pour configurer OSCAR pour la commutation logicielle :

1. Appuyez sur la touche <Impr écran> pour lancer l'interface OSCAR. La boîte de dialogue **Menu principal** s'affiche.
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 retard souhaité en secondes dans le champ **Temps de retard d'affichage de l'écran**.
5. Cliquez sur **OK**.

Pour effectuer une commutation logicielle vers un serveur :

- 1 Pour sélectionner un serveur, appuyez sur <Impr. écran>.

Si l'ordre d'affichage de votre liste de serveurs est défini par logement conformément à votre sélection à l'étape 3 (à savoir, le bouton **Logement** est enfoncé), tapez le numéro de logement et appuyez sur <Entrée>.

ou

Si l'ordre d'affichage de votre liste de serveurs est défini par nom conformément à votre sélection à l'étape 3 (à savoir, le bouton **Nom** est enfoncé), tapez les premiers caractères du nom du serveur pour l'établir comme nom unique et appuyez sur <Entrée>.

- 1 Pour retourner au serveur précédent, appuyez sur <Impr. écran>, puis sur <Retour>.

Connexions vidéo

iKVM ne comporte aucune connexion vidéo sur les panneaux avant et arrière du châssis. Les signaux de connexion du panneau avant sont prioritaires sur ceux du panneau arrière. Lorsqu'un moniteur est connecté au panneau avant, la connexion vidéo n'aboutit pas au panneau arrière et un message de l'OSCAR indique que les connexions KVM et ACI du panneau arrière sont désactivées. Si le moniteur est désactivé (à savoir, retiré du panneau avant ou désactivé par une commande CMC), la connexion ACI devient active tandis que la connexion KVM du panneau arrière reste désactivée. (Pour plus d'informations sur l'ordre de priorité des connexions, voir [Priorités de connexion d'iKVM](#).)

Pour plus d'informations sur l'activation ou la désactivation de la connexion du panneau avant, voir [Activation ou désactivation du 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 la console d'interface utilisateur d'iDRAC ont tous deux accès à la console et peuvent effectuer une saisie simultanément.

Pour empêcher que ce scénario ne se produise, l'utilisateur distant, avant de lancer la redirection de console d'interface utilisateur d'iDRAC, peut désactiver la console locale dans l'interface Web d'iDRAC. L'utilisateur local d'iKVM voit un message OSCAR indiquant que la connexion sera préemptée dans un délai spécifié. L'utilisateur local doit terminer son travail avant que la connexion d'iKVM au serveur ne soit terminée.

Aucune fonction de préemption n'est disponible pour l'utilisateur iKVM.

 **REMARQUE** : si un utilisateur distant iDRAC a désactivé la vidéo locale pour un serveur spécifique, la vidéo, le clavier et la souris de ce serveur ne seront pas disponibles pour iKVM. L'état du serveur est marqué d'un point jaune dans le menu OSCAR pour indiquer qu'il est verrouillé ou non disponible pour un usage local (voir [Affichage de la condition de vos serveurs](#)).

Paramétrage de la sécurité de la console

OSCAR vous permet de configurer les paramètres de sécurité sur votre console iKVM. Vous pouvez établir un mode économiseur d'écran qui s'active lorsque votre console reste inutilisée pendant un délai spécifié. Une fois ce mode activé, votre console demeure verrouillée jusqu'à ce que vous appuyiez sur une touche quelconque ou déplaçiez le curseur. Entrez le mot de passe d'activation de l'économiseur d'écran pour continuer.

Utilisez la boîte de dialogue **Sécurité** pour verrouiller votre console en instaurant une protection par mot de passe, définir ou changer votre mot de passe, ou 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. Voir [Suppression d'un mot de passe perdu ou oublié](#).

Accès à la boîte de dialogue Sécurité

1. Appuyez sur <Impr. écran>. La boîte de dialogue **Menu principal** s'affiche.
2. Cliquez sur **Configuration** et sur **Sécurité**. La boîte de dialogue **Sécurité** apparaît.

Paramétrage ou modification du mot de passe

1. Cliquez une fois et appuyez sur <Entrée>, ou double-cliquez dans le champ **Nouveau**.
2. Tapez le nouveau mot de passe dans le champ **Nouveau** et appuyez sur <Entrée>. Les mots de passe sont sensibles à la casse et comprennent 5 à 12 caractères. Ils doivent inclure au moins une lettre et un chiffre. Les caractères autorisés sont : 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** si vous souhaitez uniquement changer votre mot de passe, puis fermez la boîte de dialogue.

Protection de votre console par mot de passe

1. Paramétrez votre mot de passe comme indiqué dans la procédure précédente.
2. Cochez la case **Activer l'économiseur d'écran**.
3. Entrez le nombre de minutes de **temps d'inactivité** (entre 1 et 99) nécessaires à l'activation de la protection par mot de passe et de l'économiseur d'écran.
4. Pour **Mode** : si votre moniteur est compatible ENERGY STAR, sélectionnez **Energy** ; sinon, sélectionnez **Écran**.

 **REMARQUE** : si le mode est défini sur **Energy**, l'appareil place le moniteur en mode veille. Ceci est normalement indiqué par la mise hors tension du moniteur et par une lumière orange qui remplace la LED d'alimentation verte. Si le mode est défini sur **Écran**, l'indicateur OSCAR rebondit sur l'écran pendant toute la durée du test. Avant que le test ne commence, une boîte contextuelle d'avertissement affiche le message suivant : « Le mode Energy peut endommager un moniteur qui n'est pas compatible ENERGY STAR. Une fois démarré, le test peut toutefois être quitté immédiatement au moyen de la souris ou du clavier ».

 **PRÉCAUTION** : le moniteur peut être endommagé s'il est utilisé en mode Energy alors qu'il n'est pas conforme à la norme Energy Star.

5. **Facultatif** : pour activer le test d'économiseur d'écran, cliquez sur **Test**. La boîte de dialogue **Test d'économiseur d'écran** apparaît. Cliquez sur **OK** pour lancer le test.

Le test dure 10 secondes. Lorsqu'il se termine, la boîte de dialogue **Sécurité** réapparaît.

Ouverture de session

1. Appuyez sur <Impr. écran> pour lancer OSCAR. La boîte de dialogue **Mot de passe** apparaît.
2. Tapez votre mot de passe, puis cliquez sur **OK**. La boîte de dialogue **Menu principal** apparaît.

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 durée 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 votre 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** si vous souhaitez uniquement supprimer votre mot de passe.

Activation du mode économiseur d'écran sans protection par mot de passe

 **REMARQUE** : si votre console est protégée par mot de passe, vous devez d'abord supprimer cette protection. Suivez les étapes de la procédure précédente avant de procéder comme suit .

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 alors qu'il n'est pas conforme à la norme Energy Star.

4. Facultatif : pour activer le test d'économiseur d'écran, cliquez sur **Test**. La boîte de dialogue **Test d'économiseur d'écran** apparaît. Cliquez sur **OK** pour lancer le test.

Le test dure 10 secondes. Lorsqu'il se termine, la boîte de dialogue **Sécurité** réapparaît.

 **REMARQUE** : l'activation du mode économiseur d'écran déconnecte l'utilisateur d'un serveur ; aucun serveur n'est sélectionné. L'indicateur de condition affiche Disponible.

Quitter le mode économiseur d'écran

Pour quitter le mode économiseur d'écran et retourner à la boîte de dialogue **Menu principal**, appuyez sur une touche quelconque ou déplacez votre souris.

Pour désactiver l'économiseur d'écran :

1. Dans la boîte de dialogue **Sécurité**, décochez la case **Activer l'économiseur d'écran**.
2. 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 le mot de passe d'iKVM est perdu ou oublié, vous pouvez le réinitialiser sur les paramètres par défaut d'iKVM, puis changer le mot de passe. Vous pouvez réinitialiser le mot de passe avec l'interface Web de CMC ou RACADM.

Pour réinitialiser un mot de passe perdu ou oublié d'iKVM avec l'interface Web de CMC :

1. Ouvrez une session sur l'interface Web de CMC.
2. Sélectionnez **iKVM** dans le sous-menu **Châssis**.
3. Cliquez sur l'onglet **Configuration**. La page **Configuration d'iKVM** s'affiche.
4. Cliquez sur **Restaurer les valeurs par défaut**.

Vous pouvez ensuite changer le mot de passe par défaut via OSCAR. Voir [Paramétrage ou modification 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 tapez :

```
racadm racresetcfg -m kvm
```



REMARQUE : l'utilisation de la commande `racresetcfg` entraîne la réinitialisation des 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 la section `racresetcfg` du *Guide de référence de la ligne de commande pour iDRAC6 et CMC*.

Modification de la langue

Utilisez la boîte de dialogue **Langue** pour afficher le texte de l'OSCAR dans l'une des langues prises en charge. Le texte est immédiatement affiché dans la langue sélectionnée sur tous les écrans de l'OSCAR.

Pour changer la langue de l'OSCAR :

1. Appuyez sur <Impr. écran>. La boîte de dialogue **Menu principal** s'affiche.
2. Cliquez sur **Configuration**, puis sur **Langue**. La boîte de dialogue **Langue** apparaît.
3. Cliquez sur le bouton d'option correspondant à la langue souhaitée, puis 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** apparaît.
La moitié supérieure de la boîte de dialogue **Version** répertorie les versions des sous-systèmes de l'appareil.
3. Cliquez sur ou appuyez sur <Échap> pour fermer la boîte de dialogue **Version**.

Balayage de votre système

En mode de balayage, iKVM balaye automatiquement de logement en logement (de serveur en serveur). Vous pouvez balayer jusqu'à 16 serveurs en spécifiant les serveurs que vous souhaitez balayer et le nombre de secondes pendant lesquelles chaque serveur est affiché.

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** apparaît, répertoriant tous les serveurs du châssis.

3. Cochez la case en regard des serveurs que vous souhaitez balayer.

ou

Double-cliquez sur le nom ou le logement du serveur.

ou

Appuyez sur <Alt > et le numéro du serveur que vous souhaitez 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 le bouton **Ajouter/Supprimer**, puis cliquez sur **OK**.

Pour supprimer un serveur de la liste **Balayage** :

1. Dans la boîte de dialogue **Balayage**, cochez la case située en regard du serveur à supprimer.

ou

Double-cliquez sur le nom ou le logement du serveur.

ou

Cliquez sur le bouton **Effacer** pour supprimer tous les serveurs de la liste **Balayage**.

2. Cliquez sur le bouton **Ajouter/Supprimer**, puis cliquez sur **OK**.

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 **Commandes** apparaît.
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 pour fermer la boîte du message.

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 n'est *pas* ouverte, déplacez la souris ou appuyez sur une touche quelconque du clavier. Le balayage s'arrête au serveur sélectionné.
ou
Appuyez sur <Impr. écran>. La boîte de dialogue **Menu principal** apparaît ; sélectionnez un serveur dans la liste.
2. Cliquez sur le bouton **Commandes**. La boîte de dialogue **Commandes** apparaît.
3. Décochez la case **Activation du balayage**.

Diffusion aux serveurs

Vous pouvez contrôler simultanément plusieurs serveurs dans le système pour vous assurer que tous les serveurs sélectionnés reçoivent une entrée identique. Vous pouvez choisir de diffuser des séquences de touches et/ou des déplacements de souris indépendamment.

 **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 **Diffuser** apparaît.

 **REMARQUE** : diffusion de séquences de touches : lorsque vous utilisez des séquences de touches, l'état du clavier doit être identique pour tous les serveurs recevant une diffusion afin que les séquences de touches puissent être interprétées à l'identique. Plus spécifiquement, les modes <Verr Maj> et <Verr Num> doivent être les mêmes sur tous les claviers. Lorsqu'iKVM tente d'envoyer simultanément des séquences de touches aux serveurs sélectionnés, certains serveurs peuvent gêner et ainsi retarder la transmission.

 **REMARQUE** : diffusion des déplacements de la souris : pour garantir la précision de fonctionnement de la souris, tous les serveurs doivent avoir des pilotes de souris, des bureaux (icônes placées à l'identique, par exemple) et des résolutions vidéo identiques. La souris doit également se trouver exactement à la même place sur tous les écrans. Ces conditions étant extrêmement difficiles à remplir, la diffusion des déplacements de la souris à plusieurs serveurs peut générer des résultats imprévisibles.

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 fléchées haut ou bas pour déplacer le curseur vers un serveur cible. Appuyez ensuite sur <Alt><K> pour sélectionner la case du clavier et/ou sur <Alt><M> pour sélectionner la case de la souris. Répétez cette procédure pour des serveurs supplémentaires.

4. Cliquez sur **OK** pour enregistrer les paramètres et retourner à la boîte de dialogue **Configuration**. Cliquez sur  ou appuyez sur <Échap> pour retourner à la boîte de dialogue **Menu principal**.

5. Cliquez sur **Commandes**. La boîte de dialogue **Commandes** apparaît.

6. Cochez la case **Activation de la diffusion** pour activer la diffusion. La boîte de dialogue **Avertissement de diffusion** apparaît.

7. Cliquez sur **OK** pour activer la diffusion.

Pour annuler et retourner à la boîte de dialogue **Commandes**, cliquez sur  ou appuyez sur <Échap>.

8. Si la diffusion est activée, tapez les informations et/ou exécutez les déplacements de la souris que vous souhaitez diffuser depuis la station de gestion. Seuls les serveurs de la liste sont accessibles.

Pour désactiver la diffusion :

Dans la boîte de dialogue **Commandes**, décochez la case **Activation de la diffusion**.

Gestion d'iKVM depuis CMC

Activation ou désactivation du panneau avant

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 tapez :

```
racadm config -g cfgKVMInfo -o cfgKVMFrontPanelEnable <valeur>
```

où <valeur > correspond à 1 (activé) ou à 0 (désactivé).

Pour des informations supplémentaires sur la sous-commande **config**, voir la section de la commande config du *Guide de référence de la ligne de commande pour iDRAC6 et CMC*.

Pour activer ou désactiver l'accès à iKVM depuis le panneau avant à l'aide de l'interface Web :

1. Ouvrez une session sur l'interface Web de CMC.
2. Sélectionnez iKVM dans l'arborescence du système. La page **État du module iKVM** s'affiche.
3. Cliquez sur l'onglet **Configuration**. La page **Configuration d'iKVM** s'affiche.
4. Pour activer, cochez la case **USB/Vidéo du panneau avant activé**.
Pour désactiver, décochez la case **USB/Vidéo du panneau avant activé**.
5. Cliquez sur **Appliquer** pour enregistrer le paramètre.

Activation de la console Dell CMC via iKVM

Pour permettre à iKVM d'accéder à la console Dell CMC à l'aide de RACADM, ouvrez une console texte série/Telnet/SSH vers CMC, ouvrez une session et tapez :

```
racadm config -g cfgKVMInfo -o cfgKVMAccessToCMCEnable 1
```

Pour activer la console Dell CMC avec l'interface Web :

1. Ouvrez une session sur l'interface Web de CMC.
2. Sélectionnez iKVM dans l'arborescence du système. La page **État du module iKVM** s'affiche.
3. Cliquez sur l'onglet **Configuration**. La page **Configuration d'iKVM** s'affiche.
4. Cochez la case **Autoriser l'accès à l'interface de ligne de commande CMC depuis iKVM**.
5. Cliquez sur **Appliquer** pour enregistrer le paramètre.

Affichage de la condition et des propriétés d'iKVM

Le module KVM d'accès local destiné à votre châssis de serveur Dell M1000e est appelé Avocent Integrated KVM Switch Module, ou iKVM. La condition d'intégrité de l'iKVM associé au châssis peut être consultée sur la page **Intégrité des propriétés du châssis** de la section **Graphiques du châssis**.

Pour consulter la condition d'intégrité de l'iKVM à l'aide de **Graphiques du châssis** :

1. Ouvrez une session sur l'interface Web de CMC.
2. La page **Condition du châssis** s'affiche. La section de droite de la page **Graphiques du châssis** fournit une vue arrière du châssis et contient la condition d'intégrité d'iKVM. La condition d'intégrité d'iKVM est indiquée par la couleur du sous-graphique d'iKVM :
 - 1 Vert : iKVM est présent, sous tension et communique avec CMC ; il n'y a aucune indication d'événement indésirable.
 - 1 Orange : iKVM est présent, mais peut être hors tension, ou ne pas communiquer avec CMC ; un événement indésirable peut exister.
 - 1 Gris : iKVM est présent et est hors tension. Il ne communique pas avec CMC et il n'y a aucune indication d'événement indésirable.
3. Placez le curseur sur le sous-graphique de l'iKVM pour afficher le texte du champ ou l'infobulle correspondants. Le texte du champ fournit des informations complémentaires sur cet iKVM.
4. Le lien hypertexte du sous-graphique de l'iKVM permet d'accéder à l'interface graphique CMC correspondante fournissant une navigation directe vers la page **Condition d'iKVM**.

Pour plus d'informations sur iKVM, voir [Utilisation du module iKVM](#).

Pour consulter la condition d'iKVM à l'aide de la page **Condition d'iKVM** :

1. Ouvrez une session sur l'interface Web de CMC.
2. Sélectionnez **iKVM** dans l'arborescence du système. La page **Condition d'iKVM** s'affiche.

Tableau 10-5. Informations sur la condition d'iKVM

Élément	Description
Présence	Indique si le module iKVM est présent ou absent .
État de l'alimentation	Indique la condition de l'alimentation d'iKVM : sous tension , hors tension ou - (absente).
Nom	Affiche le nom de produit d'iKVM.
Fabricant	Affiche le fabricant d'iKVM.
Numéro de pièce	Affiche le numéro de pièce d'iKVM. Le numéro de pièce est un identificateur unique fourni par le fournisseur.
Version du micrologiciel	Indique la version du micrologiciel iKVM.
Version du matériel	Indique la version du micrologiciel iKVM.
Panneau avant connecté	Indique si le moniteur est connecté au connecteur VGA du panneau avant (Oui ou Non). Ces informations sont fournies à CMC afin qu'il puisse déterminer si un utilisateur local a accès au châssis via le panneau avant.
Panneau arrière connecté	Indique si le moniteur est connecté au connecteur VGA du panneau arrière (Oui ou Non). Ces informations sont fournies à CMC afin qu'il puisse déterminer si un utilisateur local a accès au châssis via le panneau arrière.
Port cascade connecté	iKVM prend en charge l'affectation de plusieurs couches de façon transparente avec les dispositifs KVM externes de Dell et d'Avocent à l'aide du matériel intégré. Lorsque plusieurs couches sont affectées à iKVM, les serveurs du châssis sont accessibles à partir de l'écran du commutateur KVM externe à partir duquel plusieurs couches sont affectées à iKVM.
USB/Vidéo du panneau avant activés	Affiche si le connecteur VGA du panneau avant est activé (Oui ou Non).
Autoriser l'accès CMC à partir d'iKVM	Indique si la console de commande CMC accessible via iKVM est activée (Oui ou Non).

Mise à jour du micrologiciel du module iKVM

Vous pouvez mettre à jour le micrologiciel iKVM avec l'interface Web de CMC ou RACADM.

Pour mettre à jour le micrologiciel iKVM avec l'interface Web de CMC :

1. Ouvrez une session sur l'interface Web de CMC.
2. Sélectionnez **Châssis** dans l'arborescence.
3. Cliquez sur l'onglet **Update** (Mise à jour). La page **Composants pouvant être mis à jour** s'affiche.
4. Cliquez sur le nom du module iKVM. La page **Mise à jour du micrologiciel** s'affiche.
5. Dans le champ **Image de micrologiciel**, entrez le chemin du fichier image du micrologiciel sur votre station de gestion ou votre réseau partagé ou cliquez sur **Parcourir** pour accéder à l'emplacement du fichier.

 **REMARQUE** : le nom de l'image par défaut du micrologiciel iKVM est **kvm.bin**. Cependant, vous pouvez modifier ce nom.

6. Cliquez sur **Commencer la mise à jour de micrologiciel**. Une boîte de dialogue vous demande de confirmer l'opération.
7. Cliquez sur **Yes (Oui)** pour continuer. La section **Avancement de la mise à jour du micrologiciel** fournit des informations sur l'état de la mise à jour du micrologiciel. Un indicateur d'état s'affiche sur la page pendant le chargement du fichier image. La durée du transfert de fichiers peut fortement varier en fonction de la vitesse de la connexion. Lorsque le processus de mise à jour interne démarre, la page s'actualise automatiquement et l'horloge de mise à jour du micrologiciel s'affiche. Instructions supplémentaires à suivre :
 - 1 N'utilisez pas le bouton **Actualiser** et ne naviguez pas sur une autre page pendant le transfert.
 - 1 Pour annuler le processus, cliquez sur **Annuler le transfert du fichier et la mise à jour**. Cette option n'est disponible que pendant le transfert du fichier.
 - 1 L'état de la mise à jour s'affiche dans le champ **État de mise à jour**. Ce champ est mis à jour automatiquement pendant le transfert du fichier. Certains anciens navigateurs ne prennent pas en charge ces mises à jour automatiques. Pour actualiser manuellement le champ **État de mise à jour**, cliquez sur **Actualiser**.

 **REMARQUE** : la mise à jour de l'iKVM peut prendre jusqu'à une minute.

À la fin de la mise à jour, iKVM est réinitialisé et le nouveau micrologiciel est mis à jour et apparaît sur la page **Composants actualisables**.

Pour mettre à jour le micrologiciel iKVM à l'aide de RACADM, ouvrez une console texte série/Telnet/SSH vers CMC, ouvrez une session et tapez :

```
racadm fwupdate -g -u -a <adresse IP ou FQND du serveur> -d <chemin de fichier/nom de fichier> -m kvm
```

Par exemple :

```
racadm fwupdate -gua 192.168.0.10 -d ikvm.bin -m kvm
```

Pour des informations supplémentaires sur la sous-commande **fwupdate**, voir la section de la commande **fwupdate** du *Guide de référence de la ligne de commande pour iDRAC6 et CMC*.

Dépannage

 **REMARQUE** : si une session de redirection de console est active et qu'un moniteur de plus faible résolution est connecté à iKVM, la résolution de console de serveur peut se réinitialiser si le serveur est sélectionné sur la console locale. Si le serveur exécute un système d'exploitation Linux, une console X11 peut ne pas être visible sur le moniteur local. Appuyez sur <Ctrl><Alt><F1> sur iKVM pour basculer Linux en mode console de texte.

Tableau 10-6. Dépannage d'iKVM

Problème	Cause probable et solution
Le message « L'utilisateur a été désactivé par le contrôle CMC » apparaît sur le moniteur connecté au panneau avant.	<p>La connexion du panneau avant a été désactivée par CMC.</p> <p>Vous pouvez activer le panneau avant avec l'interface Web de CMC ou RACADM.</p> <p>Pour activer le panneau avant avec l'interface Web :</p> <ol style="list-style-type: none">1. Ouvrez une session sur l'interface Web de CMC.2. Sélectionnez iKVM dans l'arborescence du système.3. Cliquez sur l'onglet Configuration.4. Cochez la case USB/Vidéo du panneau avant activé.5. Cliquez sur Appliquer pour enregistrer le paramètre. <p>Pour activer le panneau avant à l'aide de RACADM, ouvrez une console texte</p>

	<p>série/Telnet/SSH vers CMC, ouvrez une session et tapez :</p> <pre>racadm config -g cfgKVMInfo -o cfgKVMAccessToCMCEnable 1</pre>
L'accès au panneau arrière ne fonctionne pas.	<p>Le paramètre du panneau avant est activé par CMC et un moniteur est connecté au panneau avant.</p> <p>Une seule connexion est autorisée à la fois. La connexion du panneau avant est prioritaire sur l'ACI et le panneau arrière. Pour plus d'informations sur la priorité des connexions, voir Priorités de connexion d'iKVM.</p>
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.	<p>Un câble réseau est connecté au connecteur du port ACI d'iKVM et à un appareil KVM secondaire.</p> <p>Une seule connexion est autorisée à la fois. La connexion d'affectation de plusieurs couches ACI est prioritaire sur la connexion du moniteur sur le panneau arrière. L'ordre de priorité est le suivant : panneau avant, ACI, puis panneau arrière.</p>
La LED orange d'iKVM clignote.	<p>Trois causes sont possibles :</p> <p>iKVM présente un problème, qui nécessite sa reprogrammation. Pour corriger ce problème, suivez les instructions de mise à jour du micrologiciel d'iKVM (voir Mise à jour du micrologiciel du module iKVM).</p> <p>iKVM est en train de reprogrammer l'interface de la console CMC. Dans ce cas, la console CMC est temporairement indisponible et est représentée par un point jaune dans l'interface OSCAR. Ce processus dure jusqu'à 15 minutes.</p> <p>Le micrologiciel iKVM a détecté une erreur matérielle. Pour des informations supplémentaires, affichez la condition d'iKVM.</p> <p>Pour afficher la condition d'iKVM avec l'interface Web :</p> <ol style="list-style-type: none"> Ouvrez une session sur l'interface Web de CMC. Sélectionnez iKVM dans l'arborescence du système. <p>Pour afficher la condition d'iKVM à l'aide de RACADM, ouvrez une console texte série/Telnet/SSH vers CMC, ouvrez une session et tapez :</p> <pre>racadm getkvminfo</pre>
Plusieurs couches ont été affectées à mon iKVM via le port ACI vers un commutateur KVM externe, mais toutes les entrées pour les connexions ACI sont indisponibles.	<p>La connexion du panneau avant est activée et un moniteur y est connecté. Le panneau avant étant prioritaire sur toutes les autres connexions d'iKVM, les connecteurs de l'ACI et du panneau arrière sont désactivés.</p>
Tous les états sont indiqués par un point jaune dans l'interface OSCAR.	<p>Pour activer la connexion du port ACI, vous devez d'abord désactiver l'accès au panneau avant ou retirer le moniteur connecté au panneau avant. Les entrées OSCAR du commutateur KVM externe deviendront actives et accessibles.</p> <p>Pour désactiver le panneau avant via l'interface Web :</p> <ol style="list-style-type: none"> Ouvrez une session sur l'interface Web de CMC. Sélectionnez iKVM dans l'arborescence du système. Cliquez sur l'onglet Configuration. Décochez la case USB/Vidéo du panneau avant activé. Cliquez sur Appliquer pour enregistrer le paramètre. <p>Pour activer le panneau avant à l'aide de RACADM, ouvrez une console texte série/Telnet/SSH vers CMC, ouvrez une session et tapez :</p> <pre>racadm config -g cfgKVMInfo -o cfgKVMFrontPanelEnable 0</pre>
Dans le menu OSCAR, la connexion Dell CMC affiche un X rouge et je ne peux pas me connecter à CMC.	<p>Deux causes sont possibles :</p> <p>La console Dell CMC a été désactivée. Dans ce cas, vous pouvez l'activer avec l'interface Web de CMC ou RACADM.</p> <p>Pour activer la console Dell CMC avec l'interface Web :</p> <ol style="list-style-type: none"> Ouvrez une session sur l'interface Web de CMC. Sélectionnez iKVM dans l'arborescence du système. Cliquez sur l'onglet Configuration. Cochez la case Autoriser l'accès à l'interface de ligne de commande CMC depuis iKVM. Cliquez sur Appliquer pour enregistrer le paramètre. <p>Pour activer la connexion Dell CMC à l'aide de RACADM, ouvrez une console texte série/Telnet/SSH vers CMC, ouvrez une session et tapez :</p> <pre>racadm config -g cfgKVMInfo -o cfgKVMAccessToCMCEnable 1</pre> <p>CMC est indisponible car il s'initialise, commute vers le contrôleur CMC de secours ou se reprogramme. Dans ce cas, attendez tout simplement que CMC ait terminé de s'initialiser.</p>
Le nom de logement d'un serveur affiche « Initialisation en cours » dans OSCAR et je ne peux pas le sélectionner.	<p>Le serveur s'initialise ou le contrôleur iDRAC sur ce serveur n'a pas pu s'initialiser.</p> <p>Attendez tout d'abord 60 secondes. Si le serveur s'initialise toujours, le nom de logement apparaît dès que l'initialisation est terminée et vous pouvez sélectionner le serveur.</p> <p>Si, après 60 secondes, OSCAR indique encore que le logement s'initialise, retirez puis réinsérez le serveur dans le châssis. Cette action permet à iDRAC de se réinitialiser.</p>

[Retour à la page Contenu](#)

[Retour à la page Contenu](#)

Installation et configuration de CMC

Micrologiciel Dell Chassis Management Controller Version 3.1 Guide d'utilisation

- [Avant de commencer](#)
- [Installation du matériel CMC](#)
- [Installation du logiciel d'accès à distance sur une station de gestion](#)
- [Configuration d'un navigateur Web](#)
- [Configuration de l'accès initial à CMC](#)
- [Accès à CMC via un réseau](#)
- [Installation ou mise à jour du micrologiciel du module CMC](#)
- [Configuration des propriétés de CMC](#)
- [Fonctionnement de l'environnement CMC redondant](#)

Cette section contient des informations sur l'installation de votre matériel CMC, l'accès à CMC et la configuration de votre environnement de gestion en vue d'utiliser CMC, et vous guide dans les étapes suivantes de configuration de CMC.

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

Pour plus d'informations sur l'installation et la configuration des environnements CMC redondants, 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 sur 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 pré-installé sur votre châssis, donc aucune installation n'est requise. Vous pouvez installer un second contrôleur CMC qui servira de CMC secours. Pour plus d'informations sur l'utilisation d'un contrôleur de secours, voir [Fonctionnement de l'environnement CMC redondant](#).

Liste de contrôle pour l'intégration d'un châssis

Les étapes suivantes vous permettent de configurer le châssis avec précision :

1. Votre contrôleur CMC et la station de gestion sur laquelle vous utilisez votre navigateur doivent appartenir au même réseau appelé le réseau de gestion. Reliez le port Ethernet CMC nommé **GB** au réseau de gestion.

 **REMARQUE** : ne placez pas de câble dans le port Ethernet CMC nommé **STK**. Pour plus d'informations sur le câblage du port STK, voir [Fonctionnement de l'environnement CMC redondant](#).

2. Pour les châssis en rack, 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 situé sur le côté du châssis ou allumez le châssis depuis l'interface 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 de CMC via le navigateur web en utilisant le nom d'utilisateur (**root**) et le mot de passe (**Calvin**) par défaut.
8. À chaque iDRAC, donnez une adresse IP dans l'interface utilisateur CMC et activez l'interface LAN et IPMI.

 **REMARQUE** : l'interface LAN iDRAC sur certains serveurs est désactivée par défaut

9. À chaque module d'E/S, donnez une adresse IP dans l'interface utilisateur CMC.

10. Connectez-vous à chaque iDRAC par l'intermédiaire du navigateur Web et fournissez la configuration finale d'Idrac. Le nom d'utilisateur par défaut est root et le mot de passe par défaut est 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. Allumez les serveurs et installez le système d'exploitation.

Connexion réseau CMC de base

Pour une redondance maximale, connectez chaque contrôleur CMC à votre réseau de gestion. Si un châssis comporte un seul contrôleur CMC, établissez une seule connexion au réseau de gestion. Si le châssis a un contrôleur CMC redondant, effectuez deux connexions au réseau de gestion.

Chaque CMC dispose de deux ports Ethernet RJ-45, nommés **GB1** (port de *sortie des données*) et **STK** (port d'*extension* ou de consolidation de câble). Vous devez connecter le port GB au réseau de gestion à l'aide d'un câblage élémentaire et laisser le port STK inutilisé.

⚠ PRÉCAUTION : la connexion du port STK au réseau de gestion peut provoquer des résultats imprévisibles. Le câblage des ports GB et STK au même réseau (domaine de diffusion) peut provoquer une perturbation importante de la diffusion.

Connexion réseau CMC en chaîne

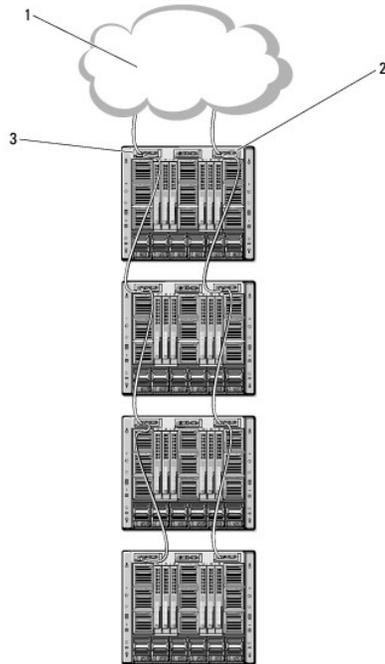
Si vous disposez de plusieurs châssis dans un rack, vous pouvez réduire le nombre de connexions au réseau de gestion en connectant jusqu'à quatre châssis en chaîne. Si chacun des quatre châssis contient un contrôleur CMC redondant, la connexion en chaîne permet de réduire le nombre des connexions au réseau de gestion de huit à deux. Si chaque châssis ne comporte un seul CMC, les connexions sont réduites de quatre à une seule.

Lors de la connexion en chaîne des châssis, GB est le port « de sortie des données » et STK est le port d'« extension » (consolidation de câble). Connectez les ports GB au réseau de gestion ou au port STK de CMC dans un châssis qui est plus proche du réseau. Vous devez vous connecter le port STK à un port GB plus éloigné de la chaîne ou du réseau seulement.

Créez des chaînes distinctes pour les contrôleurs CMC des logements CMC principaux et secondaires.

La [Figure 2-1](#) illustre l'agencement des câbles pour quatre châssis en chaîne, chacun avec un contrôleur CMC actif et un contrôleur CMC secondaire en veille.

Figure 2-1. Connexion réseau CMC en chaîne



1	réseau de gestion	2	CMC principal
3	CMC secondaire		

La [Figure 2-2](#), la [Figure 2-3](#) et la [Figure 2-4](#) montrent des exemples de câblage incorrect de CMC.

Figure 2-2. Mauvais câblage pour la connexion réseau CMC - 2 CMC

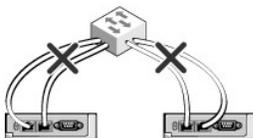
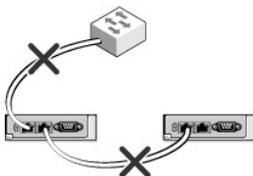


Figure 2-3. Mauvais câblage pour la connexion réseau CMC - 1 CMC



Figure 2-4. Mauvais câblage pour la connexion réseau CMC - 2 CMC



Suivez les étapes suivantes pour la connexion en chaîne de jusqu'à quatre châssis :

1. Connectez le port GB de CMC actif du premier châssis au réseau de gestion.
2. Connectez le port GB de CMC actif du second châssis au port STK de CMC actif du premier châssis.
3. Si vous disposez d'un troisième châssis, connectez le port GB de son contrôleur CMC actif au port STK du contrôleur CMC actif du second châssis.
4. Si vous disposez d'un quatrième châssis, connectez le port GB de son contrôleur CMC actif au 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 de chacun des contrôleurs CMC ne doit jamais être connecté au réseau de gestion. Il peut uniquement être connecté au port GB d'un autre châssis. La connexion d'un port STK au réseau de gestion peut perturber le réseau et entraîner une perte de données. Le câblage des ports GB et STK au même réseau (domaine de diffusion) peut provoquer une perturbation importante de la diffusion.

📌 REMARQUE : ne branchez jamais un contrôleur CMC actif sur un contrôleur CMC secondaire.

📌 REMARQUE : la réinitialisation d'un contrôleur CMC dont le port STK est connecté en chaîne à un autre contrôleur CMC peut perturber le réseau pour les contrôleurs CMC situés plus loin dans la chaîne. Les contrôleurs CMC enfants peuvent journaliser des messages qui indiquent que la liaison réseau a été perdue et peuvent basculer sur leurs contrôleurs CMC redondants.

Pour démarrer avec CMC, voir [Installation du 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 le RACADM distant à partir de votre station de gestion, installez-le en utilisant le DVD de documentation et d'outils de Dell Systems Management qui est disponible avec votre système. Ce DVD inclut les composants Dell OpenManage suivants :

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

Pour plus d'informations sur l'installation des composants logiciels Dell OpenManage, voir le *Guide d'utilisation de Dell OpenManage Installation and Security* disponible sur le DVD ou à l'adresse support.dell.com/manuals. Vous pouvez télécharger la dernière version des outils DRAC de Dell sur le site Web de support de Dell à l'adresse support.dell.com.

Installation de l'utilitaire 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 Managed System.
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** : sur le système d'exploitation Red Hat Enterprise Linux 5, les DVD sont montés automatiquement avec l'option `-noexec` `mount`. Cette option ne vous permet pas d'exécuter de fichiers exécutables à partir du DVD. Vous devez monter manuellement le DVD-ROM, puis exécuter les programmes exécutables.

4. Accédez au répertoire `SYSMGMT/ManagementStation/linux/rac`. Pour installer le logiciel RAC, entrez la commande suivante :

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

5. Si vous avez besoin d'aide avec la commande RACADM, tapez `racadm help` après avoir émis les commandes précédentes. Pour plus d'informations sur RACADM, voir [Utilisation de l'interface de ligne de commande RACADM](#).

 **REMARQUE** : lors de l'utilisation des fonctionnalités distantes de l'utilitaire RACADM, vous devez disposer d'un accès en écriture sur les dossiers sur lesquels vous utilisez les sous-commandes RACADM impliquant des opérations sur des fichiers, comme par exemple :

```
racadm getconfig -f <nom de fichier>
```

Pour plus d'informations sur `racadm` distant, voir [Accès à distance à RACADM](#) et les sections suivantes.

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 d'un navigateur Web

Vous pouvez configurer et gérer CMC ainsi que les serveurs et modules installés sur le châssis via un navigateur Web. voir la section *Navigateurs pris en charge de la Matrice de prise en charge des logiciels des systèmes Dell* sur le site Web du support de Dell à l'adresse support.dell.com/manuals.

Votre CMC et la station de gestion sur laquelle vous utilisez votre navigateur doivent appartenir au même réseau, que l'on appelle le *réseau de gestion*. En fonction de vos besoins de sécurité, le réseau de gestion peut être un réseau isolé hautement sécurisé.

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

Il convient également de garder à l'esprit que les fonctionnalités de certains navigateurs peuvent interférer avec la connectivité et les performances, en particulier si le réseau de gestion ne dispose pas d'un accès à Internet. Si votre station de gestion exécute un système d'exploitation Windows, certains paramètres d'Internet Explorer peuvent interférer avec la connectivité même si vous utilisez une interface de ligne de commande pour accéder au réseau de gestion.

Serveur proxy

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

Internet Explorer

Suivez les étapes suivantes pour modifier la liste d'exceptions dans Internet Explorer :

1. Démarrez Internet Explorer.
2. Cliquez sur **Outils**→ **Options Internet**→ **Connexions**.
3. Dans la section **Paramètres du réseau local**, cliquez sur **Paramètres réseau**.
4. Dans la section **Serveur proxy**, cliquez sur **Avancé**.
5. Dans la section **Exceptions**, ajoutez les adresses des contrôleurs CMC et iDRAC du réseau de gestion à la liste dont les éléments sont séparés par des points-virgules. Vous pouvez utiliser des noms DNS et des caractères génériques dans vos entrées.

Mozilla FireFox

Pour modifier la liste des exceptions dans Mozilla Firefox version 3.0 :

1. Lancez Mozilla Firefox.
2. Cliquez sur **Outils**→ **Options** (pour Windows) ou sur **Modifier**→ **Préférences** (pour Linux).
3. Cliquez sur **Avancé**, puis cliquez sur l'onglet **Réseau**.
4. Cliquez sur **Paramètres**.
5. Sélectionnez la Configuration manuelle de Proxy.
6. Dans le champ **Pas de proxy pour**, ajoutez les adresses des contrôleurs CMC et iDRAC du réseau de gestion à la liste dont les éléments sont séparés par des virgules. Vous pouvez utiliser des noms DNS et des caractères génériques dans vos entrées.

Filtre anti-hameçonnage de Microsoft

Si le filtre anti-hameçonnage de Microsoft est activé dans Internet Explorer 7 sur votre système de gestion, et que votre CMC n'a pas accès à Internet, l'accès à CMC peut être retardé de quelques secondes. Ce retard peut se produire si vous utilisez le navigateur ou une autre interface, comme RACADM distant. Suivez les étapes suivantes pour désactiver le filtre anti-hameçonnage :

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

Récupération de la liste de révocation des certificats

Si CMC ne dispose pas d'un accès à Internet, désactivez la fonctionnalité de récupération de la liste de révocation des certificats dans Internet Explorer. Cette fonctionnalité vérifie si un serveur comme le serveur Web de CMC utilise un certificat figurant sur une liste de certificats révoqués, récupérée à partir d'Internet. Si Internet est inaccessible, cette fonctionnalité peut provoquer des retards de plusieurs secondes lorsque vous accédez à CMC à l'aide du navigateur ou d'une interface de ligne de commande telle que RACADM distant.

Suivez les étapes suivantes pour désactiver la récupération de la liste de révocation des certificats :

1. Démarrez Internet Explorer.
2. Cliquez sur **Outils**→ **Options Internet**, puis sur **Avancé**.

3. Faites défiler la liste des paramètres jusqu'à la section Sécurité et décochez la case **Vérifier la révocation des certificats de l'éditeur**.
4. 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 lorsque 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 sur **Avancé**.
3. Défilez jusqu'à la section Sécurité et cochez **Ne pas enregistrer les pages cryptées sur le disque**.

Autorisation des animations dans Internet Explorer

Lors du transfert de fichiers vers et à partir de l'interface Web, une icône de transfert de fichiers tourne pour indiquer l'activité de transfert. Dans Internet Explorer, cela exige la configuration du navigateur pour la lecture d'animations. Il s'agit de la configuration par défaut.

Suivez les étapes suivantes pour configurer Internet Explorer pour la lecture d'animations :

1. Démarrez Internet Explorer.
2. Cliquez sur **Outils** → **Options Internet**, puis sur **Avancé**.
3. Faites défiler la liste des paramètres jusqu'à la section Multimédia et 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** : la solution M1000e doit être connectée à votre réseau de gestion pour que vous puissiez la gérer.

Pour plus d'informations sur la configuration des paramètres réseau de CMC, voir [Configuration du réseau CMC](#). Cette configuration initiale définit les paramètres réseau TCP/IP qui permettent l'accès à CMC.

CMC et iDRAC sur chaque serveur et les ports de gestion de réseau pour tous les modules d'E/S sont connectés à un réseau commun interne dans le châssis M1000e. Cela permet au réseau de gestion d'être isolé du réseau de données du serveur. Il est important de séparer ce trafic pour un accès ininterrompu à la gestion du châssis.

CMC est connecté au réseau de gestion. Tout accès externe à CMC et aux micrologiciels iDRAC s'effectue via CMC. L'accès aux serveurs gérés s'effectue, à l'inverse, via des connexions réseau aux modules d'E/S. Cela permet d'isoler le réseau applicatif du réseau de gestion.

 **REMARQUE** : il est recommandé d'isoler la gestion du châssis du réseau de données. Dell ne peut pas soutenir ou garantir la disponibilité d'un châssis qui est mal intégré à l'environnement. En raison du potentiel de trafic sur le réseau de données, les interfaces de gestion sur le réseau de gestion interne peuvent être saturées par le trafic destiné aux serveurs. Il en résulte des retards de communication dans CMC et iDRAC. Les retards peuvent donner lieu à un comportement imprévisible du châssis, par exemple, CMC peut afficher iDRAC comme étant hors ligne alors qu'il est sous tension et en cours d'exécution, entraînant à son tour un autre comportement indésirable. S'il s'avère peu pratique d'isoler physiquement le réseau de gestion, l'autre option consiste à séparer le trafic CMC et iDRAC sur un VLAN séparé. Les interfaces réseau CMC et iDRAC peuvent être configurées pour utiliser un VLAN avec la commande `racadm setniccfg`. Pour plus d'informations, voir le *Guide de référence de l'administrateur de Dell Chassis Management Controller*.

Si vous ne disposez que d'un seul châssis, connectez le contrôleur CMC principal et le cas échéant le contrôleur CMC de secours au réseau de gestion. Si vous disposez d'un contrôleur CMC redondant, utilisez un autre câble réseau et connectez le port GB CMC à un second port du réseau de gestion.

Si vous disposez de plusieurs châssis, vous pouvez choisir entre une connexion de base où chaque CMC est connecté au réseau de gestion, et une connexion en chaîne des châssis où les châssis sont connectés en série et où seul l'un d'entre eux est connecté au réseau de gestion. La connexion de base utilise un plus grand nombre de ports sur le réseau de gestion et offre une plus grande redondance. La connexion en chaîne utilise un nombre moins important de ports sur le réseau de gestion mais introduit des dépendances entre les contrôleurs CMC, ce qui réduit la redondance du système.

Pour plus d'informations sur la connexion en chaîne, voir [Connexion réseau CMC en chaîne](#).

 **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.

Configuration du réseau CMC

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

Vous pouvez effectuer la configuration réseau initiale d'un contrôleur CMC avant ou après l'obtention d'une adresse IP par CMC. Si vous configurez les paramètres réseau initiaux de CMC *avant* d'avoir obtenu une adresse IP, vous pouvez utiliser l'une des interfaces suivantes :

- 1 L'écran LCD du panneau avant du châssis
- 1 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 :

- 1 Interfaces de ligne de commande telles que la console série, Telnet, SSH ou la console CMC Dell via iKVM
- 1 RACADM distante
- 1 L'interface Web CMC

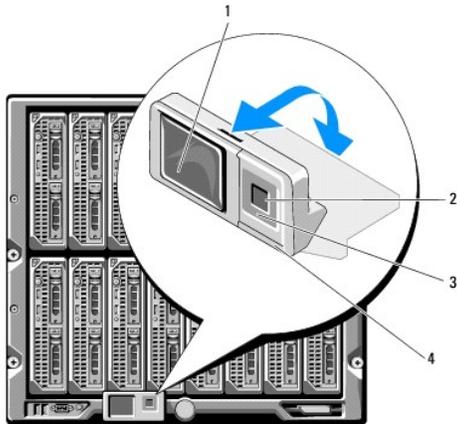
Configuration de la mise en réseau à l'aide de l'assistant de configuration de l'écran LCD

REMARQUE : Vous ne pouvez utiliser l'assistant de configuration de l'écran LCD pour configurer CMC qu'avant le déploiement de CMC ou la modification du mot de passe par défaut. Si le mot de passe n'est pas modifié, il est toujours possible d'utiliser l'écran LCD pour reconfigurer CMC, en créant un risque de sécurité.

L'écran LCD se situe dans le coin inférieur gauche à l'avant du châssis.

[Figure 2-5](#) présente l'écran LCD.

Figure 2-5. Affichage LCD



1 écran LCD	2 bouton de sélection (« cocher »)
3 boutons de défilement (4)	4 indicateur d'état LED

L'écran LCD affiche des menus, des icônes, des images et des messages.

Un indicateur d'état LED de l'écran LCD fournit une indication de l'intégrité générale du châssis et de ses composants.

- 1 Un voyant bleu continu indique une intégrité satisfaisante.
- 1 Un voyant orange clignotant indique qu'au moins un composant est défaillant.
- 1 Un voyant bleu clignotant est un signal d'identification d'un châssis au sein d'un groupe de châssis.

Navigaison dans l'écran LCD

Le côté droit de l'écran LCD comporte cinq boutons : quatre boutons fléchés (haut, bas, gauche et droite) ainsi qu'un bouton central.

- 1 *Pour vous déplacer d'un écran à l'autre*, utilisez les boutons flèche droite (suivant) et gauche (précédent). Au cours de l'utilisation de l'assistant de configuration, vous pouvez à tout moment revenir à l'écran précédent.
- 1 *Pour faire défiler les options d'un écran*, utilisez les boutons flèche bas et haut.
- 1 *Pour sélectionner et enregistrer l'élément d'un écran et passer à l'écran suivant*, utilisez le bouton central.

Pour des informations supplémentaires sur l'utilisation de l'écran LCD, voir la section portant sur l'écran LCD du *Guide de référence de la ligne de commande pour iDRAC6 et CMC*.

Utilisation de l'assistant de configuration de l'écran LCD

1. Si cela n'est pas déjà fait, appuyez sur le bouton d'alimentation du châssis pour le mettre sous tension.

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

2. Sélectionnez votre langue à l'aide des boutons fléchés, puis appuyez sur le bouton central pour sélectionner **Accepter/Oui** puis appuyez à nouveau sur le bouton central.
3. L'écran **Enceinte** s'affiche avec la question suivante : **Configurer l'enceinte ?**
 - a. Appuyez sur le bouton central pour passer à l'écran **Paramètres réseau CMC**. Voir l'étape 4.
 - b. Pour quitter le menu **Configurer l'enceinte**, sélectionnez l'icône NON et appuyez sur le bouton central. Voir l'étape 9.
4. Appuyez sur le bouton central pour passer à l'écran **Paramètres réseau CMC**.
5. Sélectionnez la vitesse de votre réseau (10 Mbits/s, 100 Mbits/s, 1 Gbit/s ou Automatique) à l'aide du bouton flèche bas.

 **REMARQUE** : le paramètre Vitesse réseau doit correspondre à votre configuration réseau afin de garantir l'efficacité du débit du réseau. Si la vitesse réseau que vous paramétrez est inférieure à la vitesse de votre configuration réseau, la consommation de bande passante augmente et les communications réseau ralentissent. **Déterminez si votre réseau prend en charge les vitesses réseau ci-dessus et paramétrez-le en conséquence.** Si votre configuration réseau ne correspond à aucune de ces valeurs, Dell vous recommande d'utiliser la négociation automatique (option **Automatique**) ou de contacter le fabricant de votre équipement réseau.

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

6. Sélectionnez le mode duplex (semi ou total) 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.

 **REMARQUE** : si la négociation automatique est activée pour un périphérique mais pas pour l'autre, alors le périphérique qui utilise la négociation automatique peut déterminer la vitesse réseau de l'autre périphérique, mais pas le mode duplex. Dans ce cas, le mode duplex adopte par défaut le paramètre Semi-duplex lors de la négociation automatique. Une telle différence de mode duplex entraîne un ralentissement des connexions réseau.

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

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

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

8. Sélectionnez le mode selon lequel vous souhaitez que CMC obtienne les adresses IP de la carte réseau :

Protocole de configuration dynamique des hôtes	CMC récupère automatiquement la configuration IP (adresse IP, masque et passerelle) auprès d'un serveur DHCP de votre réseau. CMC reçoit une adresse IP unique allouée via votre réseau. Si vous avez sélectionné l'option DHCP, appuyez sur le bouton central. L'écran Configurer iDRAC ? s'affiche. Voir étape 10 .
Statique	<p>Vous devez entrer manuellement l'adresse IP, la passerelle et le masque de sous-réseau dans les écrans qui suivent.</p> <p>Si vous avez sélectionné l'option Statique, appuyez sur le bouton central pour poursuivre avec l'écran Paramètres réseau CMC suivant, puis :</p> <ol style="list-style-type: none">a. Définissez l'adresse IP statique en utilisant les touches fléchées droite ou gauche pour vous déplacer et les touches fléchées haut et bas pour sélectionner un nombre pour chaque position. Une fois l'adresse IP statique définie, appuyez sur le bouton central pour continuer.b. Définissez le masque de sous-réseau, puis appuyez sur le bouton central.c. Définissez la passerelle, puis appuyez sur le bouton central. L'écran Résumé réseau s'affiche. <p>L'écran Résumé réseau répertorie l'adresse IP statique, le masque de sous-réseau et la passerelle que vous venez d'entrer. Vérifiez l'exactitude de ces paramètres. Pour corriger un paramètre, accédez au bouton flèche gauche, puis appuyez sur le bouton central pour retourner à l'écran de ce paramètre. Après avoir effectué une correction, appuyez sur le bouton central.</p> <ol style="list-style-type: none">a. Après avoir vérifié l'exactitude des paramètres entrés, appuyez sur le bouton central. L'écran Enregistrer le DNS ? apparaît.

 **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.

9. 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. Si vous ne possédez pas de DNS, appuyez sur la touche fléchée droite. L'écran **Enregistrer le DNS ?** apparaît ; passez à l'étape 10.

Définissez l'adresse IP du DNS en utilisant les touches fléchées droite ou gauche pour vous déplacer et les touches fléchées haut et bas pour sélectionner un nombre pour chaque position. Une fois l'adresse IP du DNS définie, appuyez sur le bouton central pour continuer.

10. Indiquez si vous souhaitez configurer iDRAC :

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

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

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

Protocole de configuration dynamique des hôtes	iDRAC récupère automatiquement la configuration IP (adresse IP, masque et passerelle) auprès d'un serveur DHCP de votre réseau. Une adresse IP unique sera attribuée à iDRAC via votre réseau. Appuyez sur le bouton central.
Statique	<p>Vous devez entrer manuellement l'adresse IP, la passerelle et le masque de sous-réseau dans les écrans qui suivent.</p> <p>Si vous avez sélectionné l'option Statique, appuyez sur le bouton central pour passer à l'écran Paramètres réseau iDRAC suivant, puis :</p> <ol style="list-style-type: none"> a. Définissez l'adresse IP statique en utilisant les touches fléchées droite ou gauche pour vous déplacer et les touches fléchées haut et bas pour sélectionner un nombre pour chaque position. Cette adresse est l'adresse IP statique de qui se trouve dans le premier logement. L'adresse IP statique de chaque iDRAC suivant est calculée en tant qu'incrément du numéro d'emplacement de cette adresse IP. Une fois l'adresse IP statique définie, appuyez sur le bouton central pour continuer. b. Définissez le masque de sous-réseau, puis appuyez sur le bouton central. c. Définissez la passerelle, puis appuyez sur le bouton central.

- a. Sélectionnez **Activer** ou **Désactiver** pour activer ou désactiver le canal IPMI LAN. Appuyez sur le bouton central pour continuer.
- b. Sur l'écran **Configuration iDRAC**, pour appliquer tous les paramètres réseau iDRAC aux serveurs installés, mettez en surbrillance l'icône **Accepter/Oui** et appuyez sur le bouton central. Pour ne pas appliquer les paramètres réseau iDRAC aux serveurs installés, mettez en surbrillance l'icône **Non** et appuyez sur le bouton central pour passer à l'étape c.
- c. Sur l'écran **Configuration iDRAC** suivant, pour appliquer tous les paramètres réseau iDRAC aux serveurs récemment installés, mettez en surbrillance l'icône **Accepter/Oui** et appuyez sur le bouton central ; lorsqu'un nouveau serveur est inséré dans le châssis, l'écran LCD invite l'utilisateur à préciser s'il souhaite déployer automatiquement le serveur à l'aide des paramètres/règles réseau précédemment configurés. Pour ne pas appliquer les paramètres réseau iDRAC aux serveurs récemment installés, mettez en surbrillance l'icône **Non** et appuyez sur le bouton central ; lorsqu'un nouveau serveur est inséré dans le châssis, les paramètres réseau iDRAC ne sont pas configurés.

12. Sur l'écran **Enceinte**, mettez en surbrillance l'icône **Accepter/Oui** et appuyez sur le bouton central pour appliquer tous les paramètres d'enceinte. Pour ne pas appliquer les paramètres d'enceinte, mettez en surbrillance l'icône **Non** et appuyez sur le bouton central.

13. Sur l'écran **Résumé IP**, vérifiez que les adresses IP que vous avez fournies sont correctes. Pour corriger un paramètre, accédez au bouton flèche gauche, puis appuyez sur le bouton central pour retourner à l'écran de ce paramètre. Après avoir effectué votre correction, appuyez sur le bouton central. Le cas échéant, accédez au bouton flèche droite, puis appuyez sur le bouton central pour retourner à l'écran **Résumé IP**.

Lorsque vous avez confirmé l'exactitude des paramètres saisis, appuyez sur le bouton central. L'assistant de configuration se ferme et revient 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 modules CMC et iDRAC sont désormais disponibles sur le réseau. Vous pouvez accéder à CMC sur l'adresse IP attribuée à l'aide de l'interface Web ou des interfaces de ligne de commande telles que la console série, Telnet et SSH.

 **REMARQUE** : une fois la configuration réseau à l'aide de l'assistant de configuration de l'écran LCD terminée, l'assistant n'est plus disponible.

Accès à CMC via un réseau

Après avoir configuré les paramètres réseau CMC, vous pouvez accéder à distance à CMC à l'aide de l'une des interfaces suivantes :

- 1 Interface Web
- 1 Console Telnet
- 1 SSH
- 1 RACADM distante

 **REMARQUE** : puisque telnet n'est pas aussi sécurisé que les autres interfaces, il est désactivé par défaut. Activez Telnet via le Web, SSH ou RACADM distant.

Tableau 2-1. Interfaces CMC

Interface	Description
-----------	-------------

Interface Web	Fournit un accès à distance à CMC à l'aide d'une interface utilisateur. L'interface Web est intégrée au micrologiciel CMC et accessible via l'interface NIC d'un navigateur Web pris en charge sur la station de gestion. Pour obtenir une liste des navigateurs Web pris en charge, consultez la section <i>Navigateurs pris en charge</i> de la <i>Matrice de prise en charge des logiciels des systèmes Dell</i> sur le site Web du support de Dell à l'adresse support.dell.com/manuals .
Interface de ligne de commande RACADM distante	Fournit un accès à distance à CMC à partir d'une station de gestion qui utilise une interface de ligne de commande. L'utilitaire RACADM distant utilise l'option <code>racadm -r</code> avec l'adresse IP de CMC pour exécuter des commandes sur CMC. Pour plus d'informations sur <code>racadm</code> distant, voir Accès à distance à RACADM et les sections suivantes.
Telnet	Fournit un accès par ligne de commande à CMC via le réseau. L'interface de ligne de commande RACADM et la commande <code>connect</code> , utilisées pour se connecter à la console série d'un serveur ou d'un module d'E/S, sont disponibles à partir de la ligne de commande CMC. REMARQUE : Telnet est un protocole non sécurisé qui transmet toutes les données, y compris les mots de passe, en texte simple. Lors de la transmission d'informations critiques, utilisez l'interface SSH.
SSH	Fournit les mêmes fonctionnalités que la console Telnet par l'utilisation d'une couche de transport cryptée pour une sécurité accrue.

 **REMARQUE** : le nom d'utilisateur par défaut de CMC est `root` et le mot de passe par défaut est `calvin`.

Vous pouvez accéder aux interfaces Web CMC et iDRAC via la carte d'interface réseau CMC à l'aide d'un navigateur Web pris en charge. Vous pouvez également les lancer à partir de Dell Server Administrator ou de Dell OpenManage IT Assistant.

Pour obtenir une liste des navigateurs Web pris en charge, consultez la section *Navigateurs pris en charge* de la *Matrice de prise en charge des logiciels des systèmes Dell* sur le site Web du support de Dell à l'adresse support.dell.com/manuals. Pour accéder à CMC via un navigateur Web pris en charge, voir [Accès à l'interface Web CMC](#). Pour plus d'informations sur Dell OpenManage IT Assistant, voir [Installation du logiciel d'accès à distance sur une station de gestion](#).

Pour accéder à l'interface CMC à l'aide de Dell Server Administrator, lancez Server Administrator sur votre station de gestion. Dans l'arborescence du système située sur le panneau gauche de la page d'accueil de Server Administrator, cliquez sur **Système** → **Châssis principal du système** → **Remote Access Controller**. Pour plus d'informations, consultez le *Guide d'utilisation de Dell Server Administrator*.

Pour accéder à la ligne de commande de CMC à l'aide de Telnet ou de SSH, voir [Configuration de CMC pour utiliser des consoles de ligne de commande](#).

Pour plus d'informations sur l'utilisation de RACADM, voir [Utilisation de l'interface de ligne de commande RACADM](#).

Pour plus d'informations sur l'utilisation de la commande `connect`, ou `racadm connect`, pour se connecter aux serveurs et modules d'E/S, voir [Connexion aux serveurs ou aux modules d'E/S à l'aide de la commande Connect](#).

Installation ou mise à jour du micrologiciel du module CMC

Téléchargement du micrologiciel du module CMC

Avant d'entamer la mise à jour du micrologiciel, téléchargez la dernière version du micrologiciel sur le site Web de support de Dell à l'adresse support.dell.com et enregistrez-la sur votre système local.

Le progiciel du micrologiciel de CMC se compose des éléments suivants :

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

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

 **REMARQUE** : par défaut, la mise à jour du micrologiciel conserve les paramètres CMC définis. Au cours de la mise à jour, vous pouvez réinitialiser les paramètres de configuration du module CMC afin de rétablir les valeurs par défaut définies en usine.

 **REMARQUE** : si des contrôleurs CMC redondants sont installés dans le châssis, il est essentiel de les mettre tous les deux à jour avec la même version du micrologiciel. Si les contrôleurs CMC utilisent des micrologiciels différents et qu'un basculement se produit, des résultats inattendus peuvent se produire.

Vous pouvez utiliser la commande `getsysinfo` de RACADM (voir la section relative à la commande `getsysinfo` du *Guide de référence de la ligne de commande pour iDRAC et CMC*) ou la page **Résumé du châssis** (voir [Affichage des versions actuelles du micrologiciel](#)) pour afficher les versions de micrologiciel actuelles des contrôleurs CMC installés dans votre châssis.

Si vous disposez d'un contrôleur CMC de secours, il est recommandé de mettre les deux contrôleurs CMC à jour en même temps en une seule opération. Une fois le contrôleur de secours mis à jour, permutez les rôles des modules CMC de manière à ce que celui qui vient d'être mis à jour devienne le contrôleur actif et que celui doté de l'ancien micrologiciel devienne le contrôleur de secours. (voir la section relative à la commande `cmchangeover` du *Guide de référence de l'administrateur de la ligne de commande pour iDRAC et CMC* pour obtenir de l'aide concernant l'échange de rôles). Ceci vous permet de vérifier que la mise à jour s'est bien déroulée et que le nouveau micrologiciel fonctionne correctement avant de procéder à la mise à jour du micrologiciel au sein du deuxième contrôleur CMC. Lorsque les deux contrôleurs CMC sont mis à jour, vous pouvez utiliser la commande `cmchangeover` pour rétablir leurs rôles précédents. Le micrologiciel CMC révision 2.x met à jour le contrôleur principal et le contrôleur redondant sans l'aide de la commande `cmchangeover`.

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

Pour des instructions sur l'utilisation de l'interface Web pour la mise à jour du micrologiciel CMC, voir [Mise à jour du micrologiciel CMC](#).

Mise à jour du micrologiciel CMC via RACADM

Pour obtenir des instructions relatives à l'utilisation de la sous-commande `fwupdate` de l'utilitaire RACADM pour mettre à jour le micrologiciel CMC, consultez la section relative à la commande `fwupdate` du *Guide de référence de la ligne de commande pour iDRAC et CMC*.

Configuration des propriétés de CMC

Vous pouvez configurer les propriétés de CMC telles que le bilan d'alimentation, 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.

Pour plus d'informations sur l'utilisation de l'interface Web, voir [Accès à l'interface Web CMC](#). Pour plus d'informations sur l'utilisation de RACADM, voir [Utilisation de l'interface de ligne de commande RACADM](#).

 **PRÉCAUTION** : l'utilisation simultanée de plusieurs outils de configuration CMC peut provoquer des résultats inattendus.

Configuration des bilans de puissance

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.

Pour plus d'informations sur la gestion de l'alimentation de CMC, voir [Gestion de l'alimentation](#).

Pour des instructions sur la configuration du bilan de puissance et des autres paramètres d'alimentation à l'aide de l'interface Web, voir [Configuration des bilans de puissance](#).

Configuration des paramètres réseau de CMC

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

Vous pouvez configurer les paramètres réseau de CMC à l'aide de l'un des outils suivants :

- 1 RACADM : pour plus d'informations, voir [Configuration de plusieurs CMC dans plusieurs châssis](#).

 **REMARQUE** : pour déployer CMC dans un environnement Linux, voir [Installation de l'utilitaire RACADM sur une station de gestion Linux](#).

- 1 Interface Web : pour plus d'informations, voir [Configuration des propriétés du réseau CMC](#).

Ajout et configuration des utilisateurs

Vous pouvez ajouter et configurer des utilisateurs CMC en utilisant soit RACADM, soit l'interface Web CMC. Vous pouvez également utiliser Microsoft Active Directory pour gérer les utilisateurs.

Pour obtenir des instructions sur l'ajout et la configuration des utilisateurs de clé publique pour CMC à l'aide de RACADM, voir [Utilisation de RACADM pour configurer l'authentification par clé publique sur SSH](#). Pour des instructions sur l'ajout et la configuration d'utilisateurs à l'aide de l'interface Web, voir [Ajout et configuration d'utilisateurs CMC](#).

Pour des instructions sur l'utilisation d'Active Directory avec votre CMC, voir [Utilisation du service d'annuaire CMC](#).

Ajout d'alertes SNMP et par e-mail

Vous pouvez configurer CMC pour générer des alertes SNMP et/ou par e-mail lorsque certains événements se produisent au niveau du châssis. Pour en savoir plus, voir [Configuration des alertes SNMP](#) et [Configuration des alertes par e-mail](#).

Configuration de Syslog distant

La fonctionnalité *syslog distant* est activée/configurée via l'interface utilisateur de CMC ou la commande `racadm`. Les options de configuration incluent le nom (ou l'adresse IP) du serveur syslog et le port UDP utilisé par CMC lors du transfert des entrées du journal. Vous pouvez spécifier jusqu'à 3 destinations de serveur syslog distinctes dans la configuration. Syslog distant constitue une cible de journal supplémentaire pour CMC. Lorsque vous avez configuré syslog distant, chaque nouvelle entrée de journal générée par CMC est transférée aux destinations.

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

Pour configurer les services CMC :

1. Ouvrez une session sur l'interface Web de CMC.
2. Cliquez sur l'onglet **Réseau**.
3. Cliquez sur le sous-onglet **Services**. La page **Services** s'affiche.

Pour plus d'informations sur la configuration de syslog distant, voir le [Tableau 5-56](#).

Fonctionnement de l'environnement CMC redondant

Vous pouvez installer un contrôleur CMC de secours qui prend la relève en cas de défaillance du contrôleur CMC actif. Le contrôleur CMC redondant peut être pré-installé ou ajouté à une date ultérieure. Il est important que le réseau de CMC soit correctement câblé pour assurer une redondance complète ou des performances optimales.

Un basculement peut survenir lorsque vous :

- 1 Exécutez la commande RACADM `cmcchangeover`. (Voir la section relative à la commande `cmcchangeover` du *Guide de référence de la ligne de commande pour iDRAC et CMC*.)
- 1 Exécutez la commande RACADM `racreset` sur le contrôleur CMC actif. (Voir la section relative à la commande `racreset` du *Guide de référence de la ligne de commande pour iDRAC et CMC*.)
- 1 Réinitialisez le contrôleur CMC actif à partir de l'interface Web. (Reportez-vous à l'option **Réinitialiser le contrôleur CMC** des **opérations de contrôle de l'alimentation** décrite dans la section [Exécution de tâches de contrôle de l'alimentation sur le châssis](#).)
- 1 Retirez le câble réseau du contrôleur CMC actif
- 1 Retirez le contrôleur CMC actif du châssis
- 1 Lancez un flash du micrologiciel CMC sur le contrôleur CMC actif
- 1 Disposez d'un contrôleur CMC actif qui n'est plus fonctionnel

 **REMARQUE** : en cas de basculement de CMC, toutes les connexions iDRAC et toutes les sessions CMC actives sont perdues. Les utilisateurs dont la session est perdue doivent se reconnecter au nouveau contrôleur CMC actif.

À propos du contrôleur CMC de secours

Le contrôleur CMC de secours est identique au contrôleur CMC actif et est maintenu comme un miroir de celui-ci. Les contrôleurs CMC actif et de secours doivent tous deux être installés avec la même révision du micrologiciel. Si les révisions du micrologiciel diffèrent, le système signale une dégradation de la redondance.

Le contrôleur CMC de secours prend en charge les mêmes paramètres et propriétés que le contrôleur actif. Vous devez maintenir la même version du micrologiciel sur les deux contrôleurs CMC mais vous n'avez pas à reproduire les paramètres de configuration sur le contrôleur CMC de secours.

 **REMARQUE** : pour des informations sur l'installation d'un contrôleur CMC de secours, consultez le *Manuel du propriétaire du matériel*. Pour des instructions sur l'installation du micrologiciel CMC sur votre CMC de secours, voir [Installation ou mise à jour du micrologiciel du module CMC](#).

Processus de sélection de CMC actif

Il n'existe aucune différence entre les deux logements CMC ; en d'autres termes, l'un ne prévaut pas sur l'autre. En effet, le contrôleur CMC qui est installé ou démarré le premier assume le rôle du contrôleur CMC actif. Si une alimentation alternative est appliquée aux deux contrôleurs CMC installés, le contrôleur CMC installé dans le logement CMC 1 du châssis (le gauche) assume normalement le rôle du contrôleur CMC actif. Le contrôleur CMC actif est signalé par une LED bleue.

Si deux contrôleurs CMC sont insérés dans un châssis qui est déjà sous tension, la négociation automatique active/de secours peut prendre jusqu'à deux minutes. Le fonctionnement normal du châssis est rétabli une fois la négociation terminée.

Obtention de la condition d'intégrité du contrôleur CMC redondant

Vous pouvez afficher la condition d'intégrité du contrôleur CMC de secours dans l'interface Web. Pour plus d'informations sur l'accès à la condition d'intégrité de CMC dans l'interface Web, voir [Affichage des résumés de châssis et composants](#).

[Retour à la page Contenu](#)

[Retour à la page Contenu](#)

Gestion de la structure d'E/S

Micrologiciel Dell Chassis Management Controller Version 3.1 Guide d'utilisation

- [Gestion de la structure](#)
- [Configurations non valides](#)
- [Scénario de nouveau démarrage](#)
- [Surveillance de l'intégrité des modules d'E/S](#)

Le châssis peut contenir jusqu'à six modules d'E/S, chacun pouvant être un module de commutation ou de transfert.

Ces modules d'E/S sont répartis en trois groupes : A, B et C. Chaque groupe comprend deux logements : 1 et 2. Les logements sont désignés par des lettres de gauche à droite à l'arrière du châssis : A1 | B1 | C1 | C2 | B2 | A2. Chaque serveur comporte des logements pour deux cartes mezzanine (MC) pour la connexion des modules d'E/S. La carte porteuse et le module d'E/S correspondant doivent avoir la même structure.

L'E/S de châssis est séparé en 3 chemins de données discrètes par lettre : A, B et C. Ces chemins sont décrits comme des « STRUCTURES » et prennent en charge Ethernet et Fibre Channel ou InfiniBand. Ces chemins de structure discrets sont répartis en « Banques » d'E/S, banque 1 et banque 2. Chaque adaptateur E/S de serveur (carte porteuse ou LOM) peut avoir 2 ou 4 ports selon la capacité. Ces ports sont répartis uniformément aux banques de modules d'E/S 1 et 2 pour permettre la redondance. Lorsque vous déployez vos réseaux Ethernet, iSCSI ou Fibre Channel, étendez leurs liens redondants sur les banques un et deux pour une disponibilité maximale. On indique le module discret avec l'identificateur de structure et le numéro de Banque.

Exemple : « A1 » indique structure « A » dans la banque « 1 ». « C2 » indique structure « C » dans la banque « 2 ».

Le châssis prend en charge trois structures ou types de protocole. Les modules d'E/S et les cartes mezzanine d'un groupe doivent comporter les mêmes types de structures ou des types compatibles.

- 1 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.
- 1 Pour le **groupe B**, les emplacements de module d'E/S sont en permanence connectés à la **première carte porteuse (MC)** dans chaque module de serveur.
- 1 Pour le **groupe C**, les emplacements de module d'E/S sont connectés en permanence à la **seconde carte porteuse (MC)** dans chaque module de serveur.

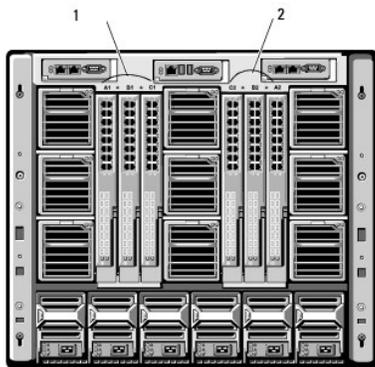
 **REMARQUE** : dans l'interface de ligne de commande CMC, les modules d'E/S sont désignés par la convention, switch-*n* : A1=switch-1, A2=switch-2, B1=switch-3, B2=switch-4, C1=switch-5 et C2=switch-6.

Gestion de la structure

La gestion de la structure permet d'éviter les problèmes d'ordre électrique, de configuration ou de connectivité lors de l'installation d'un module d'E/S ou d'une carte porteuse ayant une structure incompatible avec celle du châssis établi. Des configurations matérielles non valides peuvent provoquer des problèmes électriques ou de fonctionnement au niveau du châssis et de ses composants. La gestion de la structure empêche les configurations non valides d'être mises sous tension.

La [Figure 11-1](#) désigne l'emplacement du module d'E/S dans le châssis. L'emplacement de chaque module d'E/S est indiqué par son numéro de groupe (A, B ou C). Ces chemins de structure discrets sont divisés en deux banques, la banque 1 et la banque 2. Sur le châssis, les noms de logement des modules d'E/S sont indiqués par A1, A2, B1, B2, C1 ou C2.

Figure 11-1. Vue arrière d'un châssis illustrant 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 :

- 1 Une carte porteuse Ethernet connectée à un module d'E/S Fibre Channel n'est pas une configuration valide. Cependant, une carte porteuse Ethernet connectée à un commutateur Ethernet et à un module d'E/S de passerelle Ethernet installé dans le même groupe de module d'E/S est une connexion valide.
- 1 Un module d'E/S Fibre Channel de transfert et un commutateur d'E/S Fibre channel dans les logements B1 et B2 est une configuration valide si la première carte porteuse de tous les serveurs est également du type Fibre Channel. Dans ce cas, CMC met les modules d'E/S les serveurs sous tension. Cependant, certains logiciels de redondance Fibre Channel risquent de ne pas prendre en charge cette configuration : toutes les configurations valides ne sont pas nécessairement des configurations prises en charge.

 **REMARQUE** : la structure pour les modules d'E/S et les cartes porteuses du serveur est vérifiée uniquement à la mise sous tension du châssis. Lorsque le châssis est sur l'alimentation de secours, les micrologiciels iDRAC des modules du serveur restent éteints et ne peuvent donc pas signaler le type de structure des cartes porteuses du serveur. Le type de structure des cartes porteuses peut ne pas être signalé dans l'interface utilisateur CMC tant que le contrôleur iDRAC du serveur n'est pas mis sous tension. En outre, si le châssis est sous tension, la vérification de la structure est effectuée lorsqu'un serveur ou module d'E/S est inséré (en option). Si un décalage de structure est détecté, le serveur ou module d'E/S est autorisé à se mettre sous tension et le voyant de condition clignote en **orange**.

Configurations non valides

Il existe trois types de configurations non valides :

- 1 La configuration de cartes porteuses ou LOM non valide, où le type de structure d'un serveur récemment installé diffère de la structure du module d'E/S existant.
- 1 La configuration carte porteuse-module d'E/S non valide, où un module d'E/S récemment installé possède un type de structure différent ou est incompatible avec celui des cartes porteuses résidentes.
- 1 Une configuration module d'E/S-module d'E/S non valide, où un module d'E/S récemment installé possède un type de structure différent ou incompatible avec celui d'un module d'E/S déjà installé dans le groupe.

Configuration de cartes porteuses non valides

Une configuration de carte porteuse non valide survient dès qu'une seule carte porteuse ou LOM installée sur un serveur n'est pas prise en charge par le module d'E/S correspondant. Dans ce cas, tous les autres serveurs du châssis peuvent fonctionner, mais le serveur avec la carte porteuse discordante ne pourra pas être mis sous tension. Le bouton d'alimentation sur le serveur se met à clignoter orange pour indiquer un décalage de structure. Pour des informations sur CMC et les journaux de matériel, voir [Affichage des journaux d'événements](#).

Configuration de cartes porteuse de module d'E/S non valides

Le module d'E/S discordant sera maintenu hors tension. CMC ajoute une entrée aux journaux CMC et du matériel en indiquant la configuration non valide et en précisant le nom du module d'E/S. CMC déclenche le clignotement de la LED d'erreur du module d'E/S problématique. Si CMC est configuré pour envoyer des alertes, il envoie des alertes par e-mail et/ou SNMP pour cet événement. Pour des informations sur CMC et les journaux de matériel, voir [Affichage des journaux d'événements](#).

Configuration module d'E/S - module d'E/S non valide

CMC maintient le module d'E/S nouvellement installé hors tension, déclenche le clignotement de la LED d'erreur du module d'E/S et crée des entrées dans les journaux CMC et du matériel concernant cette non correspondance. Pour des informations sur CMC et les journaux de matériel, voir [Affichage des journaux d'événements](#).

Scénario de nouveau démarrage

Lorsque le châssis est branché et mis sous tension, les modules d'E/S ont priorité sur les serveurs. Le premier module d'E/S de chaque groupe est autorisé à démarrer avant les autres. À ce stade, aucune vérification du type de structure n'est effectuée. En l'absence d'un module d'E/S dans le premier logement d'un groupe, le module du deuxième logement de ce groupe démarre. Lorsque les deux logements comportent un module d'E/S, le module du deuxième logement est comparé à celui du premier afin d'en vérifier la cohérence.

Après démarrage des modules d'E/S, les serveurs démarrent et CMC vérifie la cohérence de la structure des serveurs.

Un module de transfert et un module de commutation sont autorisés dans le même groupe tant que leur structure est identique. Les modules de commutation et de transfert peuvent coexister dans un même groupe même s'ils sont fabriqués par des fournisseurs différents.

Surveillance de l'intégrité des modules d'E/S

Vous pouvez consulter la condition d'intégrité des modules d'E/S de deux manières : à partir de la section **Graphiques du châssis** sur la page **Condition du châssis** ou sur la page **Condition des modules d'E/S**. La page **Graphiques du châssis** fournit une représentation graphique des modules d'E/S installés dans le châssis.

Pour consulter la condition d'intégrité des modules d'E/S à l'aide des graphiques du châssis :

1. Ouvrez une session sur l'interface Web de CMC.

- La page **Condition du châssis** s'affiche. La section droite de la page **Graphiques du châssis** fournit une vue arrière du châssis et contient la condition d'intégrité des modules d'E/S. La condition d'intégrité du module d'E/S est indiquée par la couleur du graphique de module d'E/S :
 - Vert : le module d'E/S est présent, sous tension et communique avec CMC ; aucune indication d'événement indésirable.
 - Orange : le module d'E/S est présent, mais peut ne pas être sous tension ou peut ou ne pas communiquer avec CMC ; un événement indésirable peut exister.
 - Gris : le module d'E/S est présent et hors tension. Il ne communique pas avec CMC et il n'y a aucune indication d'événement indésirable.
- Placez le curseur sur un sous-graphique de module d'E/S pour afficher le champ textuel ou l'infobulle correspondant. Le champ textuel fournit des informations complémentaires sur le module d'E/S.
- Le lien hypertexte du sous-graphique de module d'E/S permet d'accéder à l'interface utilisateur CMC correspondante fournissant un accès direct vers la page **Condition des modules d'E/S** associée au module.

Pour consulter la condition d'intégrité de tous les modules d'E/S à l'aide de la page **Condition des modules d'E/S** :

- Ouvrez une session sur l'interface Web de CMC.
- Sélectionnez **Modules d'E/S** dans le menu **Châssis** de l'arborescence.
- Cliquez sur l'onglet **Propriétés**.
- Cliquez sur le sous-onglet **Condition**. La page **Condition des modules d'E/S** s'affiche.

Élément	Description	
Ordre de priorité	Indique l'emplacement du module d'E/S dans le châssis par numéro de groupe (A, B ou C) et banque (1 ou 2). Énumération de module d'E/S : A1, A2, B1, B2, C1 ou C2.	
Présent	Indique si le module d'E/S est présent (oui ou non).	
Intégrité		OK Indique que le module d'E/S est présent et communique avec CMC . En cas de perte des communications entre CMC et le serveur, CMC ne peut ni obtenir ni afficher la condition de l'intégrité du module d'E/S.
		Informatif Affiche des informations sur les modules d'E/S en l'absence de modification de la condition de l'intégrité (OK, Avertissement, Grave).
		Avertissement Indique que des alertes d'avertissement ont été émises et que des actions correctives doivent être effectuées . Si aucune action corrective n'est prise, des pannes critiques ou graves susceptibles d'affecter l'intégrité du module d'E/S pourraient se produire. Exemples de situations provoquant des avertissements : discordance de structure entre le module d'E/S et la structure de la carte mezzanine du serveur ; configuration de modules d'E/S non valide (où les modules d'E/S nouvellement installés ne correspondent pas aux modules d'E/S existants du même groupe).
		Grave Indique qu'au moins une alerte de panne a été générée. La condition Grave représente une panne système du module d'E/S et des actions correctives doivent être effectuées immédiatement . Exemples de situations provoquant une condition Grave : détection d'une panne d'un module d'E/S ; retrait d'un module d'E/S.
	REMARQUE : toute modification de l'intégrité est consignée dans les journaux du matériel et CMC. Pour plus d'informations, voir Affichage des journaux d'événements .	
Structure	Indique le type de structure du module d'E/S : Gigabit Ethernet, 10GE XAU1, 10GE KR, 10GE XAU1 KR, FC 4 Gb/s, FC 8 Gb/s, SAS 3 Gb/s, SAS 6 Gb/s, Infiniband SDR, Infiniband	

	<p>DDR, Infiniband QDR, Interconnexion PCIe 1ère génération, Interconnexion PCIe 2ème génération.</p> <p>REMARQUE : le fait de connaître les types de structure des modules d'E/S de votre châssis permet d'éviter des dissociations de modules d'E/S au sein d'un même groupe. Pour des informations sur la structure E/S, voir Gestion de la structure d'E/S.</p>
Nom	Affiche le nom de produit du module.
Lancer la console de gestion des modules d'E/S	<p> Si l'icône d'un module d'E/S spécifique est présente, le fait de cliquer dessus lance la console de gestion de ce module d'E/S dans une nouvelle fenêtre de navigateur ou sous un nouvel onglet.</p> <p>REMARQUE : cette option est uniquement disponible pour les modules d'E/S de commutateurs gérés. Elle n'est pas disponible pour les modules de transfert d'E/S ou pour les commutateurs Infiniband non gérés.</p> <p>REMARQUE : si un module d'E/S est inaccessible car il est hors tension, si son interface de réseau local est désactivée ou qu'une adresse IP valide n'a pas été assignée au module, alors l'option Lancer l'interface utilisateur de module d'E/S n'est pas affichée pour ce module d'E/S.</p> <p>REMARQUE : il vous est alors demandé d'ouvrir une session dans l'interface de gestion du module d'E/S.</p> <p>REMARQUE : vous pouvez configurer l'adresse IP du module d'E/S par l'intermédiaire de l'interface utilisateur de CMC, comme décrit dans Configuration des paramètres réseau pour un module d'E/S spécifique.</p>
Rôle	Quand les modules d'E/S sont liés ensemble, le Rôle affiche la hiérarchisation de modules d'E/S. Membre : le module fait partie d'un ensemble de piles. Maître : le module est un point d'accès principal.
État de l'alimentation	Indique la condition de l'alimentation du module d'E/S : sous tension , hors tension ou - (absente).
Numéro de service	<p>Affiche le numéro de service du module d'E/S. Le numéro de service est un identifiant unique fourni par Dell pour le support et la maintenance.</p> <p>Toute modification de l'intégrité est consignée dans les journaux du matériel et CMC. Pour plus d'informations, voir Affichage des journaux d'événements.</p> <p>REMARQUE : les transferts n'ont pas de numéros de service. Seuls les commutateurs en possèdent.</p>

Affichage de la condition d'intégrité d'un module d'E/S spécifique

La page **Condition du module d'E/S** (distincte de la page **Condition des modules d'E/S**) fournit un aperçu d'un module d'E/S spécifique.

Pour afficher la condition d'intégrité d'un module d'E/S spécifique :

1. Ouvrez une session sur l'interface Web de CMC.
2. Développez **Modules d'E/S** dans l'arborescence du système. Tous les modules d'E/S (1 à 6) s'affichent dans la liste **Modules d'E/S** développée.
3. Cliquez sur le module d'E/S que vous souhaitez afficher dans la liste **Modules d'E/S** de l'arborescence du système.
4. Cliquez sur le sous-onglet **Condition**. La page **Condition des modules d'E/S** s'affiche.

--	--

Élément	Description	
Emplacement	Indique l'emplacement d'un module d'E/S dans le châssis par numéro de groupe (A, B ou C) et numéro de logement (1 ou 2). Noms de logement : A1, A2, B1, B2, C1 ou C2.	
Nom	Affiche le nom du module d'E/S.	
Présent	Indique si le module d'E/S est Présent ou Absent .	
Intégrité	 OK 	Indique que le module d'E/S est présent et communique avec CMC. En cas de perte des communications entre CMC et le serveur, CMC ne peut ni obtenir ni afficher la condition de l'intégrité du module d'E/S.
	 Informatif	Affiche des informations sur les modules d'E/S en l'absence de modification de la condition de l'intégrité (OK, Avertissement, Grave). Exemples de situations provoquant une condition Informative : la présence du module d'E/S a été détectée ; un utilisateur a demandé un cycle d'alimentation du module d'E/S.
	 Avertissement	Indique que des alertes d'avertissement ont été émises et que des actions correctives doivent être effectuées . Si aucune action corrective n'est prise, des pannes critiques ou graves susceptibles d'affecter l'intégrité du module d'E/S pourraient se produire. Exemples de situations provoquant des avertissements : discordance de structure entre le module d'E/S et la structure de la carte mezzanine du serveur ; configuration de modules d'E/S non valide, dans laquelle les modules d'E/S récemment installés ne correspondent pas aux modules d'E/S existants du même groupe.
	 Grave	Indique qu'au moins une alerte de panne a été générée. La condition Grave représente une panne système du module d'E/S et des actions correctives doivent être effectuées immédiatement . Exemples de situations provoquant une condition Grave : détection d'une panne d'un module d'E/S ; retrait d'un module d'E/S.
	REMARQUE : toute modification de l'intégrité est consignée dans les journaux du matériel et CMC. Pour des informations sur l'affichage des journaux, voir Affichage du journal du matériel et Affichage du journal CMC .	
État de l'alimentation	Indique la condition de l'alimentation du module d'E/S : sous tension , hors tension ou - (absente).	
Numéro de service	Affiche le numéro de service du module d'E/S. Le numéro de service est un identifiant unique fourni par Dell pour le support et la maintenance.	
Structure	Indique le type de structure du module d'E/S : Gigabit Ethernet, 10GE XAUI, 10GE KR, 10GE XAUI KR, FC 4 Gb/s, FC 8 Gb/s, SAS 3 Gb/s, SAS 6 Gb/s, Infiniband SDR, Infiniband DDR, Infiniband QDR, Interconnexion PCIe 1ère génération, Interconnexion PCIe 2ème génération. REMARQUE : le fait de connaître les types de structure des modules d'E/S de votre châssis permet d'éviter des dissociations de modules d'E/S au sein d'un même groupe. Pour des informations sur la structure E/S, voir Gestion de la structure d'E/S .	
MAC Address (Adresse Mac)	Affiche l'adresse MAC du module d'E/S. L'adresse MAC est une adresse unique attribuée à un périphérique par le fournisseur du matériel à des fins d'identification. REMARQUE : les transferts n'ont pas d'adresses MAC. Seuls les commutateurs possèdent une adresse MAC.	
Rôle	Affiche l'adhésion à l'empilage du module d'E/S lorsque les modules sont reliés : <ul style="list-style-type: none"> ○ Membre : le module fait partie d'un ensemble de piles. 	

- o **Maître** : le module est un point d'accès principal.

Configuration des paramètres réseau pour un module d'E/S spécifique

La page Configuration des modules d'E/S vous permet de spécifier les paramètres réseau pour l'interface utilisée pour gérer le module d'E/S. Le port de gestion hors bande (adresse IP) est configuré pour les commutateurs Ethernet. Le port de gestion intra-bande (VLAN1) n'est pas configuré via cette interface.

-  **REMARQUE** : pour modifier des paramètres dans la page Configuration des modules d'E/S, vous devez posséder des privilèges administrateur : de la structure A afin de configurer le groupe A des modules d'E/S ; de la structure B afin de configurer la groupe B des modules d'E/S ; ou de la structure C afin de configurer le groupe C des modules d'E/S.
-  **REMARQUE** : concernant les commutateurs Ethernet, les adresses IP de gestion hors bande et intra-bande (VLAN1) ne peuvent pas être identiques ni se trouver sur le même réseau ; cette configuration empêcherait toute définition de l'adresse IP de gestion hors bande. Pour plus d'informations sur l'adresse IP de gestion intra-bande par défaut, reportez-vous à la documentation du module d'E/S.
-  **REMARQUE** : seuls les modules d'E/S présents dans le châssis s'affichent.
-  **REMARQUE** : ne tentez pas de configurer les paramètres réseau du module d'E/S pour le module d'intercommunication Ethernet ou les commutateurs Infiniband.

Pour configurer les paramètres réseau d'un module d'E/S spécifique :

1. Ouvrez une session sur l'interface Web de CMC.
2. Développez **Modules d'E/S** dans l'arborescence du système. Cliquez sur le sous-onglet **Configuration**. La page **Configuration des paramètres réseau des modules d'E/S** s'affiche.
3. Pour configurer les paramètres réseau des modules d'E/S, entrez/sélectionnez les valeurs des propriétés suivantes, puis cliquez sur **Appliquer**.

-  **REMARQUE** : seuls les modules d'E/S sous tension peuvent être configurés.
-  **REMARQUE** : l'adresse IP définie sur les modules d'E/S à partir de CMC n'est pas enregistrée dans la configuration permanente de démarrage du commutateur. Pour enregistrer l'adresse IP de manière permanente, entrez la commande `connect switch-n` ou la commande `racadm connect switch -n RACADM`, ou bien utilisez une interface directe de l'interface utilisateur du module d'E/S afin d'enregistrer l'adresse dans le fichier de configuration de démarrage.

Élément	Description
Ordre de priorité	Indique l'emplacement d'un module d'E/S dans le châssis par numéro de groupe (A, B ou C) et numéro de logement (1 ou 2). Noms de logement : A1, A2, B1, B2, C1 ou C2. (La valeur du logement ne peut pas être modifiée.)
Nom	Affiche le nom de produit du module. (Le nom du module d'E/S ne peut pas être modifié.)
État de l'alimentation	Affiche l'état d'alimentation du module d'E/S. (L'état d'alimentation ne peut pas être modifié depuis cette page.)
DHCP activé	Permet au module d'E/S du châssis de demander et d'obtenir automatiquement une adresse IP auprès du serveur DHCP (protocole de configuration dynamique des hôtes). Par défaut : coché (activé). Si cette option est cochée, le module d'E/S récupère automatiquement la configuration IP (adresse IP, masque de sous-réseau et passerelle) auprès d'un serveur DHCP de votre réseau. REMARQUE : lorsque cette fonctionnalité est activée, les champs des propriétés Adresse IP, Passerelle et Masque de sous-réseau (situés en regard de cette option) sont désactivés et les valeurs précédemment saisies pour ces propriétés sont ignorées. Si cette option n'est pas cochée, vous devez saisir manuellement une adresse IP valide, une passerelle et un masque de sous-réseau dans les champs de texte correspondants situés juste en dessous de cette option.
Adresse IP	Indique l'adresse IP de l'interface réseau du module d'E/S.
Masque de sous-réseau	Indique le masque de sous-réseau de l'interface réseau du module d'E/S.
Passerelle	Indique la passerelle de l'interface réseau du module d'E/S.

Dépannage des paramètres réseau de module d'E/S

La liste suivante contient les éléments de dépannage pour les paramètres réseau de module d'E/S :

- 1 CMC peut lire le paramètre d'adresse IP après une modification de la configuration. Il affiche 0.0.0.0 une fois que vous avez cliqué sur **Appliquer**. Cliquez sur le bouton Actualiser pour voir si l'adresse IP est correctement définie sur le commutateur.
- 1 Si vous ne définissez pas correctement l'adresse IP, le masque ou la passerelle, le commutateur ne définit pas l'adresse IP et rétablit tous les champs sur 0.0.0.0. Erreurs les plus courantes :
 - 1 Les adresses IP de gestion hors bande et intra-bande sont identiques ou configurées sur le même réseau.
 - 1 Le masque de sous-réseau n'est pas valide.
 - 1 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 de module d'E/S, reportez-vous au document *Dell PowerConnect M6220 Switch Important Information* et au livre blanc *Dell PowerConnect 6220 Series Port Aggregator*.

[Retour à la page Contenu](#)

[Retour à la page Contenu](#)

Présentation

Micrologiciel Dell Chassis Management Controller Version 3.1 Guide d'utilisation

- [Nouveautés de cette version](#)
- [Fonctionnalités de gestion de CMC](#)
- [Fonctionnalités de sécurité](#)
- [Présentation du châssis](#)
- [Caractéristiques matérielles](#)
- [Connexions d'accès à distance prises en charge](#)
- [Plateformes prises en charge](#)
- [Navigateurs Web pris en charge](#)
- [Applications de console de gestion prises en charge](#)
- [Prise en charge WS-Management](#)
- [Autres documents utiles](#)

Dell Chassis Management Controller (CMC) est une solution matérielle et logicielle de gestion de systèmes enfichable à chaud, conçue pour fournir des fonctionnalités de gestion à distance et de contrôle de l'alimentation pour les systèmes de châssis Dell PowerEdge M1000e.

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.

Le module CMC qui possède son propre microprocesseur et sa propre mémoire, est alimenté par le châssis modulaire sur lequel il est branché. Pour démarrer avec CMC, voir [Installation et configuration de CMC](#).

Nouveautés de cette version

Cette version de CMC prend en charge les fonctionnalités suivantes :

- 1 Gestion de plusieurs châssis. Celle-ci permet à jusqu'à 8 autres châssis d'être visibles depuis le châssis chef.
- 1 Journalisation de l'alimentation. Celle-ci permet à l'utilisateur de recueillir des mesures de consommation électrique et de les journaliser sur un serveur distant.
- 1 Enregistrement et restauration de la configuration sur un hôte.
- 1 Optimisation d'un journal SEL.
- 1 Conforme à GPL/Open source.
- 1 Fibre Channel Dell 8/4Gbit/s via le module d'E/S.
- 1 Module d'E/S Dell M8428-k.
- 1 Carte Mezzanine double-port Brocade BR1741M-k.
- 1 Performances du serveur contre mode de redondance de l'alimentation pour la gestion de l'alimentation.

Fonctionnalités de gestion de CMC

CMC dispose des fonctionnalités de gestion suivantes :

- 1 Environnement CMC redondant.
- 1 Enregistrement du système de noms de domaine dynamique (DDNS) pour IPv4 et IPv6.
- 1 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.
- 1 Prise en charge de l'authentification Microsoft Active Directory : centralise les identifiants et les mots de passe des utilisateurs CMC dans Active Directory à l'aide du schéma standard ou d'un schéma étendu.
- 1 Surveillance : permet d'accéder aux informations sur le système et à la condition des composants.
- 1 Accès aux journaux des événements système : accès au journal du matériel et au journal CMC.
- 1 Mises à jour du micrologiciel pour les différents composants : permet de mettre à jour le micrologiciel pour CMC, les serveurs, le module iKVM, et les dispositifs d'infrastructure de module d'E/S.
- 1 Intégration du logiciel Dell OpenManage : permet de lancer l'interface Web CMC à partir de Dell OpenManage Server Administrator ou d'IT Assistant.
- 1 Alertes CMC : vous avertit des problèmes potentiels du nud géré au moyen d'un message électronique ou d'une interruption SNMP.
- 1 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.
- 1 Rapport sur l'alimentation.
- 1 Cryptage SSL (Secure Sockets Layer) : permet une gestion sécurisée du système distant via l'interface Web.
- 1 Gestion de la sécurité de niveau mot de passe : empêche tout accès non autorisé à un système distant.
- 1 Autorisation basée sur le rôle : permet d'attribuer des droits pour diverses tâches de gestion de systèmes.
- 1 Point de lancement de l'interface Web Integrated Dell Remote Access Controller (iDRAC).
- 1 Prise en charge de la gestion WS.

- 1 Fonctionnalité FlexAddress : remplace les ID de nom mondial/Media Access Control (WWN/MAC) d'usine par les ID WWN/MAC de châssis pour un emplacement spécifique ou une mise à jour optionnelle. Pour plus d'informations, voir [Utilisation de FlexAddress](#).
- 1 Affichage graphique de la condition et de l'intégrité du composant de châssis.
- 1 Prise en charge des serveurs à connecteur unique ou multiple.
- 1 Mise à jour de plusieurs micrologiciels de consoles de gestion iDRAC simultanément.
- 1 L'assistant de configuration iDRAC LCD prend en charge la configuration réseau iDRAC.
- 1 Connexion unique iDRAC.
- 1 Prise en charge du protocole de temps du réseau (NTP).
- 1 Pages de résumé du serveur, de rapports de l'alimentation et de contrôle de l'alimentation améliorées.
- 1 Basculement CMC forcé et réattribution de sièges virtuelle de serveurs.
- 1 Gestion de plusieurs châssis. Celle-ci permet à jusqu'à 8 autres châssis d'être visibles depuis le châssis chef.

Fonctionnalités de sécurité

CMC dispose des fonctionnalités de sécurité suivantes :

- 1 Authentification des utilisateurs via Active Directory (en option) ou via les ID d'utilisateur et les mots de passe stockés sur le matériel
- 1 Autorité basée sur le rôle qui permet à un administrateur de configurer des privilèges spécifiques pour chaque utilisateur
- 1 Configuration des réf. utilisateur et des mots de passe via l'interface Web
- 1 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)

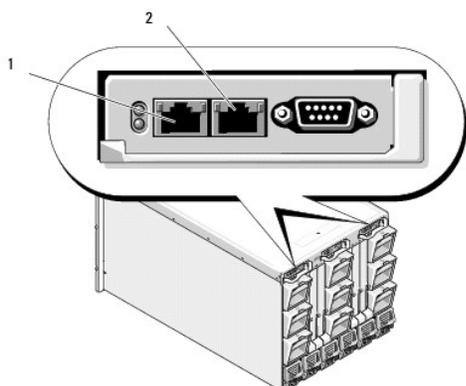
 **REMARQUE** : Telnet ne prend pas en charge le cryptage SSL.

- 1 Ports IP configurables (si applicable)
- 1 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
- 1 Délai de session configurable, et plus d'une session simultanée
- 1 Plage d'adresses IP limitée pour les clients se connectant à CMC
- 1 Secure Shell (SSH) qui utilise une couche cryptée pour une sécurité plus élevée
- 1 Connexion directe, authentification bifactorielle et authentification par clé publique

Présentation du châssis

La [Figure 1-1](#) illustre la face avant d'une carte CMC (installée) et les emplacements des logements CMC dans le châssis.

Figure 1-1. Châssis Dell M1000e et CMC



1	Port GB	2	Port STK
---	---------	---	----------

Caractéristiques matérielles

Ports TCP/IP

Vous devez fournir les informations du port lorsque vous ouvrez des pare-feu pour l'accès à distance à un module CMC.

Tableau 1-1. Ports d'écoute des serveurs CMC

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

Tableau 1-2. Port 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	

Connexions d'accès à distance prises en charge

Tableau 1-3. Connexions d'accès à distance prises en charge

Connexion	Fonctionnalités
Ports d'interface réseau CMC	<ul style="list-style-type: none">1 Deux ports 10/100 Go, un pour la gestion et l'autre pour la consolation câble châssis à châssis1 Ethernet 10 Mbits/100 Mbits/ 1 Mbits sur port GbE CMC1 Prise en charge de DHCP1 Interruptions SNMP et notifications d'événements par e-mail1 Port GB : interface réseau dédiée pour l'interface Web CMC1 STK : port Uplink pour consolation câble réseau de gestion châssis à châssis1 Interface réseau pour le micrologiciel iDRAC et les modules d'E/S1 Prise en charge de la console de commande Telnet/SSH et des commandes de l'interface de ligne de commande RACADM, y compris les commandes d'amorçage du système, de réinitialisation, de mise sous tension et d'arrêt
Port série	<ul style="list-style-type: none">1 Prise en charge de la console série et des commandes CLI RACADM, y compris les commandes de démarrage du système, de réinitialisation, de mise sous tension et d'arrêt1 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/S1 Le port série peut être connecté à la console série d'un serveur ou à un module d' E/S à l'aide de la commande connect (ou racadm connect)
Autres connexions	<ul style="list-style-type: none">1 Accès à la console Dell CMC via le module de commutation KVM intégré (iKVM) Avocent

Plateformes prises en charge

CMC prend en charge les systèmes modulaires conçus pour la plateforme M1000e. Pour des informations concernant la compatibilité avec CMC, consultez la documentation de votre périphérique.

Pour connaître les systèmes d'exploitation et les navigateurs Web pris en charge, consultez la *Matrice de prise en charge logicielle des systèmes Dell* sur le site Web de support de Dell à l'adresse support.dell.com/manuals.

Navigateurs Web pris en charge

Les navigateurs Web suivants sont pris en charge par CMC3.1 :

- 1 Microsoft Internet Explorer 8.0 pour Windows 7, Windows Vista, Windows XP et Windows Server 2003.
- 1 Microsoft Internet Explorer 7.0 pour Windows 7, Windows Vista, Windows XP et Windows Server 2003.
- 1 Mozilla Firefox 1.5 (32-bit) (fonctionnalité limitée).

Pour les dernières informations relatives aux navigateurs Web pris en charge, consultez la *Matrice de prise en charge des logiciels des systèmes Dell* sur le site Web du support de Dell à l'adresse support.dell.com/manuals.

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

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

Applications de console de gestion prises en charge

CMC prend en charge l'intégration de Dell OpenManage IT Assistant. Pour plus d'informations, reportez-vous au jeu de documentation d'IT Assistant disponible sur le site Web du support de Dell à l'adresse support.dell.com/manuals.

Prise en charge WS-Management

Web Services for Management (WS-MAN) est un protocole basé sur SOAP (protocole simplifié d'accès aux objets) utilisé pour la gestion des systèmes. WS-MAN fournit un protocole interopérable pour les périphériques afin de partager et d'échanger des données sur les réseaux. CMC utilise WS-MAN pour transmettre les informations de gestion CIM-DMTF. Les informations CIM définissent la sémantique et les types d'informations qui peuvent être manipulés dans un système géré. Les interfaces de gestion de plate-forme de serveurs intégrées à Dell sont organisées en profils où chaque profil définit les interfaces spécifiques d'un domaine de gestion particulier ou la zone de fonctionnalité. En outre, Dell a défini plusieurs extensions de modèle et de profil qui fournissent des interfaces pour des capacités supplémentaires.

L'accès à WS-Management nécessite d'ouvrir une session à l'aide des privilèges d'utilisateur local au moyen d'une authentification de base sur le protocole SSH (Secured Socket Layer) au port 443. Pour des informations supplémentaires sur la configuration de comptes utilisateurs, voir la section Propriétés de la bases de données de la gestion de sessions du *Guide de référence de la ligne de commande pour iDRAC6 et CMC*.

Les données disponibles via WS-Management constituent un sous-ensemble de données fournies par l'interface d'instrumentation CMC mise en correspondance avec les profils DMTF suivants (version 1.0.0) :

- 1 Profil d'allocations de fonctionnalités
- 1 Profil des mesures de base
- 1 Profil du serveur de base
- 1 Profil du système informatique
- 1 Profil du système modulaire
- 1 Profil des actifs physiques
- 1 Profil d'allocation de l'alimentation Dell
- 1 Profil du bloc d'alimentation Dell
- 1 Profil de la topologie d'alimentation Dell
- 1 Profil de gestion de l'état de l'alimentation
- 1 Profil d'enregistrement du profil
- 1 Profil du journal des enregistrements
- 1 Profil d'allocation des ressources

- 1 Profil d'autorisation basée sur les rôles
- 1 Profil des capteurs
- 1 Profil des processeurs de services
- 1 Profil de gestion simple de l'identité
- 1 Profil de client Dell Active Directory
- 1 Profil de contrôle de l'amorçage
- 1 Profil de carte réseau simplifié de Dell

La mise en œuvre WS-MAN CMC utilise SSL sur le port 443 pour sécuriser le transport et prend en charge l'authentification de base. Pour des informations supplémentaires sur la configuration de comptes utilisateurs, voir la section Propriétés de la bases de données de la gestion de sessions du *Guide de référence de la ligne de commande pour iDRAC6 et CMC*. Les interfaces des services Web peuvent être utilisées en exploitant l'infrastructure client, comme Windows WinRM et l'interface de ligne de commande Powershell, les utilitaires open source comme WSMANCLI et les environnements de programmation d'application comme Microsoft .NET.

Pour la connexion client à l'aide de Microsoft WinRM, la version minimale requise est 2.0. Pour plus d'informations, consultez l'article **Microsoft** <<http://support.microsoft.com/kb/968929>>.

Le Centre technique de Dell contient des guides de mise en œuvre supplémentaires, des livres blancs, des profils et des exemples de codes à l'adresse www.delltechcenter.com. Pour plus d'informations, voir :

- 1 Le site Web DMTF : www.dmtf.org/standards/profiles/
- 1 Notes de mise à jour ou fichier « Lisez-moi » de WS-MAN.
- 1 www.wbemsolutions.com/ws_management.html
- 1 Spécifications DMTF WS-Management : www.dmtf.org/standards/wbem/wsman

Autres documents utiles

Outre ce Guide d'utilisation, les guides suivants se trouvent sur le site Web du support de Dell à l'adresse support.dell.com/manuals. Sur la page **Manuels**, cliquez sur → **Gestion de systèmes**. Cliquez sur le lien du produit approprié sur le côté droit pour accéder aux documents :

- 1 L'*aide en ligne de CMC* fournit des informations sur l'utilisation de l'interface Web.
- 1 Les *caractéristiques techniques de la carte Secure Digital de CMC* fournissent une version du micrologiciel et un BIOS minimum, plus des informations sur son installation et son utilisation.
- 1 Le *Guide d'utilisation d'Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise pour les serveurs lames* fournit des informations concernant l'installation, la configuration et la maintenance d'iDRAC sur les systèmes gérés.
- 1 Le *Guide d'utilisation de Dell OpenManage IT Assistant* fournit des informations relatives à IT Assistant.
- 1 Documentation spécifique à votre application tierce de console de gestion.
- 1 Le *Guide d'utilisation de Dell OpenManage Server Administrator* donne des informations sur l'installation et l'utilisation de Server Administrator.
- 1 Le *Guide d'utilisation des progiciels Dell Update Package* fournit des informations sur l'obtention et l'utilisation des progiciels Dell Update Package dans le cadre de la stratégie de mise à jour de votre système.

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

- 1 les instructions de sécurité fournies avec votre système contiennent d'importantes informations se rapportant à la sécurité et à la réglementation. Pour obtenir des informations supplémentaires sur la réglementation, voir la page d'accueil Regulatory Compliance (Conformité à la réglementation) à l'adresse www.dell.com/regulatory_compliance. Les informations sur la garantie se trouvent dans ce document ou dans un document distinct.
- 1 Les documents *Guide d'installation du rack* et *Instructions d'installation du rack* fournis avec la solution rack décrivent l'installation du système.
- 1 Le *Manuel du propriétaire du matériel* présente les fonctionnalités du système et contient des informations de dépannage du système et des instructions d'installation ou de remplacement des composants du système.
- 1 La documentation relative aux logiciels de gestion de systèmes décrit les fonctionnalités, la configuration requise, l'installation et l'utilisation de base du logiciel.
- 1 La documentation fournie avec les composants achetés séparément indique comment configurer et installer ces options.
- 1 Les notes de version 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.
- 1 Pour plus d'informations sur les paramètres réseau de module d'E/S, reportez-vous au document *Dell PowerConnect M6220 Switch Important Information* et au livre blanc *Dell PowerConnect 6220 Series Port Aggregator*.

Des mises à jour sont parfois fournies avec le système pour décrire les modifications apportées au système, au logiciel et/ou à la documentation. Lisez toujours les mises à jour en premier, car elles remplacent souvent les informations contenues dans d'autres documents.

[Retour à la page Contenu](#)

[Retour à la page Contenu](#)

Power Management (Gestion de l'alimentation)

Micrologiciel Dell Chassis Management Controller Version 3.1 Guide d'utilisation

- [Présentation](#)
- [Règles de redondance](#)
- [Configuration et gestion de l'alimentation](#)

Présentation

L'enceinte du serveur Dell PowerEdge M1000e est le serveur modulaire à plus faible consommation énergétique du marché. Elle a été conçue pour inclure des blocs d'alimentation et des ventilateurs haute performance, possède une disposition optimisée afin que l'air circule plus facilement à travers le système et comporte des composants à faible consommation énergétique répartis dans l'enceinte. La conception matérielle optimisée est conjuguée à des capacités de gestion de l'alimentation sophistiquées intégrées dans Chassis Management Controller (CMC), des blocs d'alimentation et iDRAC pour vous permettre d'améliorer davantage la gestion de l'alimentation et d'avoir un contrôle total sur votre environnement d'alimentation.

L'enceinte modulaire PowerEdge M1000e est alimentée alternative et distribue la charge sur toutes les unités d'alimentation internes actives. Le système peut délivrer jusqu'à 11 637 watts d'alimentation alternative allouée aux modules de serveurs et à l'infrastructure d'enceinte associée.

REMARQUE : la puissance de sortie réelle est basée sur la configuration et la charge de travail.

Les fonctionnalités de gestion de l'alimentation du châssis M1000e aident les administrateurs à configurer l'enceinte afin de réduire la consommation électrique et à adapter la gestion de l'alimentation à leurs besoins et environnements uniques.

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.

Mode de redondance de l'alimentation alternative

La règle de redondance de l'alimentation alternative vise à permettre à un système d'enceinte modulaire de fonctionner dans un mode dans lequel il peut tolérer des pannes d'alimentation alternative. Ces pannes peuvent provenir du réseau d'alimentation alternative, du câblage et de la distribution, ou d'une unité d'alimentation elle-même.

Lorsque vous configurez un système pour une redondance alternative, les unités d'alimentation sont divisées en réseaux : les unités d'alimentation dans les logements 1, 2 et 3 sont dans le premier réseau tandis que les unités d'alimentation dans les logements 4, 5 et 6 sont dans le deuxième réseau. Le contrôleur CMC gère l'alimentation de sorte qu'en cas de défaillance d'un réseau le système continue à fonctionner sans dégradation. La redondance d'alimentation alternative tolère également les pannes des unités d'alimentation individuelles.

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.

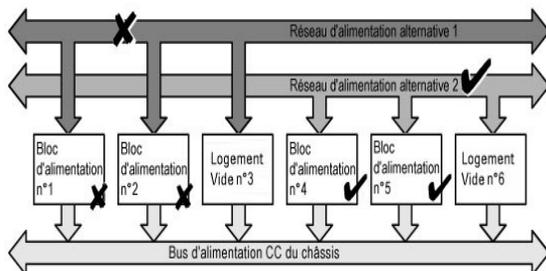
REMARQUE : la redondance d'alimentation alternative n'est atteinte que lorsque les conditions de charge ne dépassent pas la capacité du réseau ayant la plus faible puissance.

Niveaux de redondance d'alimentation alternative

La configuration minimum est une unité d'alimentation dans chaque réseau pour la redondance d'alimentation alternative. D'autres configurations sont possibles avec toutes les combinaisons qui ont au moins une unité d'alimentation dans chaque réseau. Cependant, pour rendre disponible la puissance maximale, la puissance totale des unités d'alimentation dans chaque colonne doit être aussi égale que possible. La limite maximale de la puissance tout en conservant la redondance d'alimentation alternative est la puissance disponible sur le plus faible des deux réseaux.

Si pour une raison quelconque CMC est incapable de maintenir la redondance d'alimentation alternative, les alertes E-mail et/ou SNMP sont envoyées aux administrateurs si l'événement Redondance perdue est configuré pour les alertes.

Figure 9-1. 2 unités d'alimentation par réseau et une panne électrique sur le réseau 1



REMARQUE : En cas de panne d'une seule unité d'alimentation dans cette configuration, les deux unités d'alimentation restantes dans le réseau défaillant sont marquées comme En ligne. L'une des unités d'alimentation restantes peut alors tomber en panne sans interrompre le fonctionnement du système. En cas de panne d'une unité d'alimentation, l'intégrité du châssis est marquée comme Non critique. Si le réseau plus petit ne peut pas prendre en charge la totalité des allocations d'alimentation du châssis, la condition de la redondance d'alimentation alternative est rapportée comme Sans redondance et l'intégrité du châssis est affichée comme Critique.

Mode de redondance des blocs d'alimentation

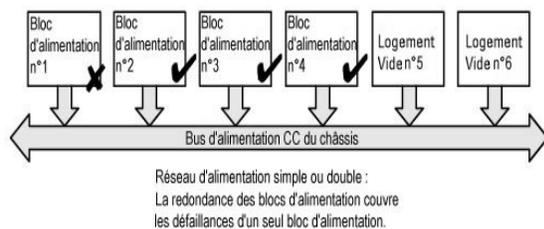
Le mode de redondance des blocs d'alimentation est utile lorsque des réseaux d'alimentation redondants ne sont pas disponibles, mais que vous souhaitez être protégé en cas de panne d'une seule unité d'alimentation entraînant l'arrêt de vos serveurs dans une enceinte modulaire. L'unité d'alimentation ayant la plus haute capacité est gardée en ligne à cette fin. Ceci forme un pool de redondance des 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 : L'enclenchement dynamique des blocs d'alimentation (DPSE) permet de mettre des unités d'alimentation en veille. L'état de veille indique un état physique où l'alimentation n'est pas fournie. Lorsque vous activez l'enclenchement dynamique des blocs d'alimentation, les unités d'alimentation supplémentaires sont mises en mode veille pour accroître l'efficacité et économiser de l'énergie.

Figure 9-2. Alimentation redondante : 4 blocs d'alimentation au total avec un bloc d'alimentation en panne



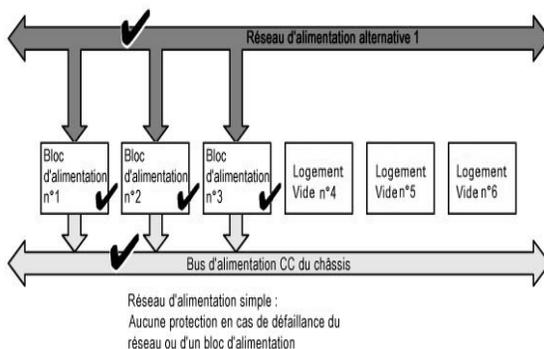
Mode Sans redondance

Le mode **Sans redondance** est le paramètre d'usine de la configuration à 3 unités d'alimentation et indique qu'aucune redondance de l'alimentation n'est configurée pour le châssis. Dans cette configuration, la condition générale de la redondance du châssis indique toujours **Sans redondance**.

CMC n'a pas besoin que les unités d'alimentation soient présentes dans des positions de logement spécifiques lorsqu'aucune redondance n'est configurée.

REMARQUE : toutes les unités d'alimentation dans le châssis sont répertoriées comme étant **En ligne** si l'enclenchement dynamique des blocs d'alimentation est désactivé en mode **Sans redondance**. Lorsque l'enclenchement dynamique des blocs d'alimentation est activé, tous les blocs d'alimentation actifs dans le châssis sont répertoriés comme **En ligne** et les unités d'alimentation supplémentaires peuvent être mises en mode **Veille** pour augmenter l'efficacité du système.

Figure 9-3. Sans redondance avec trois unités d'alimentation dans le châssis



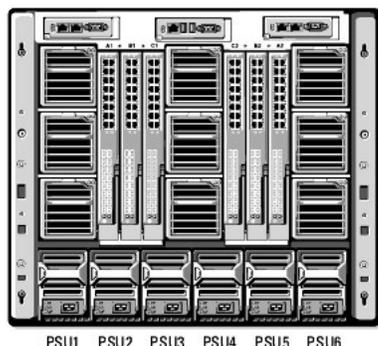
Lorsqu'une unité d'alimentation est en panne, les autres unités d'alimentation quittent le mode veille, selon les besoins, afin de prendre en charge les allocations d'alimentation du châssis. Si vous avez 4 blocs d'alimentation, et n'en avez besoin que de trois, alors dans le cas où l'un des blocs tombe en panne, le quatrième bloc est mis en ligne. Un châssis peut avoir les 6 unités d'alimentation en ligne.

Lorsque vous activez l'enclenchement dynamique des blocs d'alimentation, les unités d'alimentation supplémentaires sont mises en mode veille pour accroître l'efficacité et économiser de l'énergie. Pour plus d'informations, voir [Enclenchement dynamique des blocs d'alimentation](#).

Bilan de puissance pour les modules matériels

La [Figure 9-4](#) illustre un châssis contenant une configuration à six unités d'alimentation. Les unités d'alimentation portent les nombres 1 à 6, en commençant par le côté gauche de l'enceinte.

Figure 9-4. Châssis doté de six unités d'alimentation



CMC maintient un bilan de puissance de l'enceinte qui réserve la puissance nécessaire pour tous les serveurs et composants installés.

CMC alloue l'alimentation à l'infrastructure CMC et aux serveurs dans le châssis. L'infrastructure CMC comprend les composants du châssis tels que les ventilateurs, les modules d'E/S et iKVM (si celui-ci est présent). Le châssis peut comporter jusqu'à 16 serveurs qui communiquent avec le châssis par le biais d'iDRAC. Pour plus d'informations, consultez le *Guide d'utilisation d'iDRAC* à l'adresse support.dell.com/manuals.

iDRAC fournit à CMC son enveloppe d'alimentation requise avant d'alimenter le serveur. L'enveloppe d'alimentation comprend les exigences d'alimentation maximale et minimale requises pour le fonctionnement du serveur. L'estimation initiale d'iDRAC est fondée sur sa compréhension initiale des composants du serveur. Après le début de l'exploitation et la découverte des composants supplémentaires, iDRAC peut augmenter ou diminuer ses besoins de puissance initiaux.

Lorsqu'un serveur est alimenté dans une enceinte, le logiciel iDRAC refait une estimation des besoins en alimentation et demande une modification ultérieure de l'enveloppe d'alimentation.

CMC accorde l'alimentation demandée au serveur et la puissance allouée est soustraite du bilan disponible. Une fois la demande d'alimentation du serveur satisfaite, le logiciel iDRAC du serveur surveille en continu la consommation électrique réelle. Selon les besoins d'alimentation réels, l'enveloppe d'alimentation d'iDRAC peut changer au fil du temps. iDRAC demande une augmentation de l'alimentation uniquement si les serveurs consomment la totalité de l'alimentation allouée.

Sous forte charge les performances des processeurs du serveur peuvent être dégradées pour s'assurer que la consommation d'énergie reste en dessous de la **Limite de la puissance d'entrée système** configurée par l'utilisateur.

L'enceinte PowerEdge M1000e peut fournir une alimentation suffisante pour obtenir des performances optimales de la plupart des configurations de serveur, mais plusieurs configurations de serveurs disponibles ne consomment pas l'alimentation maximale pouvant être délivrée par l'enceinte. Pour aider les centres de données à alimenter leurs enceintes, le châssis M1000e vous permet de spécifier une **limite de la puissance d'entrée système** pour garantir le maintien de l'alimentation alternative du châssis sous un seuil donné. CMC assure d'abord que suffisamment de puissance est disponible pour faire fonctionner les ventilateurs, les modules d'E/S, iKVM (le cas échéant) et CMC lui-même. Cette allocation de l'alimentation est appelée **Alimentation d'entrée allouée à l'infrastructure du châssis**. À la suite de l'infrastructure du châssis, les serveurs dans une enceinte sont mis sous tension. Toute tentative de définir une **limite de la puissance d'entrée système** en dessous de la consommation réelle échouera.

S'il est nécessaire que le bilan d'alimentation total reste inférieur à la valeur de la **Limite de la puissance d'entrée du système**, CMC alloue aux serveurs une valeur inférieure à l'alimentation maximale demandée. L'alimentation allouée aux serveurs est fonction de leur paramètre **Priorité des serveurs**, les serveurs de priorité 1 obtenant une alimentation maximale, les serveurs de priorité 2 étant alimentés après les serveurs de priorité 1, et ainsi de suite. Les serveurs de priorité moindre peuvent être moins alimentés que les serveurs de priorité 1 en fonction de la **capacité maximale de l'alimentation d'entrée du système** et du paramètre **Limite de la puissance d'entrée système** configuré par l'utilisateur.

Les changements de configuration, tels que l'ajout d'un serveur dans le châssis, peuvent imposer l'augmentation de la **limite de la puissance d'entrée système**. Les besoins d'alimentation de l'enceinte modulaire augmentent également lorsque les conditions thermiques changent et que les ventilateurs doivent fonctionner à une vitesse plus élevée, entraînant une plus forte consommation électrique. L'insertion de modules d'E/S et iKVM augmente également les besoins d'alimentation de l'enceinte modulaire. Une petite quantité d'énergie est consommée par les serveurs même lorsqu'ils sont mis hors tension afin de maintenir alimenté le contrôleur de gestion. Des serveurs supplémentaires ne peuvent être alimentés au sein de l'enceinte modulaire que si une alimentation suffisante est disponible. La **limite de la puissance d'entrée système** peut être augmentée à tout moment jusqu'à une valeur maximale de 11 637 watts pour permettre l'alimentation de serveurs supplémentaires.

Les changements dans l'enceinte modulaire permettant de réduire l'allocation de puissance sont :

- 1 Mise hors tension du serveur
- 1 Serveur
- 1 module d'E/S
- 1 Suppression du module iKVM
- 1 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 une priorité d'alimentation pour chacun des seize logements de serveur au sein d'une enceinte. Les paramètres de priorité vont de **1** (la plus haute) à **9** (la plus basse). Ces paramètres sont assignés aux logements du châssis et la priorité du logement sera héritée par tout serveur inséré dans ce logement. CMC utilise la priorité des logements en vue d'alimenter en priorité les serveurs à priorité supérieure de l'enceinte.

Selon le paramètre de priorité de logement de serveur par défaut, l'alimentation est répartie de façon égale dans tous les logements. La modification des priorités des logements permet aux administrateurs de décider quels serveurs ont la priorité pour les allocations d'alimentation. Si la priorité des modules serveurs les plus critiques est laissée à la valeur par défaut de 1 et que les modules serveurs les moins critiques sont définis sur une valeur de priorité de 2 ou plus, les modules serveurs de priorité 1 sont alimentés en premier. Ces serveurs à priorité supérieure obtiennent alors leur allocation d'alimentation maximale, tandis que les serveurs à priorité inférieure peuvent ne pas disposer d'une allocation d'alimentation suffisante pour fonctionner à leurs performances maximales, voire ne pas du tout être alimentés, selon la faiblesse de la limite de la puissance d'entrée système définie et les exigences d'alimentation du serveur.

Si un administrateur alimente manuellement les modules de serveur à faible priorité avant ceux à priorité plus élevée, les modules de serveur à faible priorité seront les premiers à avoir une allocation de puissance abaissée à la valeur minimale, afin d'accommoder les serveurs à priorité plus élevée. Ainsi, après épuisement de la puissance disponible pour l'allocation, CMC récupère la puissance des serveurs à faible priorité ou priorité égale jusqu'à ce qu'ils soient à leur niveau de puissance minimum.

 **REMARQUE** : Les modules d'E/S, les ventilateurs et iKVM (s'il est présent) reçoivent la priorité la plus élevée. CMC récupère l'alimentation uniquement pour répondre aux besoins d'alimentation d'un module ou d'un serveur de priorité supérieure.

Enclenchement dynamique des blocs d'alimentation

Le mode Enclenchement dynamique des blocs d'alimentation (DPSE) est désactivé par défaut. L'enclenchement dynamique des blocs d'alimentation économise l'énergie en optimisant l'efficacité énergétique de la puissance d'alimentation de l'unité d'alimentation au châssis. Cela entraîne également une augmentation de la vie de l'unité d'alimentation et une réduction de la production de chaleur.

CMC surveille l'allocation d'alimentation totale de l'enceinte et met les unités d'alimentation non nécessaires en condition de secours, entraînant la distribution de l'allocation d'alimentation totale du châssis à un nombre moindre d'unités d'alimentation. Les unités d'alimentation connectées sont plus efficaces lorsqu'elles fonctionnent à des niveaux de performance plus élevés. Ainsi cela améliore-t-il leur efficacité tout en améliorant la longévité des unités d'alimentation en veille.

Pour faire fonctionner les unités d'alimentation restantes à leur maximum d'efficacité :

- 1 Le mode **Sans redondance** avec enclenchement dynamique des blocs d'alimentation économise beaucoup d'énergie, avec seulement le nombre minimal d'unités d'alimentation en ligne. Les unités d'alimentation non requises sont placées en mode veille.
- 1 Le mode **Redondance des unités d'alimentation** avec enclenchement dynamique des blocs d'alimentation permet également d'économiser de l'énergie. Au moins deux blocs d'alimentations sont actifs, avec une unité d'alimentation nécessaire à l'alimentation de la configuration et une pour fournir la redondance en cas de panne de l'unité d'alimentation. Le mode **Redondance des unités d'alimentation** offre une protection contre la panne de toute unité d'alimentation, mais ne protège pas en cas de perte d'un réseau d'alimentation en CA.
- 1 Le mode **Redondance de l'alimentation alternative** avec enclenchement dynamique des blocs d'alimentation, dans lequel au moins deux des six blocs d'alimentation sont actifs, un sur chaque réseau d'alimentation, offre un bon compromis entre l'efficacité et la disponibilité maximale pour une configuration d'enceinte modulaire partiellement chargée.
- 1 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**.

- 1 Dans une configuration **Sans redondance** avec enclenchement dynamique des blocs d'alimentation, le châssis M1000e peut comporter jusqu'à cinq blocs d'alimentation condition de secours. Dans une configuration à six unités d'alimentation, certaines unités d'alimentation sont mises en veille et restent inutilisées afin d'améliorer l'efficacité énergétique. Le retrait ou une panne d'une unité d'alimentation connectée dans cette configuration entraînera la connexion d'une unité d'alimentation en mode **Veille** ; cependant, les unités d'alimentation en Veille peuvent nécessiter jusqu'à 2 secondes pour s'activer. Aussi certains modules de serveurs peuvent-ils perdre de la puissance durant la transition dans la configuration **Sans redondance**.

 **REMARQUE** : dans une configuration à trois unités d'alimentation, la charge du serveur peut empêcher la transition vers le mode **Veille** d'une unité d'alimentation.

- 1 Dans une configuration **Redondance des blocs d'alimentation**, l'enceinte maintient toujours une unité d'alimentation supplémentaire sous tension et marquée **En ligne** en sus des unités d'alimentation requises pour l'alimentation de l'enceinte. L'utilisation de l'alimentation est surveillée et jusqu'à quatre unités d'alimentation peuvent être mises en **veille** en fonction de la charge globale du système. Dans une configuration à six unités d'alimentation, deux blocs d'alimentation au minimum sont toujours sous tension.

Étant donné qu'une enceinte dans la configuration **Redondance des blocs d'alimentation** possède toujours une unité d'alimentation supplémentaire activée, l'enceinte peut tolérer la perte d'une unité d'alimentation en ligne et disposer encore d'une alimentation suffisante pour les modules serveurs installés. La perte de l'unité d'alimentation en ligne entraîne la mise en ligne d'une unité d'alimentation en veille. Une panne simultanée de plusieurs unités d'alimentation peut entraîner la perte d'alimentation de plusieurs modules serveurs pendant la mise sous tension des unités d'alimentation.

- 1 Dans la configuration **Redondance de l'alimentation alternative**, tous les blocs d'alimentation sont activés lors de l'alimentation du châssis. L'utilisation d'énergie est surveillée, et si la configuration du système et l'utilisation d'énergie le permettent, les unités d'alimentation sont placées en mode **veille**. Étant donné que l'état **Connecté** des unités d'alimentation d'un réseau met en miroir celles de l'autre réseau, l'enceinte peut subir une perte d'alimentation d'un réseau entier sans aucune interruption de l'alimentation vers l'enceinte.

Une augmentation de la demande d'électricité dans la configuration de la **redondance de l'alimentation alternative** entraîne l'activation des unités d'alimentation en mode de **veille**. Cela permet de maintenir la configuration en miroir nécessaire pour une redondance de réseau double.

 **REMARQUE** : une fois le mode Enclenchement dynamique des blocs d'alimentation activé, les unités d'alimentation en veille sont mises en état **En ligne** afin de récupérer de l'alimentation si la demande en alimentation augmente dans les trois modes de règles de redondance.

Règles de redondance

La règle de redondance est un ensemble configurable de propriétés qui détermine la manière dont CMC gère l'alimentation du châssis. Les règles de redondance suivantes sont configurables avec ou sans enclenchement dynamique des unités d'alimentation :

- 1 Redondance de l'alimentation alternative
- 1 Redondance des blocs d'alimentation
- 1 Sans redondance

La configuration de la redondance par défaut d'un châssis dépend du nombre d'unités d'alimentation qu'il contient, tel qu'indiqué dans [Tableau 9-1](#).

Tableau 9-1. Configuration de la 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	Désactivé
Trois unités d'alimentation	Sans redondance	Désactivé

Redondance de l'alimentation alternative

En mode Redondance d'alimentation alternative avec six unités d'alimentation, les six sont toutes actives. Les trois unités d'alimentation situées à gauche doivent être connectées à un réseau de courant alternatif, alors que les trois unités situées à droite doivent être connectées à un réseau de courant alternatif différent.

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 trois unités d'alimentation du réseau d'alimentation alternative opérationnel prennent la relève sans interruption pour les serveurs ou l'infrastructure.

PRÉCAUTION : en mode Redondance d'alimentation alternative, vous devez disposer d'une série équilibrée d'unité d'alimentation (au moins une unité d'alimentation sur chaque réseau). Si cette condition n'est pas remplie, la redondance d'alimentation alternative n'est pas possible.

Redondance des blocs d'alimentation

Lorsque le mode Redondance des blocs d'alimentation est activé, une unité d'alimentation du châssis est conservée comme alimentation de secours, garantissant ainsi que la défaillance de l'une des unités d'alimentation n'engendre pas la mise hors tension des serveurs ou du châssis. Le mode Redondance des blocs d'alimentation nécessite jusqu'à quatre unités d'alimentation. Des unités d'alimentation supplémentaires, si elles sont présentes, seront utilisées pour améliorer l'efficacité énergétique du système si le mode Enclenchement dynamique des blocs d'alimentation est activé. Les pannes ultérieures après une perte de redondance peuvent entraîner la mise hors tension des serveurs du châssis.

Sans redondance

Une alimentation excédant l'alimentation nécessaire pour que le châssis soit disponible, même lors d'une panne, continue d'alimenter le châssis.

PRÉCAUTION : le mode Sans redondance utilise les meilleures unités d'alimentation lorsque le mode Enclenchement dynamique des blocs d'alimentation est activé pour les nécessités du châssis. Dans ce mode, l'échec d'une seule unité d'alimentation entraîne la perte d'alimentation des serveurs et des données.

Préservation de l'alimentation et modifications du bilan de puissance

CMC préserve l'alimentation lorsque la limite d'alimentation maximale configurée par l'utilisateur est atteinte. Lorsque la demande en alimentation excède la **Limite de la puissance d'entrée système** configurée par l'utilisateur, CMC réduit l'alimentation des serveurs dans l'ordre de priorité inverse afin de libérer de l'alimentation pour les serveurs de priorité supérieure et pour les autres modules du châssis.

Lorsque tous les logements du châssis, ou plusieurs d'entre eux, sont configurés avec le même niveau de priorité, CMC diminue l'alimentation des serveurs par ordre croissant de numéro 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 sera diminuée en premier.

REMARQUE : vous pouvez définir un niveau de priorité à chaque serveur du châssis en lui attribuant un numéro de 1 à 9 inclus. Le niveau de priorité par défaut est 1 pour l'ensemble des serveurs. Plus le nombre est faible, plus le niveau de priorité est élevé.

Pour des instructions concernant l'attribution de niveaux de priorité aux serveurs, voir [Utilisation de la RACADM](#).

Vous pouvez attribuer une priorité aux serveurs à l'aide de l'interface utilisateur :

1. Cliquez sur **Serveurs** dans l'arborescence système.
2. Cliquez sur **Alimentation** → **Priorité**.

Modes Conservation d'énergie et Conservation max

CMC assure la conservation de la puissance maximale lorsque :

- 1 L'utilisateur sélectionne le mode de conservation maximale en utilisant l'interface Web ou RACADM.
- 1 Un script de commande automatisé en ligne, fourni par un onduleur, sélectionne le mode de conservation maximale.

En mode de conservation maximale, tous les serveurs commencent à fonctionner à leur niveau de puissance minimum, et toutes les demandes ultérieures d'attribution de puissance aux serveurs sont refusées. Dans ce mode, les performances des serveurs sous tension peuvent être dégradées. Des serveurs supplémentaires ne peuvent pas être mis sous tension, quelle que soit la priorité du serveur.

Le système est restauré à son plein rendement lorsque l'utilisateur ou un script de commande automatisé en ligne autorise le mode de conservation maximale.

Utilisation de l'interface Web

Vous pouvez activer ou désactiver le mode de conservation maximale à l'aide de l'interface :

1. Cliquez sur **Présentation du châssis** dans l'arborescence.
2. Cliquez sur **Alimentation** → **Configuration**.
3. Sélectionnez le **Mode de conservation d'énergie max** pour activer l'économie d'énergie maximale et cliquez sur **Appliquer**.
4. Décochez la case **Mode de conservation énergétique max** pour rétablir le fonctionnement normal et cliquez sur **Appliquer**.

Utilisation de la RACADM

Ouvrez une console série/Telnet/SSH d'accès à CMC, puis ouvrez une session.

- 1 Pour activer le mode de consommation énergétique maximale, tapez :

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

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

Fonctionnement des unités d'alimentation 110 V

Certaines unités d'alimentation prennent en charge l'entrée 110V CA. Cette entrée peut dépasser ce qui est autorisé pour le circuit de dérivation. Si une unité d'alimentation est connectée au courant 110V CA, l'utilisateur doit définir CMC pour le fonctionnement normal de l'enceinte. S'il n'est pas défini et si des unités d'alimentation 110 V sont détectées, toutes les demandes ultérieures d'attribution de puissance aux serveurs seront refusées. Dans ce cas, les serveurs complémentaires ne peuvent être mis sous tension, quelle que soit leur priorité. Vous pouvez définir CMC pour une utilisation avec les unités d'alimentation 110 V en utilisant l'interface Web ou RACADM.

Utilisation de l'interface Web

Vérifiez que le circuit 110 V est conçu pour le courant prévu, puis procédez comme suit :

1. Cliquez sur **Présentation du châssis** dans l'arborescence.
2. Cliquez sur **Alimentation** → **Configuration**.
3. Sélectionnez **Autoriser le fonctionnement 110 VCA** et cliquez sur **Appliquer**.

Utilisation de la RACADM

Vérifiez que le circuit 110 V est conçu pour le courant prévu, puis procédez comme suit :

1. Ouvrez une console série/Telnet/SSH d'accès à CMC, puis ouvrez une session.
2. Activez les unités d'alimentation 110 VCA :

```
racadm config -g cfgChassisPower -o cfgChassisAllow110VACOperation 1
```

Performance du serveur contre redondance de l'alimentation

Lorsqu'elle est activée, cette option favorise la performance du serveur et sa mise sous tension plutôt que le maintien de la redondance de l'alimentation. Lorsqu'elle est désactivée, le système favorise la redondance de l'alimentation plutôt que la performance du serveur. Lorsqu'elle est désactivée et que l'alimentation du châssis est insuffisante, pour la redondance comme pour une pleine performance, alors afin de préserver la redondance, il se peut que certains serveurs :

- 1 ne reçoivent pas assez d'alimentation pour assurer une pleine performance.
- 1 ne soient pas alimentés.

Utilisation de l'interface Web

Pour activer l'option Performance du serveur contre redondance de l'alimentation, procédez comme suit :

1. Cliquez sur **Présentation du châssis** dans l'arborescence.
2. Cliquez sur **Alimentation** → **Configuration**.
3. Sélectionnez **Performance du serveur contre redondance de l'alimentation**, puis cliquez sur **Appliquer**.

Pour désactiver l'option Performance du serveur contre redondance de l'alimentation, procédez comme suit :

1. Cliquez sur **Présentation du châssis** dans l'arborescence.
2. Cliquez sur **Alimentation** → **Configuration**.
3. Désélectionnez **Performance du serveur contre redondance de l'alimentation**, puis cliquez sur **Appliquer**.

Utilisation de la RACADM

Pour activer l'option Performance du serveur contre redondance de l'alimentation, procédez comme suit :

1. Ouvrez une console série/Telnet/SSH d'accès à CMC, puis ouvrez une session.
2. Activer Performance du serveur contre redondance de l'alimentation :

```
racadm config -g cfgChassisPower -o cfgChassisPerformanceOverRedundancy 1
```

Pour désactiver l'option Performance du serveur contre redondance de l'alimentation, procédez comme suit :

1. Ouvrez une console série/Telnet/SSH d'accès à CMC, puis ouvrez une session.
2. Désactiver Performance du serveur contre redondance de l'alimentation :

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

Journalisation distante

La consommation d'alimentation peut être enregistrée sur un serveur syslog distant. La consommation d'alimentation totale, minimale, maximale et moyenne du châssis tout au long d'une période de collecte peut être journalisée. Pour des informations supplémentaires sur l'activation de cette fonctionnalité et la configuration de l'intervalle de collecte/journalisation, voir les sections associées ci-dessous.

Utilisation de l'interface Web

Vous pouvez activer la journalisation de l'alimentation distante à l'aide de l'interface utilisateur. Pour ce faire, ouvrez une session dans l'interface utilisateur, puis procédez comme suit :

1. Cliquez sur **Présentation du châssis** dans l'arborescence.

2. Cliquez sur **Alimentation** → **Configuration**.
3. Sélectionnez **Journalisation de l'alimentation distante** afin de pouvoir journaliser des événements d'alimentation sur une hôte distant.
4. Spécifiez l'intervalle de journalisation requis (1 à 1 440 minutes).
5. Cliquez sur **Appliquer** pour enregistrer les modifications.

Utilisation de la RACADM

Ouvrez une console texte série, Telnet ou SSH vers CMC, ouvrez une session, puis configurez la journalisation de l'alimentation distante tel qu'illustré :

1. Pour activer la fonctionnalité de journalisation de l'alimentation distante, entrez la commande suivante :

```
racadm config -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingEnabled 1
```

2. 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.

3. Pour déterminer si la fonction de journalisation de l'alimentation distante est activée, entrez la commande suivante :

```
racadm getconfig -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingEnabled
```

4. Pour déterminer l'intervalle de journalisation de l'alimentation distante, entrez la commande suivante :

```
racadm getconfig -g cfgRemoteHosts -o cfgRhostsSyslogPowerLoggingInterval
```

 **REMARQUE** : la fonctionnalité de journalisation d'alimentation distante dépend des hôtes syslog distants et s'ils ont été précédemment configurés. La journalisation vers un ou plusieurs hôtes syslog distants doit être activée ; sinon, la consommation d'alimentation est journalisée. Ceci peut être effectuée à l'aide de l'interface utilisateur Web ou l'interface RACADM. Pour plus de détails, voir les instructions de configuration syslog distant.

Défaillance d'une unité d'alimentation avec règle de redondance dégradée ou absente

CMC diminue l'alimentation des serveurs en cas d'alimentation insuffisante, par exemple suite à une défaillance d'une unité d'alimentation. Après avoir diminué l'alimentation des serveurs, CMC évalue à nouveau les besoins d'alimentation du châssis. Si les besoins d'alimentation ne sont toujours pas satisfaits, CMC met hors tension les serveurs moins prioritaires.

L'alimentation des serveurs à priorité plus élevée est progressivement rétablie tandis que les besoins d'alimentation respectent le bilan de puissance.

 **REMARQUE** : pour configurer la stratégie de redondance, voir [Configuration du bilan de puissance et de la redondance](#).

Règle d'enclenchement d'un nouveau serveur

Lorsqu'un nouveau serveur est mis sous tension, il se peut que CMC doive diminuer l'alimentation des serveurs à priorité inférieure afin d'attribuer une alimentation plus importante au nouveau serveur si l'ajout de ce dernier engendre une demande supérieure à l'alimentation disponible pour le châssis. Ceci se produit lorsque l'administrateur configure une limite d'alimentation du châssis inférieure à celle nécessaire pour alimenter pleinement les serveurs, ou lorsque l'alimentation disponible est insuffisante en cas de besoin énergétique critique de l'ensemble des serveurs présents dans le châssis. Si l'alimentation libérée en réduisant l'alimentation allouée aux serveurs de priorité inférieure est insuffisante, il est possible que le nouveau serveur ne soit pas alimenté.

L'alimentation la plus élevée à fournir, nécessaire au fonctionnement optimal du châssis et de l'ensemble des serveurs (y compris le nouveau serveur), constitue le cas le plus défavorable pour les besoins d'alimentation. Lorsque cette alimentation est disponible, tous les serveurs bénéficient d'une alimentation suffisante et le nouveau serveur peut être mis sous tension.

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 9-2](#) décrit les actions effectuées par CMC lors de la mise sous tension d'un nouveau serveur dans le scénario décrit ci-dessus.

Tableau 9-2. Prise en charge par CMC d'une tentative de mise sous tension d'un serveur

L'alimentation du cas le plus défavorable est disponible	Prise en charge par CMC	Mise sous tension du serveur
Oui	La préservation de l'alimentation n'est pas nécessaire	Autorisé
Non	Passage en mode d'économie d'énergie :	

	<ul style="list-style-type: none"> 1 L'alimentation nécessaire au nouveau serveur est disponible 1 L'alimentation nécessaire au nouveau serveur n'est pas disponible 	<p>Autorisé</p> <p>Non autorisée</p>
--	--	--------------------------------------

En cas de défaillance d'une unité d'alimentation, l'état d'intégrité devient non critique et un événement de défaillance d'unité d'alimentation est généré. Le retrait d'une unité d'alimentation entraîne un événement de retrait d'unité d'alimentation.

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 ultérieure ou la capacité d'alimentation de l'utilisateur est supérieure aux allocations de serveurs, les performances des serveurs seront dégradées ou, dans le pire des cas, les serveurs pourront être mis hors tension. Les deux conditions sont dans l'ordre de priorité inverse. En d'autres termes, les serveurs de priorité inférieure sont mis hors tension en premier.

Le [Tableau 9-3](#) décrit la prise en charge par le micrologiciel de l'arrêt ou du retrait d'une unité d'alimentation dans le cadre de différentes configurations de redondance des unités d'alimentation.

Tableau 9-3. Impact d'une défaillance ou du retrait d'une unité d'alimentation sur le châssis

Configuration des unités d'alimentation	Unités d'alimentation dynamiques Enclenchement	Prise en charge par le micrologiciel
Redondance de l'alimentation alternative	Désactivé	CMC vous alerte sur la perte de redondance d'alimentation alternative.
Redondance des blocs d'alimentation	Désactivé	CMC vous alerte sur la perte de redondance des blocs d'alimentation.
Sans redondance	Désactivé	Réduit l'alimentation des serveurs de priorité inférieure, le cas échéant.
Redondance de l'alimentation alternative	Activé	CMC vous alerte sur la perte de redondance d'alimentation alternative. Les unités d'alimentation en mode Attente (s'il y en a) sont activées afin de compenser la perte d'énergie suite à la défaillance ou au retrait de l'unité d'alimentation.
Redondance des blocs d'alimentation	Activé	CMC vous alerte sur la perte de redondance des blocs d'alimentation. Les unités d'alimentation en mode Attente (s'il y en a) sont activées afin de compenser la perte d'énergie suite à une défaillance ou une déconnexion de l'unité d'alimentation.
Sans redondance	Activé	Réduit l'alimentation des serveurs de priorité inférieure, le cas échéant.

Retraits d'unités d'alimentation avec règle de redondance dégradée ou absente

CMC conserve une alimentation lorsque vous retirez une unité d'alimentation ou un cordon d'alimentation alternative d'une unité d'alimentation. CMC réduit l'alimentation des serveurs à priorité inférieure jusqu'à ce qu'elle soit prise en charge par les unités d'alimentation restantes du châssis. Si vous retirez plusieurs unités d'alimentation, CMC évalue à nouveau les besoins d'alimentation lors du retrait de la seconde unité d'alimentation afin de déterminer la réponse du micrologiciel. Si les besoins d'alimentation ne sont toujours pas satisfaits, CMC peut mettre hors tension les serveurs de priorité inférieure.

Limites

- 1 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.
- 1 Les modifications apportées à la règle de redondance des unités d'alimentation sont limitées par le nombre d'unités d'alimentation du châssis. Vous pouvez sélectionner l'une des trois configurations de redondance des unités d'alimentation répertoriées dans [Règles de redondance](#).

Modifications d'alimentation et de la règle de redondance dans le journal des événements système

Les modifications de l'état des blocs d'alimentation et de la règle de redondance de l'alimentation sont enregistrées en tant qu'événements. Les événements liés au bloc d'alimentation enregistrant des entrées dans le journal des événements système (SEL) sont les insertions et retraits de blocs d'alimentation, l'insertion et le retrait d'entrée d'alimentation et la confirmation/annulation de sorties d'alimentation. Le [Tableau 9-4](#) répertorie les entrées du journal SEL relatives aux changements des blocs d'alimentation.

Tableau 9-4. Événements du journal SEL relatifs aux modifications 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 annulée
Alimentation alternative reçue	La perte de l'alimentation a été annulée
perte de l'alimentation alternative	La perte de l'alimentation a été confirmée

sortie CC produite	La panne d'un bloc d'alimentation a été annulée
perte de sortie en CC	La panne d'un bloc d'alimentation a été confirmée
Fonctionnement 110 V non reconnu détecté	L'alimentation basse tension d'entrée (110) a été confirmée
Fonctionnement 110 V reconnu	L'alimentation basse tension d'entrée (110) a été annulée

Les événements liés aux modifications de la condition de la redondance d'alimentation qui enregistrent des entrées dans le journal SEL sont une perte de redondance et un regain de redondance de l'enceinte modulaire qui est configurée pour la règle d'alimentation en mode **Redondance de l'alimentation alternative** ou la règle d'alimentation en mode **Redondance des blocs d'alimentation**. Le [Tableau 9-5](#) liste les entrées du journal SEL liées aux modifications de la stratégie d'alimentation en mode Redondance de l'alimentation.

Tableau 9-5. Événements du journal SEL relatifs aux modifications de la condition de la redondance d'alimentation

Événement de stratégie d'alimentation	Entrée du journal d'événements système (SEL)
Perte de la redondance	La perte de la redondance a été affirmée
Regain de la redondance	La perte de la redondance a été annulée

Condition de la redondance et intégrité énergétique globale

La condition de la redondance est un facteur de détermination de l'intégrité énergétique globale. Lorsque la règle de redondance d'alimentation est définie, par exemple, sur le mode Redondance d'alimentation alternative et que la condition de la redondance indique que le système fonctionne avec la redondance, l'intégrité énergétique globale sera généralement OK. Toutefois, si les conditions d'utilisation de la redondance d'alimentation alternative ne peuvent pas être remplies, la condition de la redondance est **Non** et l'intégrité énergétique globale est **Critique**. Ceci s'explique par le fait que le système ne peut pas fonctionner conformément à la règle de redondance configurée.



REMARQUE : CMC n'effectue pas un contrôle préalable de ces conditions lorsque vous modifiez la règle de redondance par ou vers le mode Redondance d'alimentation alternative. Ainsi, la configuration de la règle de redondance peut entraîner immédiatement une perte de redondance ou un regain.

Configuration et gestion de l'alimentation

Vous pouvez utiliser les interfaces Web et RACADM pour gérer et configurer les commandes d'alimentation de CMC. Vous pouvez notamment :

- 1 Consulter les allocations, la consommation et la condition d'alimentation du châssis, des serveurs et des unités d'alimentation
- 1 Configurer le paramètre Limite de la puissance d'entrée système et la règle de redondance pour le châssis
- 1 Exécuter des opérations de contrôle de l'alimentation (mise sous tension, mise hors tension, réinitialisation du système, cycle d'alimentation) du châssis

Affichage de la condition d'intégrité des unités d'alimentation

La page **Condition du bloc d'alimentation** affiche la condition et les mesures des unités d'alimentation associées au châssis.

Utilisation de l'interface Web

L'état d'intégrité d'une unité d'alimentation peut être consulté de deux façons : à partir de la section **Graphiques du châssis** sur la page **Condition du châssis** ou sur la page **État du bloc d'alimentation**. La page **Graphiques du châssis** fournit une représentation graphique de l'ensemble des unités d'alimentation installées dans le châssis.

Pour consulter la condition d'intégrité des unités d'alimentation à l'aide de la page **Graphiques du châssis** :

1. Ouvrez une session sur l'interface Web de CMC.
2. La page **Condition du châssis** s'affiche. La section droite de la page **Graphiques du châssis** fournit une vue arrière du châssis et contient la condition d'intégrité de toutes les unités d'alimentation. L'état d'intégrité de l'unité d'alimentation est indiqué par la couleur du sous-graphique unité d'alimentation :
 - 1 Vert : l'unité d'alimentation est présente, sous tension et communique avec CMC ; il n'y a aucune indication d'événement indésirable.
 - 1 Orange : défaillance d'une unité d'alimentation. Consulter le journal CMC pour des détails sur la défaillance.
 - 1 Gris : se produit lors de l'initialisation d'unité d'alimentation et lorsque le bloc d'alimentation est réglé en mode veille, pendant l'allumage du châssis ou l'insertion d'unité d'alimentation. L'unité d'alimentation est présente et hors tension. Aucune condition défavorable n'est indiquée.
3. Placez le curseur sur un sous-graphique de l'unité d'alimentation pour afficher le champ textuel ou l'infobulle correspondant. Le champ textuel fournit des informations complémentaires sur l'unité d'alimentation.
4. Le lien hypertexte du sous-graphique de l'unité d'alimentation permet d'accéder à la page de l'interface utilisateur de CMC correspondante pour une navigation directe vers la page **État du bloc d'alimentation** associée à l'ensemble des unités d'alimentation.

Pour consulter la condition d'intégrité des unités d'alimentation à l'aide de la page **État du bloc d'alimentation** :

1. Ouvrez une session sur l'interface Web de CMC.
2. Sélectionnez **Blocs d'alimentation** dans l'arborescence du système. La page **État du bloc d'alimentation** s'affiche.

Le [Tableau 9-6](#) et le [Tableau 9-7](#) décrivent les informations mentionnées à la page Condition du bloc d'alimentation.

Tableau 9-6. Blocs d'alimentation

Élément	Description	
Nom	Indique le nom de l'unité d'alimentation : PS-[n], [n] étant le numéro du bloc d'alimentation.	
Présent	Indique si l'unité d'alimentation est Présente ou Absente .	
Intégrité	 OK	Indique que l'unité d'alimentation est présente et qu'elle communique avec CMC. En cas de perte des communications entre CMC et l'unité d'alimentation, CMC ne pourra pas obtenir ni afficher l'état de l'intégrité de l'unité d'alimentation
	 Avertissement	Indique que des alertes d'avertissement seules ont été émises et que des actions correctives doivent être effectuées. Si aucune action corrective n'est prise, des pannes d'alimentation critiques ou graves susceptibles d'affecter l'intégrité du serveur pourraient se produire.
	 Grave	Indique qu'au moins une alerte de panne a été générée pour le bloc d'alimentation. L'état grave indique une panne d'alimentation du châssis et la nécessité d'effectuer une action corrective immédiatement .
État de l'alimentation	Indique l'état d'alimentation des blocs d'alimentation (un seul à la fois) : En cours d'initialisation , En ligne , Veille , Test de diagnostic , Échec , Hors ligne , Inconnu ou Absent .	
Capacité	Affiche la capacité d'alimentation en watts.	

Tableau 9-7. Condition de la puissance système

Élément	Description
Intégrité globale énergétique	Indique la condition d'intégrité (OK , Non critique , Critique , Non récupérable , Autre , Inconnu) de la gestion de l'alimentation du châssis entier.
Condition de la puissance système	Affiche la condition de l'alimentation (Activé , Désactivé , Mis sous tension , Mis hors tension) du châssis.
Redondance	Indique la condition de la redondance des blocs d'alimentation. Les valeurs sont les suivantes : Non : les blocs d'alimentation ne sont pas redondants. Oui : une redondance totale est appliquée.

Utilisation de la RACADM

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

```
racadm getpminfo
```

Pour des informations supplémentaires sur la commande `getpminfo`, y compris les détails de sorties, voir le *Guide de référence de la ligne de commande pour iDRAC6 et CMC* sur le site de support Dell à l'adresse support.dell.com/manuals.

Affichage de l'état de la consommation de puissance

CMC fournit la consommation électrique d'entrée réelle de l'intégralité du système à la page **Condition de la consommation énergétique**.

Utilisation de l'interface Web

 **REMARQUE** : pour réaliser des tâches de gestion de l'alimentation, vous devez disposer du privilège d'**Administrateur de contrôle du châssis**.

1. Ouvrez une session sur l'interface Web de CMC.

2. Cliquez sur **Présentation du châssis** dans l'arborescence.
3. Cliquez sur **Alimentation** → **Consommation énergétique**. La page **Consommation énergétique** s'affiche.

[Tableau 9-8](#) à [Tableau 9-11](#) décrivent les informations affichées sur la page **Consommation énergétique**.

 **REMARQUE** : vous pouvez également afficher la condition de la redondance d'alimentation sous **Blocs d'alimentation** dans l'arborescence des **systèmes** → onglet **Condition**.

Utilisation de la RACADM

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

```
racadm getpminfo
```

Tableau 9-8. Statistiques de l'alimentation en temps réel

Élément	Description
Alimentation d'entrée du système	Affiche la consommation actuelle cumulée en courant alternatif de l'ensemble des modules du châssis, mesurée à l'entrée des unités d'alimentation. La valeur de puissance d'entrée dans le système est indiquée en watts et en BTU/h.
Alimentation maximale du système	Affiche la consommation d'énergie maximale du système depuis que l'ancienne valeur a été effacée. Cette propriété vous permet d'effectuer le suivi de la puissance maximale consommée par le système (châssis et modules) enregistrée sur une période spécifiée. Cliquez sur le bouton de réinitialisation des statistiques d'alimentation maximale/minimale sous le tableau pour effacer cette valeur. La valeur de l'alimentation maximale du système est indiquée en watts et en BTU/h.
Point de départ de l'alimentation maximale du système	Affiche la date et l'heure enregistrées depuis que la dernière valeur relative à la consommation d'énergie maximale du système a été effacée. L'horodatage s'affiche au format hh:mm:ss MM/JJ/AAAA, où hh correspond aux heures (0 à 24), mm à minutes (00 à 60), ss à secondes (00 à 60), MM à mois (1 à 12), JJ à jours (1 à 31) et AAAA à année. Cette valeur est réinitialisée à l'aide du bouton de réinitialisation des statistiques d'alimentation maximale/minimale et également lorsque CMC se réinitialise ou échoue.
Horodatage de la puissance maximale du système	Affiche la date et l'heure enregistrées lorsque le pic de consommation électrique du système a été atteint au cours de la période analysée. L'horodatage est affiché au format hh:mm:ss MM/JJ/AAAA, où hh correspond aux heures (de 0 à 24), mm aux minutes (de 00 à 60), ss aux secondes (de 00 à 60), MM au mois (de 1 à 12), JJ au jour (de 1 à 31) et AAAA à l'année.
Puissance minimale du système	Affiche le niveau minimum de consommation en courant alternatif du système (en watts) depuis la dernière réinitialisation de cette valeur par un utilisateur. Cette propriété vous permet d'effectuer le suivi de la consommation électrique minimale du système (châssis et modules) enregistrée sur une période spécifiée. Cliquez sur le bouton de réinitialisation des statistiques d'alimentation maximale/minimale sous le tableau pour effacer cette valeur. La valeur de l'alimentation minimale du système est indiquée en watts et en BTU/h. Cette valeur est réinitialisée à l'aide du bouton de réinitialisation des statistiques d'alimentation maximale/minimale et également lorsque CMC se réinitialise ou échoue.
Point de départ de l'alimentation minimale du système	Affiche la date et l'heure enregistrées depuis que la dernière valeur relative à la consommation de courant minimale du système a été effacée. L'horodatage s'affiche au format hh:mm:ss MM/JJ/AAAA, où hh correspond aux heures (0 à 24), mm à minutes (00 à 60), ss à secondes (00 à 60), MM à mois (1 à 12), JJ à jours (1 à 31) et AAAA à année. Cette valeur est réinitialisée à l'aide du bouton de réinitialisation des statistiques d'alimentation maximale/minimale et également lorsque CMC se réinitialise ou échoue.
Horodatage de l'alimentation minimale du système	Affiche la date et l'heure enregistrées lorsque la consommation électrique minimale du système s'est produite sur la période enregistrée. Le format de l'horodatage est identique à celui décrit pour l' horodatage de l'alimentation maximale du système .
Alimentation à l'état inactif	Affiche la consommation de courant estimée du châssis à l'état inactif. L'état inactif est défini comme l'état du châssis lorsqu'il est sous tension et que tous les modules consomment du courant alors qu'il est à l'état inactif. <i>Il s'agit d'une valeur estimée et non mesurée.</i> Cette dernière est estimée en fonction de l'alimentation cumulée allouée aux composants de l'infrastructure du châssis tels que les modules d'E/S, les ventilateurs, le module iKVM, les contrôleurs iDRAC et l'écran LCD. Elle est également estimée en fonction des besoins minimum en courant pour tous les serveurs auxquels une alimentation a été allouée et qui sont sous-tension. La valeur de l'alimentation du système à l'état inactif est indiquée en watts et en BTU/h.
Alimentation potentielle du système	Affiche la consommation de courant estimée du châssis lorsqu'il fonctionne à pleine puissance. La consommation de courant maximale définit l'état du châssis lorsqu'il est mis sous tension et que tous les modules consomment une alimentation maximale. <i>Il s'agit d'une valeur estimée calculée d'après la consommation électrique agrégée de l'historique de la configuration système, et non d'une valeur mesurée.</i> Elle est calculée comme étant l'alimentation cumulée allouée aux composants de l'infrastructure du châssis (modules d'E/S, ventilateurs, iKVM, contrôleurs iDRAC et l'écran LCD du panneau avant) et comme correspondant aux besoins d'alimentation maximum de tous les serveurs auxquels une alimentation a été allouée et qui sont sous tension. La valeur de l'alimentation potentielle du système est indiquée en watts et en BTU/h.
Lecture du courant d'entrée du système	Affiche la consommation de courant d'entrée totale du châssis basée sur la somme des consommations de courant d'entrée de chaque module d'unité d'alimentation spécifique présent dans le châssis. La valeur du courant d'entrée du système est indiquée en A (ampères).

Tableau 9-9. État des statistiques de l'énergie en temps réel

Élément	Description
Consommation d'énergie du système	Affiche la consommation d'énergie cumulée en courant alternatif de tous les modules du châssis, mesurée à l'entrée des blocs d'alimentation. La valeur est indiquée en kWh (valeur cumulée).
Heure de début de la consommation	Affiche la date et l'heure enregistrées depuis que la dernière valeur relative à la consommation d'énergie du système a été effacée et qu'un nouveau cycle de mesures a débuté. L'horodatage s'affiche au format hh:mm:ss MM/JJ/AAAA, où : hh

énergétique du système	correspond aux heures (0 à 23), mm à minutes (00 à 59), ss à secondes (00 à 59), MM à mois (1 à 12), JJ à jours (1 à 31) et AAAA à année. Cette valeur est réinitialisée à l'aide du bouton de réinitialisation des statistiques énergétiques et est conservée en cas de réinitialisation ou d'échec de CMC.
Horodatage de la consommation d'énergie du système	Affiche la date et l'heure de calcul de la consommation d'énergie du système pour l'affichage. L'horodatage s'affiche au format hh:mm:ss MM/JJ/AAAA , où : hh correspond aux heures (0 à 23), mm à minutes (00 à 59), ss à secondes (00 à 59), MM à mois (1 à 12), JJ à jours (1 à 31) et AAAA à année.

Tableau 9-10. Condition de la puissance système

Élément	Description
Intégrité globale énergétique	Indique la condition de l'intégrité du sous-système de puissance du châssis. : <ul style="list-style-type: none"> Icône de coche verte pour OK Icône de point d'exclamation jaune pour Non critique Icône de croix rouge pour Critique
Condition de la puissance système	Affiche l'état de l'alimentation (activé, désactivé, mis sous tension, mis hors tension) du châssis.
Redondance	Affiche l'état de la redondance. Les valeurs valides sont les suivantes : <p>Non : les unités d'alimentation ne sont pas redondantes</p> <p>Oui : une redondance totale est appliquée</p>

Tableau 9-11. Modules serveurs

Élément	Description
Ordre de priorité	Affiche l'emplacement du module de serveur. Le numéro de logement est un numéro séquentiel (de 1 à 16) qui identifie le module serveur en fonction de son emplacement dans le châssis.
Nom	Affiche le nom du serveur. Le nom du serveur peut être redéfini par l'utilisateur.
Présent	Indique si le serveur est présent dans le logement (Oui ou Non). Si ce champ affiche Extension de n° (où n° est compris entre 1 et 8), le nombre qui suit correspond au logement principal d'un serveur à logements multiples.
Réelle (AC)	Mesure en temps réel de la consommation de puissance réelle du serveur. La mesure est affichée en watts CA.
Heure de début de la consommation énergétique cumulée	Mesure en temps réel de la consommation énergétique cumulée que le serveur a consommée depuis l'heure affichée dans le champ Heure de début . L'unité de mesure est le Kilowattheure (kWh).
Horodatage de la consommation de puissance maximale	Affiche la consommation de puissance maximale consommée par le serveur à un moment donnée. L'heure à laquelle le pic de consommation électrique s'est produit est enregistrée dans le champ Horodatage . La mesure est affichée en watts.

Affichage de la condition du bilan de puissance

CMC fournit des aperçus de la condition d'alimentation du sous-système d'alimentation à la page [Condition du bilan d'alimentation](#).

Utilisation de l'interface Web

 **REMARQUE** : pour réaliser des tâches de gestion de l'alimentation, vous devez disposer du privilège d'**Administrateur de contrôle du châssis**.

1. Ouvrez une session sur l'interface Web de CMC.
2. Cliquez sur **Présentation du châssis** dans l'arborescence.
3. Cliquez sur **Alimentation** → **Condition du bilan**.

La page **Condition du bilan de puissance** s'affiche.

Les tableaux [Tableau 9-12](#) à [Tableau 9-15](#) décrivent les informations affichées sur la page **Condition du bilan de puissance**.

Pour plus d'informations sur la configuration des paramètres de cette activité, voir [Configuration du bilan de puissance et de la redondance](#).

Utilisation de la RACADM

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

```
racadm getpbinfo
```

Pour des informations supplémentaires sur la commande `getpbinfo`, y compris les détails de sortie, voir la section sur la commande `getpbinfo` du *Guide de référence de la ligne de commande pour iDRAC6 et CMC*.

Tableau 9-12. Configuration de la règle d'alimentation du système

Élément	Description
Limite de la puissance d'entrée système	<p>Affiche la limite de consommation électrique maximale configurée par l'utilisateur pour l'intégralité du système (châssis, CMC, serveurs, modules d'E/S, blocs d'alimentation, iKVM et ventilateurs). CMC applique cette limite en réduisant l'alimentation du serveur ou en mettant hors tension les modules de serveur à priorité inférieure. La valeur de la limite de la puissance d'entrée système est indiquée en watts, BTU/h et pourcentages.</p> <p>Si la consommation d'énergie du châssis dépasse la limite de la puissance d'entrée système, les performances des serveurs à priorité inférieure sont réduites jusqu'à ce que la consommation d'énergie totale tombe en dessous de cette valeur.</p> <p>Lorsque les serveurs sont configurés avec la même priorité, la réduction d'alimentation ou la mise hors tension du serveur s'applique en fonction de son numéro de connecteur. Par exemple, le serveur sur le connecteur 1 est sélectionné en premier et celui sur le connecteur 16 est sélectionné en dernier.</p>
Règle de redondance	<p>Indique la configuration de la redondance actuelle : Redondance de l'alimentation alternative, Redondance du bloc d'alimentation et Sans redondance.</p> <p>Redondance de l'alimentation alternative : la charge de l'alimentation est équilibrée sur l'ensemble des unités d'alimentation. La moitié d'entre elles doivent être câblées avec un réseau d'alimentation alternative et l'autre moitié doit être câblée avec un autre réseau. Lorsque le système s'exécute de manière optimale en mode Redondance de l'alimentation alternative, la charge de la puissance est répartie de manière équilibrée sur tous les blocs d'alimentation actifs. En cas de défaillance d'un réseau, les unités d'alimentation du réseau de courant alternatif opérationnel prennent le relais en fonctionnant à 100 % de leur capacité.</p> <p>Redondance des blocs d'alimentation : la capacité de l'unité d'alimentation la plus puissante du châssis est conservée comme alimentation de secours, garantissant ainsi que la défaillance de l'une des unités d'alimentation n'engendre pas la mise hors tension des modules serveurs ou du châssis.</p> <p>Redondance des blocs d'alimentation : peut ne pas utiliser les six blocs d'alimentation ; il utilise assez d'unités d'alimentation pour s'assurer qu'en cas de panne l'un des autres peut continuer à alimenter le châssis. Les autres blocs d'alimentation peuvent être mis en mode veille si le mode Enclenchement dynamique des blocs d'alimentation est activé.</p> <p>Sans redondance : La puissance de tous les blocs d'alimentation actifs est suffisante pour alimenter l'ensemble du châssis, y compris le châssis, les serveurs, les modules d'E/S, iKVM et CMC. Les blocs d'alimentation restants peuvent être mis en mode veille si le mode Enclenchement dynamique des blocs d'alimentation est activé.</p> <p>⚠ PRÉCAUTION : le mode Sans redondance utilise uniquement le nombre minimum requis de blocs d'alimentation en même temps, sans sauvegarde. La panne de l'une des trois unités d'alimentation utilisées peut entraîner une coupure de courant et la perte des données des modules de serveur.</p>
Enclenchement dynamique des blocs d'alimentation	<p>Indique si l'activation des blocs d'alimentation dynamique est activée ou désactivée. L'activation de cette fonctionnalité permet à CMC de mettre les unités d'alimentation sous-utilisées en mode attente en fonction de la règle de redondance définie et des besoins d'alimentation du système. La mise en mode attente des unités d'alimentation sous-utilisées augmente l'utilisation et l'efficacité des unités d'alimentation connectées, ce qui permet d'économiser l'énergie.</p>

Tableau 9-13. Allocation d'énergie

Élément	Description
Capacité maximale de l'alimentation d'entrée du système	Alimentation d'entrée maximale que les blocs d'alimentation disponibles peuvent fournir au système (en watts).
Réserve de redondance d'entrée	<p>Affiche la quantité d'alimentation redondante (en watts) en réserve pouvant être utilisée en cas de panne d'un réseau de courant alternatif ou d'un bloc d'alimentation.</p> <p>Lorsque le châssis est configuré pour fonctionner en mode de redondance de l'alimentation alternative, la réserve de redondance de l'alimentation d'entrée correspond à la quantité de courant réservée pouvant être utilisée en cas de panne du réseau de courant alternatif.</p> <p>Lorsque le châssis est configuré pour fonctionner en mode de redondance des blocs d'alimentation, la réserve de redondance de l'alimentation d'entrée correspond à la quantité d'alimentation de réserve pouvant être utilisée en cas de panne d'une unité d'alimentation spécifique.</p>
Alimentation d'entrée allouée aux serveurs	Affiche l'alimentation d'entrée cumulée (en watts) que CMC alloue aux serveurs en fonction de leur configuration.
Alimentation d'entrée allouée à l'infrastructure du châssis	Affiche l'alimentation d'entrée cumulée (en watts) que CMC alloue à l'infrastructure du châssis (ventilateurs, modules d'E/S, iKVM, CMC, CMC et iDRAC en attente sur les serveurs).
Total de l'alimentation	Affiche la puissance totale du châssis, en watts, toujours disponible pour l'attribution.

d'entrée disponible pour l'allocation	
Capacité d'alimentation d'entrée en attente	<p>Affiche la quantité de courant d'entrée en attente (en watts) disponible en cas de panne ou de suppression d'un bloc d'alimentation. Ce champ affiche des relevés lorsque le système possède au moins quatre blocs d'alimentation et que l'enclenchement dynamique des blocs d'alimentation est activé.</p> <p>REMARQUE : il est possible de voir une unité d'alimentation en attente mais cela n'affecte pas la valeur de la capacité d'alimentation d'entrée en attente. Dans ce cas, la valeur en watts de cette unité d'alimentation contribue à la valeur Total de l'alimentation d'entrée disponible pour l'allocation.</p>

Tableau 9-14. Modules serveurs

Élément	Description
Ordre de priorité	Affiche l'emplacement du module de serveur. Le numéro de logement est un numéro séquentiel (de 1 à 16) qui identifie le module serveur en fonction de son emplacement dans le châssis.
Nom	Affiche le nom du serveur. Le nom du serveur est défini par l'utilisateur.
Type	Affiche le type du serveur.
Priorité	<p>Indique le niveau de priorité affecté au logement du serveur dans le châssis pour l'établissement du bilan de puissance. CMC utilise cette valeur dans ses calculs lorsque l'alimentation doit être réduite ou réattribuée selon les limites d'alimentation définie par l'utilisateur, ou les défaillances des blocs d'alimentation ou des réseaux d'alimentation.</p> <p>Niveaux de priorité : 1 (le plus élevé) à 9 (le plus faible)</p> <p>Par défaut : 1</p> <p>REMARQUE : le niveau de priorité du logement du serveur est associé au logement du serveur, et non au serveur inséré dans le logement. Si vous déplacez un serveur vers un logement différent du châssis ou vers un autre châssis, la priorité précédemment associée au nouveau logement détermine celle du serveur déplacé.</p>
État de l'alimentation	<p>Affiche l'état d'alimentation du serveur :</p> <ul style="list-style-type: none"> ○ - : CMC n'a pas déterminé l'état d'alimentation du serveur. ○ Désactivé : le serveur ou le châssis est désactivé. ○ Activé : le châssis et le serveur sont activés. ○ Activation : tat temporaire entre le mode Désactivé et Activé. Lorsque le cycle d'activation est terminé, l'état d'alimentation passe en mode Activé. ○ Désactivation : état temporaire entre le mode Activé et Désactivé. Lorsque le cycle de désactivation est terminé, l'état d'alimentation passe en mode Désactivé.
Bilan alloué : réel	<p>Indique la quantité d'alimentation allouée au module de serveur.</p> <p>1 Réel : puissance actuelle allouée à chaque serveur.</p>

Tableau 9-15. Blocs d'alimentation du châssis

Élément	Description
Nom	Affiche le nom de l'unité d'alimentation au format PS- <i>n</i> , où <i>n</i> correspond au numéro du bloc d'alimentation.
État de l'alimentation	Indique l'état de l'alimentation de l'unité d'alimentation : En cours d'initialisation, En ligne, En veille, Test de diagnostic, Échec, Inconnu ou Absent (manquant).
Tension d'entrée	Affiche la tension d'entrée actuelle dans le bloc d'alimentation.
Courant d'entrée	Affiche le courant d'entrée actuel dans le bloc d'alimentation.
Alimentation nominale de sortie	Affiche l'alimentation nominale de sortie maximale du bloc d'alimentation.

Configuration du bilan de puissance et de la redondance

Le service de gestion de l'alimentation CMC optimise la consommation électrique pour l'ensemble du châssis (châssis, serveurs, modules d'E/S, iKVM, CMC et unités d'alimentation) et réattribue l'alimentation aux différents modules en fonction de la demande.

Utilisation de l'interface Web

 **REMARQUE** : pour réaliser des tâches de gestion de l'alimentation, vous devez disposer du privilège d'**Administrateur de contrôle du châssis**.

1. Ouvrez une session sur l'interface Web de CMC.
2. Cliquez sur **Présentation du châssis** dans l'arborescence.
3. Cliquez sur **Alimentation** → **Configuration**.

La page **Configuration du bilan/de la redondance** s'affiche.

4. Définissez une ou toutes les propriétés décrites dans le [Tableau 9-16](#) en fonction de vos besoins.
5. Cliquez sur **Appliquer** pour enregistrer les modifications.

Pour actualiser le contenu de la page **Configuration du bilan/de la redondance**, cliquez sur **Actualiser**. Pour en imprimer le contenu, cliquez sur **Imprimer**.

Tableau 9-16. Propriétés du budget/de la redondance d'alimentation configurables

Élément	Description
Limite de la puissance d'entrée système	<p>La limite de la puissance d'entrée système correspond à la quantité maximale de courant alternatif que le système peut allouer aux serveurs et à l'infrastructure du châssis. Cette dernière peut être configurée par l'utilisateur sur n'importe quelle valeur supérieure à celle de l'alimentation minimale nécessaire aux serveurs activés et à l'infrastructure du châssis. La configuration d'une valeur inférieure nécessaire aux serveurs provoque un échec de l'infrastructure du châssis.</p> <p>L'alimentation allouée aux serveurs et à l'infrastructure de châssis se trouve dans l'interface utilisateur à la page Présentation du châssis → Alimentation → Condition du bilan de puissance dans la section Bilan de puissance ou via la commande d'utilitaires CLI <code>RACADM (racadm getpbinfo)</code>.</p> <p>Les utilisateurs peuvent désactiver un ou plusieurs serveurs afin de réduire l'allocation d'alimentation en cours et tenter à nouveau de configurer une valeur inférieure pour la limite de la puissance d'entrée ou simplement configurer la capacité avant de mettre les serveurs sous tension.</p> <p>Pour modifier ce paramètre, vous pouvez entrer une valeur dans n'importe quelle unité. Lors de l'application des modifications, l'interface vérifie que la valeur soumise est bien celle du champ d'unité dernièrement modifié.</p> <p>REMARQUE : pour planifier la capacité, consultez le planificateur de capacité pour les centres de données (DCCP) à l'adresse www.dell.com/calc.</p> <p>REMARQUE : lorsque des modifications de valeur sont spécifiées en watts, la valeur suggérée reflète exactement ce qui est réellement appliqué. Toutefois, lorsque ces modifications sont soumises en BTU/h ou en pourcentage, la valeur soumise peut ne pas refléter exactement ce qui est appliqué. Cette différence vient du fait que ces unités sont converties en watts, puis appliquées (la conversion peut entraîner une erreur d'arrondi).</p>
Règle de redondance	<p>Cette option vous permet de sélectionner l'une des options suivantes :</p> <ol style="list-style-type: none"> 1 Sans redondance : la puissance des blocs d'alimentation est utilisée pour alimenter l'ensemble du châssis, y compris le châssis, les serveurs, les modules d'E/S, iKVM et CMC. Aucun bloc d'alimentation ne doit être gardé en réserve. <p>REMARQUE : le mode Sans redondance utilise uniquement le nombre minimum requis de blocs d'alimentation en même temps. Si le nombre minimum de blocs d'alimentation est installé, il n'y a pas de sauvegarde disponible. La panne de l'un des trois blocs d'alimentation utilisés peut provoquer une perte d'alimentation et/ou de données sur les serveurs. Si le nombre de blocs d'alimentation requis est dépassé, les blocs d'alimentation supplémentaires peuvent être placés en mode de veille afin d'améliorer l'efficacité énergétique si le mode Enclenchement dynamique des blocs d'alimentation est activé.</p> <ol style="list-style-type: none"> 1 Redondance des blocs d'alimentation : la capacité du bloc d'alimentation nominal le plus important dans le châssis est conservée comme alimentation de réserve, garantissant ainsi le maintien de la mise sous tension des modules serveurs ou du châssis en cas de défaillance de l'un des blocs d'alimentation (unité de remplacement). <p>Le mode Redondance des blocs d'alimentation peut ne pas utiliser tous les blocs installés. Les blocs d'alimentation supplémentaires, s'ils sont présents, peuvent être mis en veille afin d'améliorer l'efficacité énergétique si le mode d'enclenchement dynamique des blocs d'alimentation est activé. Le mode Redondance des blocs d'alimentation empêche toute activation des modules de serveur lorsque la consommation de courant du châssis dépasse l'alimentation nominale. La panne de deux blocs d'alimentation peut entraîner la mise hors tension de tout ou partie des modules de serveur se trouvant dans le châssis. Les performances des modules serveurs ne sont pas dégradées dans ce mode.</p> <ol style="list-style-type: none"> 1 Redondance de l'alimentation alternative : ce mode sépare la moitié des unités d'alimentation en deux réseaux d'alimentation (par exemple, les unités d'alimentation 1 à 3 composent le réseau d'alimentation 1 et les unités d'alimentation 4 à 6 le réseau d'alimentation 2). La panne d'une unité d'alimentation ou la perte de l'alimentation alternative vers un réseau indique la perte de la redondance.
Performance du	<p>Lorsqu'elle est activée, cette option favorise la performance du serveur et sa mise sous tension plutôt que le maintien de la</p>

serveur contre redondance de l'alimentation	redondance de l'alimentation. Pour des informations supplémentaires sur cette fonctionnalité, voir Performance du serveur contre redondance de l'alimentation .
Enclenchement dynamique des blocs d'alimentation	Permet la gestion d'énergie dynamique lorsque sélectionné. En mode Enclenchement dynamique , les blocs d'alimentation sont activés (en ligne) ou désactivés (en veille) en fonction de la consommation électrique afin d'optimiser la consommation énergétique dans l'ensemble du châssis. Par exemple, si votre budget d'alimentation s'élève à 5000 watts, votre stratégie de redondance est définie en mode Redondance de l'alimentation alternative et vous disposez de 6 unités d'alimentation. CMC définit 4 unités d'alimentation destinées à la redondance alternative alors que les deux autres restent en mode attente. Si 2 000 W supplémentaires sont requis pour les nouveaux serveurs installés ou si l'efficacité de l'alimentation de la configuration système existante doit être améliorée, les deux blocs d'alimentation en veille sont alors activés.
Désactiver le bouton d'alimentation du châssis	Désactive le bouton d'alimentation du châssis lorsque sélectionné. Si la case est cochée et si vous tentez de modifier l'état de l'alimentation du châssis en appuyant sur le bouton d'alimentation du châssis, l'opération est ignorée.
Autoriser le fonctionnement 110 VCA	Permet une utilisation normale, si les unités d'alimentation sont connectées à une entrée 110 VCA, lorsque sélectionné. Pour plus d'informations, voir Fonctionnement des unités d'alimentation 110 V .
Mode de conservation max	Lorsque sélectionné, active immédiatement le mode de conservation maximale de la puissance. Pour plus d'informations, voir Modes Conservation d'énergie et Conservation max .

Utilisation de la RACADM

Pour activer la redondance et définir la règle de redondance :

 **REMARQUE** : pour réaliser des tâches de gestion de l'alimentation, vous devez disposer du privilège d'**Administrateur de contrôle du châssis**.

- Ouvrez une console série/Telnet/SSH d'accès à CMC, puis ouvrez une session.
- Définissez les propriétés selon vos besoins :

- Pour sélectionner une règle de redondance, tapez la commande :

```
racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy <valeur>
```

où *<valeur>* est égale à **0** (Sans redondance), **1** (Redondance de l'alimentation alternative) ou **2** (Redondance des blocs d'alimentation). L'adresse par défaut est 0.

Par exemple, la commande suivante :

```
racadm config -g cfgChassisPower -o cfgChassisRedundancyPolicy 1
```

définit la règle de redondance sur 1.

- Pour activer ou désactiver l'enclenchement dynamique des unités d'alimentation, tapez la commande :

```
racadm config -g cfgChassisPower -o cfgChassisDynamicPSUEngagementEnable <valeur>
```

où *<valeur>* est égale à **0** (désactiver) ou **1** (activer). L'adresse par défaut est 0.

Par exemple, la commande suivante :

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

désactive l'enclenchement dynamique des unités d'alimentation.

Pour des information supplémentaires sur les commandes RACADM pour l'alimentation du châssis, voir les sections `config`, `getConfig`, `getpbinfo` et `cfgChassisPower` dans le *Guide de référence pour la ligne de commande iDRAC6 et CMC*.

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 que vous affectez à un serveur est liée au logement dans lequel il est installé et non au serveur lui-même. Si vous déplacez le serveur, vous devez redéfinir la priorité à partir de son nouveau logement.

 **REMARQUE** : vous devez disposer du privilège **Administrateur de configuration du châssis** pour effectuer des tâches de gestion de l'alimentation.

Utilisation de l'interface Web

- Ouvrez une session sur l'interface Web de CMC.
- Cliquez sur **Présentation des serveurs** dans l'arborescence. La page **État des serveurs** s'affiche.
- Cliquez sur **Alimentation** → **Priorité des serveurs**.

La page **Priorité des serveurs** affiche tous les serveurs installés dans le châssis.

4. Sélectionnez un niveau de priorité (de 1 à 9, 1 étant le niveau le plus élevé) pour le ou les serveurs voulus. La valeur par défaut est 1. Vous pouvez affecter le même niveau de priorité à plusieurs serveurs.
5. Cliquez sur **Appliquer** pour enregistrer les modifications.

Utilisation de la RACADM

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

```
racadm config -g cfgServerInfo -o cfgServer Priority -i <numéro du 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, la commande suivante :

```
racadm config -g cfgServerInfo -o cfgServer Priority -i 5 1
```

définit le niveau de priorité sur 1 pour le serveur dans le logement 5.

Définition du bilan de puissance

 **REMARQUE** : pour réaliser des tâches de gestion de l'alimentation, vous devez disposer du privilège d'**Administrateur de contrôle du châssis**.

Utilisation de l'interface Web

1. Ouvrez une session sur l'interface Web de CMC.
2. Cliquez sur **Présentation du châssis** dans l'arborescence. La page **Intégrité du châssis** s'affiche.
3. Cliquez sur l'onglet **Alimentation**.
La page **Condition de la consommation de puissance** s'affiche.
4. Cliquez sur le sous-onglet **Configuration**.
La page **Configuration du bilan/de la redondance** s'affiche.
5. Entrez une valeur d'allocation d'énergie allant jusqu'à 11 637 watts dans le champ textuel **Limite de la puissance d'entrée système**.

 **REMARQUE** : le bilan d'alimentation maximal correspond à l'alimentation de l'ensemble de trois unités d'alimentation le plus faible. Si vous tentez de définir une valeur du bilan d'alimentation alternative supérieure, CMC affiche un message de panne.

 **REMARQUE** : lorsque des modifications de valeur sont spécifiées en watts, la valeur suggérée reflète exactement ce qui est réellement appliqué. Toutefois, lorsque les modifications sont soumises en BTU/h ou en pourcentage, la valeur soumise peut ne pas refléter exactement ce qui est réellement appliqué. Cette différence vient du fait que ces unités sont converties en watts, puis appliquées (la conversion peut entraîner une erreur d'arrondi).

6. Cliquez sur **Appliquer** pour enregistrer les modifications.

Utilisation de la RACADM

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

```
racadm config -g cfgChassisPower -o cfgChassisPowerCap <valeur>
```

où <valeur> est un nombre compris entre 2 715 et 11 637 qui représente la limite d'alimentation maximale en watts. La valeur par défaut est 11 637.

Par exemple, la commande suivante :

```
racadm config -g cfgChassisPower -o cfgChassisPowerCap 5400
```

définit le bilan de puissance maximal sur 5 400 watts.

 **REMARQUE** : la limite du bilan d'alimentation correspond à 11 637 watts. Si vous tentez de définir une valeur de bilan d'alimentation alternative supérieure à la capacité d'alimentation du châssis, CMC affiche un message de panne.

Diminution de l'alimentation des serveurs afin de préserver le bilan d'alimentation

CMC réduit les allocations d'alimentation des serveurs de priorité inférieure lorsqu'une alimentation supplémentaire s'avère nécessaire afin de maintenir la consommation électrique du système dans la **limite de la puissance d'entrée système** configurée par l'utilisateur. Par exemple, lorsqu'un nouveau serveur est activé, CMC peut réduire l'alimentation des serveurs de priorité inférieure afin de libérer davantage d'alimentation pour le nouveau serveur. Si cette alimentation demeure insuffisante après réduction des allocations d'alimentation des serveurs de priorité inférieure, CMC diminue les performances des serveurs jusqu'à libération d'une alimentation suffisante pour le nouveau serveur.

CMC réduit l'allocation d'alimentation des serveurs dans deux cas :

- 1 La consommation électrique globale excède la **limite de la puissance d'entrée système** configurable (voir [Définition du bilan de puissance](#).)
- 1 Une panne d'alimentation survient dans le cadre d'une configuration non redondante

Pour plus d'informations sur l'attribution de niveaux de priorité aux serveurs, voir [Exécution de tâches de contrôle de l'alimentation sur le châssis](#).

Exécution de tâches de contrôle de l'alimentation sur le châssis

 **REMARQUE** : pour réaliser des tâches de gestion de l'alimentation, vous devez disposer du privilège d'**Administrateur de contrôle du châssis**.

 **REMARQUE** : les opérations de contrôle de l'alimentation affectent l'intégralité du châssis. Pour les tâches de contrôle de l'alimentation effectuées sur un module d'E/S, voir [Exécution d'opérations de contrôle de l'alimentation sur un module d'E/S](#). Pour les tâches de contrôle de l'alimentation effectuées sur des serveurs, voir [Exécution de tâches de contrôle de l'alimentation sur un serveur](#).

CMC vous permet d'exécuter à distance plusieurs opérations de gestion de l'alimentation, comme par exemple une séquence d'arrêt correcte, sur l'ensemble du châssis (châssis, serveurs, modules d'E/S, iKVM et unités d'alimentation).

Utilisation de l'interface Web

1. Ouvrez une session sur l'interface Web de CMC.

2. Cliquez sur **Présentation du châssis** dans l'arborescence.

3. Cliquez sur l'onglet **Alimentation**.

La page **Condition de la consommation de puissance** s'affiche.

4. Cliquez sur le sous-onglet **Contrôle**.

La page **Contrôle de l'alimentation du châssis** s'affiche.

5. Cliquez sur les boutons radio correspondant pour sélectionner l'une des **opérations de contrôle de l'alimentation** suivantes :

- 1 **Mise sous tension du système** : met le châssis sous tension (équivalent à appuyer sur le bouton d'alimentation quand le châssis est **désactivé**). Cette option est désactivée si le châssis est déjà sous tension.

 **REMARQUE** : cette action met le châssis et autres sous-systèmes (iDRAC sur les serveurs, les modules d'E/S et le module iKVM) sous tension. Les serveurs ne sont pas mis sous tension.

- 1 **Mise hors tension du système** : met le châssis hors tension. Cette option est désactivée si le châssis est déjà hors tension.

 **REMARQUE** : cette action met le châssis hors tension (châssis, serveurs, modules d'E/S, module iKVM et blocs d'alimentation). Les modules CMC restent sous tension, mais en veille virtuelle ; dans cet état, un bloc d'alimentation et des ventilateurs refroidissent les modules CMC. Le bloc d'alimentation alimente également les ventilateurs qui fonctionnent à vitesse réduite.

- 1 **Exécuter un cycle d'alimentation sur le système (redémarrage à froid)** : arrête, puis redémarre le système. Cette option est désactivée si le châssis est déjà hors tension.

 **REMARQUE** : cette action met hors tension puis redémarre l'ensemble du châssis (le châssis, les serveurs configurés pour être sous tension en permanence, les modules d'E/S, l'iKVM et les blocs d'alimentation).

- 1 **Réinitialiser CMC** : réinitialise CMC sans arrêter le système (redémarrage à chaud). (Cette option est désactivée lorsque CMC est déjà arrêté.)

 **REMARQUE** : cette action redémarre uniquement CMC. Elle n'a aucun effet sur les autres composants.

- 1 **Arrêt anormal** : force la coupure de l'alimentation de tout le châssis (châssis, serveurs, modules d'E/S, module iKVM et blocs d'alimentation). Cette action ne permet pas l'arrêt normal du système d'exploitation des serveurs avant la mise hors tension.

6. Cliquez sur **Appliquer**. Une boîte de dialogue vous demande de confirmer l'opération.

7. Cliquez sur **OK** pour exécuter l'action de gestion de l'alimentation (réinitialisation du système, par exemple).

Utilisation de la RACADM

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

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

où <action> a pour valeur `powerup` (mise sous tension), `powerdown` (mise hors tension), `powercycle` (cycle d'alimentation), `nongraceshutdown` (coupure franche) ou `reset` (réinitialisation).

Exécution d'opérations de contrôle de l'alimentation sur un module d'E/S

Vous pouvez exécuter à distance une opération de réinitialisation ou lancer un cycle d'alimentation sur un module d'E/S.

 **REMARQUE** : pour réaliser des tâches de gestion de l'alimentation, vous devez disposer du privilège d'**Administrateur de contrôle du châssis**.

Utilisation de l'interface Web

1. Ouvrez une session sur l'interface Web de CMC.
2. Sélectionnez **Présentation des modules d'E/S**.
La page **Condition des modules d'E/S** s'affiche.
3. Cliquez sur l'onglet **Alimentation**.
La page **Contrôle de l'alimentation** s'affiche.
4. Sélectionnez l'opération à exécuter (**réinitialiser** ou **cycle d'alimentation**) dans le menu déroulant situé en regard du module d'E/S correspondant dans la liste.
5. Cliquez sur **Appliquer**.
Une boîte de dialogue vous demande de confirmer l'opération.
6. Cliquez sur **OK** pour exécuter l'action de gestion de l'alimentation (par exemple, lancer un cycle d'alimentation du module d'E/S).

Utilisation de la RACADM

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

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

où <n> est un nombre compris entre 1 et 6 qui indique le module d'E/S (A1, A2, B1, B2, C1, C2) et <action> l'opération à exécuter : `cycle d'alimentation` ou `réinitialisation`.

Exécution de tâches de contrôle de l'alimentation sur un serveur

 **REMARQUE** : pour réaliser des tâches de gestion de l'alimentation, vous devez disposer du privilège d'**Administrateur de contrôle du châssis**.

CMC vous permet d'exécuter à distance plusieurs actions de gestion de l'alimentation sur un serveur donné du châssis, par exemple une séquence d'arrêt correcte.

Utilisation de l'interface Web

1. Ouvrez une session sur l'interface Web de CMC.
2. Développez **Présentation des serveurs** dans l'arborescence système, puis sélectionnez le serveur auquel vous souhaitez appliquer une opération de contrôle de l'alimentation. La page **Condition du serveur** s'affiche.
3. Cliquez sur l'onglet **Alimentation**.
La page **Gestion de l'alimentation du serveur** s'affiche.
4. **État de l'alimentation** : affiche l'un des états d'alimentation du serveur suivants :

- 1 - : CMC n'a pas encore déterminé l'état d'alimentation du serveur.
 - 1 **Désactivé** : le serveur ou le châssis est hors tension.
 - 1 **Activé** : le châssis et le serveur sont sous tension.
 - 1 **Activation** : état temporaire entre le mode Désactivé et Activé. Lorsque l'action est terminée, l'**État d'alimentation** est **activé**.
 - 1 **Mise hors tension** : état temporaire entre le mode Activé et Désactivé. Lorsque l'action est terminée, l'**État d'alimentation** est **désactivé**.
5. Sélectionnez l'une des **opérations de contrôle de l'alimentation** suivantes en cliquant sur le bouton d'option correspondant :
- 1 **Mise sous tension du système** : met le serveur sous tension (équivalent à appuyer sur le bouton d'alimentation quand le système est hors tension). Cette option est désactivée si le serveur est déjà sous tension.
 - 1 **Mise hors tension du système** : met le serveur hors tension (équivalent à appuyer sur le bouton d'alimentation quand le système est sous tension).
 - 1 **Arrêt normal** : arrête le serveur, puis le redémarre.
 - 1 **Réinitialisation du serveur (redémarrage à chaud)** : redémarre le serveur sans l'arrêter. Cette option est désactivée si le serveur est hors tension.
 - 1 **Mettre le serveur en cycle d'alimentation (redémarrage à froid)** : arrête, puis redémarre le serveur. Cette option est désactivée si le serveur est hors tension.
6. Cliquez sur **Appliquer**. Une boîte de dialogue vous demande de confirmer l'opération.
7. Cliquez sur **OK** pour lancer la tâche de gestion de l'alimentation (réinitialisation du serveur, par exemple).

 **REMARQUE** : toutes les opérations de contrôle de l'alimentation peuvent être effectuées sur plusieurs serveurs depuis la page **Serveurs** → **Alimentation** → **Contrôle**.

Utilisation de la RACADM

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

```
racadm serveraction -m <module> <action>
```

où *<module>* désigne le serveur par son numéro d'emplacement dans le châssis (de 1 à 16) et *<action>* indique l'opération à exécuter : *powerup* (mettre sous tension), *powerdown* (mettre hors tension), *powercycle* (cycle d'alimentation), *graceshutdown* (arrêt normal) ou *hardreset* (réinitialisation matérielle).

Fonctionnement 110 V

Certains modèles d'unités d'alimentation sont capables de fonctionner à la fois en 220 V et 110 V. L'alimentation 110 V peut avoir une capacité limitée ; lorsqu'une connexion 110 V est détectée, le châssis n'accorde pas de demande supplémentaire d'alimentation de serveur jusqu'à ce que l'utilisateur accepte le fonctionnement 110 V en changeant la propriété de configuration de la puissance. L'utilisateur doit vérifier que le circuit 110 V en cours d'utilisation peut fournir la puissance nécessaire pour la configuration du châssis avant l'acceptation. Après acceptation, le châssis accorde toutes les futures demandes appropriées d'alimentation de serveur et utilise toute la capacité de puissance disponible.

L'utilisateur peut réinitialiser l'acceptation du 110V à tout moment depuis l'interface graphique ou RACADM après l'installation initiale. Les entrées de blocs d'alimentation sont enregistrées dans le journal lorsque les blocs d'alimentation 110V sont détectés et retirés. Les entrées de blocs sont également enregistrées dans le journal lorsqu'ils sont reconnus ou non reconnus par l'utilisateur.

L'intégrité globale énergétique est au moins à l'état non critique lorsque le châssis est en mode 110 V et que l'utilisateur n'a pas reconnu ce mode. L'icône « Avertissement » est affichée sur la page principale de l'interface utilisateur quand l'état est non critique.

Le mode mixte 110 V et 220 V n'est pas pris en charge. Si CMC détecte que les deux tensions sont en cours d'utilisation, une tension est sélectionnée et les blocs d'alimentation reliés à l'autre tension sont mis hors tension et marqués comme défaillants.

Dépannage

Pour le dépannage de problèmes d'alimentation et de puissance, voir [Dépannage et récupération](#).

[Retour à la page Contenu](#)

[Retour à la page Contenu](#)

Utilisation de l'interface de ligne de commande RACADM

Micrologiciel Dell Chassis Management Controller Version 3.1 Guide d'utilisation

- [Utilisation d'une console série, Telnet ou SSH](#)
- [Utilisation de la RACADM](#)
- [Utilisation de RACADM pour la configuration CMC](#)
- [Configuration des propriétés du réseau CMC](#)
- [Utilisation de RACADM pour la configuration des utilisateurs](#)
- [Utilisation de RACADM pour configurer l'authentification par clé publique sur SSH](#)
- [Configuration de l'envoi de notifications par e-mail ou d'alertes SNMP](#)
- [Configuration de plusieurs CMC dans plusieurs châssis](#)
- [Utilisation de RACADM pour configurer les propriétés sur iDRAC](#)
- [Dépannage](#)

L'utilitaire RACADM fournit une série de commandes qui vous permet de configurer de gérer CMC via une interface textuelle. L'utilitaire RACADM est accessible grâce à une connexion Telnet/SSH ou série, à l'aide de la console CMC Dell du module iKVM ou à distance à l'aide de l'interface de ligne de commande RACADM installée sur la station de gestion.

L'interface RACADM est classée comme suit :

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

1. 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 de CMC.
1. Micrologiciel RACADM : permet de se connecter à CMC à l'aide d'une connexion Telnet, SSH, série ou du module iKVM. Le micrologiciel RACADM permet la mise en œuvre de RACADM (qui fait partie du micrologiciel CMC).

Vous pouvez utiliser des commandes de RACADM distant dans des scripts pour configurer plusieurs contrôleurs CMC. CMC ne prend pas en charge les scripts de sorte que vous ne pouvez pas exécuter directement des scripts sur CMC. Pour plus d'informations sur la configuration de plusieurs contrôleurs CMC, voir [Configuration de plusieurs CMC dans plusieurs châssis](#).

Utilisation d'une console série, Telnet ou SSH

Vous pouvez ouvrir une session CMC via une connexion série ou Telnet/SSH, ou encore via la console Dell CMC du module iKVM. Pour la configuration d'un accès à distance ou en série à CMC, voir [Configuration de CMC pour utiliser des consoles de ligne de commande](#). Les options de sous-commandes couramment utilisées sont répertoriées dans [Tableau 4-2](#). Une liste exhaustive des sous-commandes RACADM est répertoriée dans le chapitre Sous-commandes RACADM du *Guide de référence de la ligne de commande pour iDRAC6 et CMC*.

Ouverture d'une session CMC

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

1. Connectez-vous à 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.

Démarrage d'une console texte

Vous pouvez ouvrir une session sur CMC via un réseau Telnet ou SSH, un port série ou la console Dell CMC de l'iKVM. Ouvrez une session Telnet ou SSH, connectez-vous et ouvrez une session sur CMC.

Pour plus d'informations sur la connexion à CMC via le module iKVM, voir [Utilisation du module iKVM](#).

Utilisation de la RACADM

Les sous-commandes RACADM peuvent être exécutées à distance à partir de l'invite de commande d'une console série, Telnet ou SSH, ou d'une invite de commande normale.

Utilisez les sous-commandes RACADM pour configurer les propriétés CMC et effectuer des tâches de gestion à distance. Pour afficher la liste des sous-commandes RACADM, tapez :

```
racadm help
```

Utilisé sans option ou sous-commande, RACADM affiche des informations de syntaxe et des instructions sur la manière d'accéder aux sous-commandes et à l'aide. Pour obtenir la liste des options de syntaxe et de ligne de commande des différentes sous-commandes, tapez :

```
racadm help <sous-commande>
```

Sous-commandes RACADM

Le [Tableau 4-1](#) fournit une liste abrégée des sous-commandes les plus courantes utilisées dans RACADM. Pour une liste exhaustive des sous-commandes RACADM, comprenant la syntaxe et les entrées valides, reportez-vous au chapitre Sous-commandes RACADM du *Guide de référence de la ligne de commande pour iDRAC6 et CMC*.

 **REMARQUE** : la commande `connect` est disponible en tant que commande RACADM et en tant que commande CMC intégrée. Les commandes `exit`, `quit` et `logout` sont des commandes CMC intégrées, et non des commandes RACADM. Aucune de ces commandes ne peut être utilisée avec RACADM distant. Pour plus d'informations sur l'utilisation de ces commandes, consultez [Connexion aux serveurs ou aux modules d'E/S à l'aide de la commande Connect](#).

Tableau 4-1. Sous-commandes RACADM

Commande	Description
help	Répertorie les descriptions des sous-commandes CMC.
help < sous-commande >	Répertorie une synthèse de l'utilisation de la sous-commande spécifiée.
?	Répertorie les descriptions des sous-commandes CMC.
? < sous-commande >	Répertorie une synthèse de l'utilisation de la sous-commande spécifiée.
arp	Affiche le contenu de la table ARP. Les entrées de la table ARP ne peuvent être ni ajoutées, ni supprimées.
chassisaction	Exécute les opérations power-up, power-down, reset et power-cycle sur le châssis, le commutateur et le module KVM.
closeasn	Ferme une session.
clrraclog	Efface le journal CMC et crée une entrée unique qui indique l'utilisateur et l'heure d'effacement du journal.
clrsel	Efface les entrées du journal des événements système.
cmchangeover	Modifie l'état de CMC d'actif à veille ou vice versa, dans les environnements CMC redondants.
config	Configure CMC.
connect	Se connecte à la console série d'un serveur ou d'un module d'E/S. Voir Connexion aux serveurs ou aux modules d'E/S à l'aide de la commande Connect pour obtenir de l'aide sur l'utilisation de la sous-commande connect.
deploy	Déploie un serveur en spécifiant les propriétés requises.
feature	Affiche les fonctionnalités actives et non actives.
featurecard	Affiche des informations sur l'état de la carte de fonction.
fwupdate	Effectue des mises à jour du micrologiciel de composant du système et affiche l'état de la mise à jour.
getassettag	Affiche le numéro d'inventaire du châssis.
getchassisname	Affiche le nom du châssis.
getconfig	Affiche les propriétés de configuration CMC actuelles.
getdcinfo	Affiche les informations générales relatives aux défaillances de configuration du module d'E/S et de la carte fille.
getflexaddr	Affiche l'état activé/désactivé de la fonctionnalité FlexAddress en fonction de la relation emplacement/structure. Si elle est utilisée avec l'option -i, la commande affiche l'adresse WWN et MAC d'un emplacement spécifique.
getioinfo	Affiche des informations générales relatives au module d'E/S.
getkvminfo	Affiche des informations concernant le module iKVM.
getled	Affiche les paramètres des LED d'un module.
getmacaddress	Affiche l'adresse MAC d'un serveur.
getmodinfo	Affiche les informations de configuration et de condition d'un module.
getniccfg	Affiche la configuration IP actuelle du contrôleur.
getpbinfo	Affiche des informations sur la condition du bilan de puissance.
getpminfo	Affiche des informations sur la condition de la gestion d'alimentation.
getraclog	Affiche le journal CMC.
getractime	Affiche l'heure CMC.
getredundancymode	Affiche le mode de redondance CMC.
getsel	Affiche le journal des événements système (journal du matériel).
getsensorinfo	Affiche des informations concernant les capteurs du système.
getslotname	Affiche le nom d'un logement du châssis.
getssninfo	Affiche des informations sur les sessions actives.
getsvctag	Affiche les numéros de service.
getsysinfo	Affiche des informations générales concernant CMC et le système.
gettracelog	Affiche le journal CMTrace. Si elle est utilisée avec l'option -i, la commande affiche le nombre d'entrées du journal de suivi CMC.
getversion	Affiche la version actuelle du logiciel, les informations sur le modèle et indique si le périphérique peut être mis à jour.
ifconfig	Affiche la configuration IP CMC actuelle.
krbkeytabupload	Téléverse un keytab Kerberos dans CMC.
netstat	Affiche la table de routage et les connexions actuelles.
ping	Vérifie que l'adresse IPv4 de destination est accessible à partir de CMC avec le contenu actuel du tableau de routage.

ping6	Vérifie que l'adresse IPv6 de destination est accessible à partir de CMC avec le contenu actuel du tableau de routage.
racdump	Affiche l'état du châssis complet, des informations sur l'état de configuration, ainsi que des journaux d'événements de l'historique. Utilisée pour vérifier la configuration après le déploiement et pendant les sessions de débogage.
racreset	Réinitialise CMC.
racresetcfg	Restaure la configuration CMC par défaut.
remoteimage	Connecte, déconnecte ou déploie un fichier de média sur un serveur distant
serveraction	Effectue des opérations de gestion de l'alimentation sur le système géré.
setassettag	Définit le numéro d'inventaire du châssis.
setchassisname	Définit le nom du châssis.
setflexaddr	Active/désactive FlexAddress sur un emplacement/structure spécifique, lorsque la fonctionnalité FlexAddress est activée sur le châssis.
setled	Définit les paramètres des LED d'un module.
setniccfg	Définit la configuration IP du contrôleur.
setractime	Définit l'heure CMC.
setslotname	Définit le nom d'un logement dans le châssis.
setsysinfo	Définit le nom et l'emplacement du châssis.
sshpkauth	Téléverse jusqu'à 6 différentes clés SSH publiques, supprime des clés existantes et affiche les clés déjà existantes dans CMC.
sslcertdownload	Télécharge un certificat signé par une autorité de certification.
sslcertupload	Téléverse un certificat signé par une autorité de certification ou un certificat de serveur vers CMC.
sslcertview	Affiche un certificat signé par une autorité de certification ou un certificat de serveur dans CMC.
sslcsrgen	Génère et télécharge la RSC SSL.
sslresetcfg	Restaure le certificat auto-signé utilisé par l'interface utilisateur Web CMC.
testemail	Force CMC à envoyer un e-mail en passant par le NIC de CMC.
testfeature	Vous permet de vérifier les paramètres de configuration d'une fonctionnalité donnée. Par exemple, il prend en charge le test de la configuration Active Directory avec l'authentification simple (nom d'utilisateur et mot de passe) ou l'authentification Kerberos (connexion directe ou ouverture de session par carte à puce).
testtrap	Force CMC à envoyer une alerte SNMP via la carte d'interface réseau CMC.
traceroute	Imprime le trajet emprunté par les paquets IPv4 vers un nud réseau.
traceroute6	Imprime le trajet emprunté par les paquets IPv6 vers un nud réseau.

Accès à distance à RACADM

Tableau 4-2. Options des sous-commandes de RACADM distant

Option	Description
-r <racIpAddr>	Spécifie l'adresse IP distante du contrôleur.
-r <racIpAddr>:<port>	Utilisez <numéro de port> lorsque le numéro de port CMC n'est pas le port par défaut (443)
-i	Ordonne à RACADM de demander le nom d'utilisateur et le mot de passe à l'utilisateur de manière interactive.
-u <nom_utilisateur>	Spécifie le nom d'utilisateur qui est utilisé pour authentifier la transaction de commande. Si l'option -u est utilisée, l'option -p doit l'être également et l'option -i (interactive) n'est pas autorisée.
-p <mot de passe>	Spécifie le mot de passe utilisé pour authentifier la transaction de commande. Si l'option -p est utilisée, l'option -i n'est pas autorisée.

Pour accéder à distance à RACADM, tapez les commandes suivantes :

```
racadm -r <adresse IP CMC> -u <nom d'utilisateur> -p <mot de passe> <sous-commande> <options de la sous-commande>
```

```
racadm -i -r <adresse IP CMC> <sous-commande> <options de la sous-commande>
```

 **REMARQUE** : l'option -i ordonne à RACADM de demander le nom d'utilisateur et le mot de passe de manière interactive. Sans l'option -i, vous devez indiquer le nom d'utilisateur et le mot de passe dans la commande à l'aide des options -u et -p.

Par exemple :

```
racadm -r 192.168.0.120 -u root -p calvin getsysinfo
```

```
racadm -i -r 192.168.0.120 getsysinfo
```

Si le numéro de port HTTPS CMC a été remplacé par un port personnalisé autre que le port par défaut (443), la syntaxe suivante doit être utilisée :

```
racadm -r <adresse IP CMC>:<port> -u <nom d'utilisateur> -p <mot de passe> <sous-commande> <options de la sous-commande>
```

```
racadm -i -r <adresse IP CMC>:<port> <sous-commande> <options de la sous-commande>
```

Activation et désactivation de la fonctionnalité distante de RACADM

 **REMARQUE** : Dell recommande l'exécution de ces commandes sur le châssis.

La fonctionnalité distante de RACADM est activée par défaut sur CMC. Dans les commandes suivantes, l'option `-g` précise le groupe de configuration auquel appartient l'objet et l'option `-o` précise l'objet de configuration à configurer.

Pour désactiver la fonctionnalité distante de RACADM, tapez :

```
racadm config -g cfgRacTuning -o cfgRacTuneRemoteRacadmEnable 0
```

Pour réactiver la fonctionnalité distante de RACADM, tapez :

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

Utilisation de la RACADM à distance

 **REMARQUE** : configurez l'adresse IP de CMC avant d'utiliser la fonctionnalité distante de RACADM. Pour plus d'informations sur la configuration de CMC, voir [Installation et configuration de CMC](#).

L'option distante (`-r`) de la console RACADM vous permet de vous connecter au système géré et d'exécuter des sous-commandes RACADM à partir d'une console ou d'une station de gestion distante. Pour utiliser la capacité distante, vous avez besoin d'un nom d'utilisateur (option `-u`) et d'un mot de passe (option `-p`) valides, ainsi que de l'adresse IP de CMC.

Avant d'essayer d'accéder à distance à RACADM, vérifiez que vous disposez des autorisations nécessaires. Pour afficher vos privilèges utilisateur, tapez :

```
racadm getconfig -g cfguseradmin -i n
```

où `n` est votre réf. utilisateur (1 à 16).

Si vous ne connaissez pas votre réf. utilisateur, essayez différentes valeurs pour `n`.

 **REMARQUE** : la fonctionnalité distante de RACADM est uniquement prise en charge sur les stations de gestion via un navigateur pris en charge. Pour plus d'informations, consultez la section Navigateurs pris en charge de la *Matrice de prise en charge des logiciels des systèmes Dell* sur le site Web du support de Dell à l'adresse support.dell.com/manuals.

 **REMARQUE** : lorsque vous utilisez la fonctionnalité distante de RACADM, vous devez posséder un droit d'écriture pour les dossiers sur lesquels vous exécutez des sous-commandes RACADM impliquant des opérations sur les fichiers. Par exemple :

```
racadm getconfig -f <nom de fichier> -r <adresse IP>
```

ou

```
racadm sslcertupload -t 1 -f c:\cert\cert.txt
```

Lorsque vous utilisez RACADM distant pour capturer les groupes de configuration dans un fichier, si aucune propriété de clé n'est définie dans un groupe, le groupe de configuration n'est pas enregistré en tant qu'élément du fichier de configuration. Si ces groupes de configuration doivent être clonés sur d'autres contrôleurs CMC, la propriété de clé doit être définie avant d'exécuter la commande `getconfig -f`. Sinon, vous pouvez saisir manuellement les propriétés manquantes dans le fichier de configuration après avoir exécuté la commande `getconfig -f`. Ceci s'applique à tous les groupes racadm indexés.

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

Messages d'erreur RACADM

Pour des informations concernant les messages d'erreur de l'interface de ligne de commande RACADM, voir [Dépannage](#).

Utilisation de RACADM pour la configuration CMC

 **REMARQUE** : pour la configuration initiale du CMC, vous devez être connecté en tant qu'utilisateur `root` pour exécuter des commandes RACADM sur un système distant. Un autre utilisateur doté de privilèges permettant la configuration du CMC peut être créé.

L'interface Web CMC permet de configurer rapidement CMC (voir [Utilisation de l'interface Web de CMC](#)). Toutefois, si vous préférez la configuration par ligne de commande ou script, ou si vous devez configurer plusieurs contrôleurs CMC, utilisez RACADM distant installé avec les agents CMC sur la station de gestion.

Configuration des propriétés du réseau CMC

Préalablement à la configuration CMC, vous devez configurer les paramètres réseau CMC afin de permettre la gestion à distance de CMC. Cette configuration initiale définit les paramètres de mise en réseau TCP/IP qui permettent l'accès à CMC.

Configuration de l'accès initial à CMC

Cette section explique comment exécuter la configuration réseau initiale CMC à l'aide des commandes RACADM. Toutes les opérations de configuration décrites dans cette section peuvent être effectuées à l'aide de l'écran LCD du panneau avant. Voir [Configuration de la mise en réseau à l'aide de l'assistant de configuration de l'écran LCD](#).

 **PRÉCAUTION** : la modification des paramètres sur l'écran Paramètres réseau CMC peut entraîner la déconnexion de votre connexion réseau actuelle.

Pour plus d'informations sur les sous-commandes réseau, consultez les chapitres Sous-commandes RACADM et Définitions des groupes et des objets de la base de données des propriétés du *Guide de référence de la ligne de commande pour iDRAC et CMC*.

 **REMARQUE** : vous devez disposer de privilèges **Administrateur de configuration du châssis** pour configurer les paramètres réseau CMC.

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

Affichage des paramètres réseau IPv4 actuels

Pour afficher un résumé des paramètres du NIC, DHCP, de vitesse réseau et du mode duplex, tapez :

```
racadm getniccfg
```

ou

```
racadm getconfig -g cfgCurrentLanNetworking
```

Affichage des paramètres réseau IPv6 actuels

Pour afficher un résumé des paramètres réseau, tapez :

```
racadm getconfig -g cfgIPv6LanNetworking
```

Pour afficher les informations sur l'adressage IPv4 et IPv6 correspondant au type de châssis :

```
racadm getsysinfo
```

Par défaut, CMC demande et obtient automatiquement une adresse IP auprès du serveur DHCP (Protocole de configuration dynamique des hôtes).

Vous pouvez désactiver cette fonctionnalité et préciser l'adresse IP statique de CMC, la passerelle et le masque de sous-réseau.

Pour désactiver DHCP et préciser l'adresse IP statique de CMC, la passerelle et le masque de sous-réseau, tapez :

```
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>
```

Affichage des paramètres réseau actuels

Pour afficher un résumé des paramètres du NIC, DHCP, de vitesse réseau et du mode duplex, tapez :

```
racadm getniccfg
```

ou

```
racadm getconfig -g cfgCurrentLanNetworking
```

Pour afficher l'adresse IP et les informations DHCP, d'adresse MAC et du DNS pour le châssis, tapez :

racadm getsysinfo

Configuration des paramètres du réseau local

-  **REMARQUE** : pour effectuer les étapes suivantes, vous devez disposer des privilèges **Administrateur de configuration du châssis**.
-  **REMARQUE** : les paramètres du réseau local tels que, la chaîne de communauté et l'adresse IP du serveur SMTP, affectent CMC et les paramètres externes du châssis.
-  **REMARQUE** : 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.
-  **REMARQUE** : lorsque IPv6 est activé au moment du démarrage, trois demandes de routeur sont envoyées toutes les quatre secondes. Si des commutateurs réseau externes exécutent le protocole Spanning Tree (SPT), les ports du commutateur externe peuvent être bloqués pendant plus de douze secondes pendant lesquelles les demandes de routeur IPv6 sont envoyées. Dans de tels cas, la connectivité IPv6 peut être limitée jusqu'à ce que des annonces de routeur soient gratuitement envoyées par les routeurs IPv6.

Activation de l'interface réseau CMC

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

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

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

-  **REMARQUE** : le NIC de CMC est activé par défaut.

Pour activer/désactiver l'adressage IPv4 de CMC, tapez :

```
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 l'adressage IPv6 de CMC, tapez :

```
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, CMC demande et obtient automatiquement une adresse IP CMC auprès du serveur DHCP (protocole de configuration dynamique des hôtes). Vous pouvez désactiver la fonctionnalité DHCP et préciser l'adresse IP CMC statique, la passerelle et le masque de sous-réseau.

Pour un réseau IPv4, pour désactiver DHCP et préciser l'adresse IP CMC statique, la passerelle et le masque de sous-réseau, tapez :

```
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.

Pour un réseau IPv6, pour désactiver la fonctionnalité Configuration automatique et spécifier une adresse IPv6 CMC statique, une passerelle et une longueur de préfixe, tapez :

```
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 du protocole DHCP pour l'adresse IP du NIC de CMC demande et obtient automatiquement une adresse IP auprès du serveur DHCP (protocole de configuration dynamique des hôtes). Cette fonctionnalité est activée par défaut.

Vous pouvez désactiver la fonctionnalité DHCP pour l'adresse du NIC et préciser 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 du protocole DHCP pour les adresses IP du DNS

La fonctionnalité d'utilisation du protocole DHCP pour l'adresse du DNS de CMC est désactivée par défaut. Lorsqu'elle est activée, cette fonctionnalité obtient les adresses principale et secondaire du serveur DNS auprès du serveur DHCP. Si vous utilisez cette fonctionnalité, vous n'avez pas à configurer d'adresses IP statiques pour le serveur 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, tapez :

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

Pour désactiver la fonctionnalité DHCP pour les adresses DNS pour IPv6 et spécifier les adresses statiques préférées et alternatives du serveur DNS, tapez :

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

Définition des adresses IP statiques du DNS

 **REMARQUE** : les paramètres des adresses IP de DNS statique ne sont pas valides tant que la fonction adresse DNS pour DHCP est désactivée.

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

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

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

Pour IPv6, pour définir les adresses IP préférées et secondaires du serveur DNS, tapez :

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

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

Configuration des paramètres DNS (IPv4 et IPv6)

- 1 **Enregistrement CMC** : pour enregistrer CMC sur le serveur DNS, tapez :

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

 **REMARQUE** : certains serveurs DNS ne peuvent enregistrer que des noms de 31 caractères maximum. Assurez-vous que le nom désigné se trouve dans la limite DNS requise.

 **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.

- 1 **Nom CMC** : le nom par défaut du contrôleur CMC sur le serveur DNS est `cmc-<numéro de service>`. Pour modifier le nom CMC sur le serveur DNS, tapez :

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

où `<nom>` est une chaîne de 63 caractères alphanumériques et traits d'union maximum. Par exemple, `cmc-1` ou `d-345`.

- 1 **Nom de domaine DNS** : le nom de domaine DNS par défaut contient un espace unique. Pour définir un nom de domaine DNS, tapez :

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

où `<nom>` est une chaîne de 254 caractères alphanumériques et traits d'union maximum. Par exemple : `p45, a-tz-1` ou `r-id-001`.

Configuration de l'auto-négociation, du mode duplex et de la vitesse du réseau (IPv4 et IPv6)

Lorsqu'elle est activée, la fonctionnalité Négociation automatique détermine si CMC définit automatiquement le mode duplex et la vitesse réseau en entrant en communication 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>` correspond à 10 ou 100 (par défaut).

Configuration du VLAN CMC (IPv4 et IPv6)

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

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

2. Spécifiez l'ID de VLAN pour le réseau de gestion du châssis externe :

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

Les valeurs valides pour <VLAN id> sont comprises entre 1- 4000 et 4021- 4094. La valeur par défaut est 1.

Par exemple :

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

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

```
racadm config -g cfgLanNetworking -o cfgNicVlanPriority <priorité VLAN>
```

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

Par exemple :

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

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

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

Par exemple :

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

Suppression du VLAN de CMC

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 d'un VLAN de serveur

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- 4000 et 4021- 4094. La valeur par défaut est 1.

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

Par exemple :

```
racadm setniccfg -m server-1 -v 1 7
```

Suppression d'un VLAN de serveur

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
```

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

La propriété MTU permet la définition d'une limite de taille pour les paquets pouvant être transmis via l'interface. Pour définir cette propriété MTU, tapez :

```
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 requiert une MTU minimale de 1 280. Si IPv6 est activé et que `cfgNetTuningMtu` est défini sur une valeur inférieure, CMC utilisera une MTU de 1 280.

Configuration de l'adresse IP du serveur SMTP (IPv4 et IPv6)

Vous pouvez activer CMC pour l'envoi d'alertes par e-mail via le protocole SMTP (Simple Mail Transfer Protocol) vers une adresse IP spécifiée. Pour activer cette fonctionnalité, tapez :

```
racadm config -g cfgRemoteHosts -o cfgRhostsSmtServerIpAddr <adresse IP SMTP>
```

où <adresse IP SMTP> est l'adresse IP du serveur SMTP du réseau.

 **REMARQUE** : si votre réseau dispose d'un serveur SMTP qui diffuse et renouvelle périodiquement les baux d'adresses IP et si les adresses sont différentes, ce paramètre de propriété ne fonctionne pas pendant un certain temps en raison des modifications apportées à l'adresse IP spécifiée du serveur SMTP. Si c'est le cas, utilisez le nom DNS.

Configuration des paramètres de sécurité réseau (IPv4 uniquement)

 **REMARQUE** : pour effectuer les étapes suivantes, vous devez disposer des privilèges **Administrateur de configuration du châssis**.

Activation de la vérification de plage d'adresses IP (IPv4 uniquement)

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 :

- 1 `cfgRacTuneIpRangeAddr`
- 1 `cfgRacTuneIpRangeMask`

L'ouverture de session à partir de l'adresse IP entrante est autorisée uniquement si les deux éléments suivants sont identiques :

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

Utilisation de RACADM pour la configuration des utilisateurs

Avant de commencer

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 des utilisateurs actuels. Si vous configurez un nouveau contrôleur CMC ou avez exécuté la commande `racresetcEgde` de RACADM, le seul utilisateur actuel est `root`, avec le mot de passe `calvin`. La sous-commande `racresetcfg` restaure les paramètres CMC par défaut d'origine.

 **PRÉCAUTION** : **Utilisez la commande `racresetcfg` avec précaution car elle restaure les valeurs par défaut de tous les paramètres de configuration. Toute modification précédente est perdue.**

 **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 tapez la commande suivante une fois pour chaque indice compris entre 1 et 16 :

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

Plusieurs paramètres et références d'objet sont affichés avec leurs valeurs actuelles. Les deux objets d'intérêt sont :

```
# cfgUserAdminIndex=XX
```

```
cfgUserAdminUserName=
```

Si l'objet `cfgUserAdminUserName` n'a pas de valeur, ce numéro d'index, indiqué par l'objet `cfgUserAdminIndex`, peut être utilisé. Si un nom suit le signe « = », l'index est pris par ce nom d'utilisateur.

REMARQUE : lorsque vous activez ou désactivez manuellement un utilisateur avec la sous-commande `racadm config`, vous devez spécifier l'index via l'option `-i`. L'objet `cfgUserAdminIndex` affiché dans l'exemple précédent contient un caractère « # ». De même, si vous utilisez la commande `racadm config -f racadm.cfg` pour spécifier 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 permet une plus grande flexibilité dans la configuration d'un second contrôleur CMC possédant les mêmes paramètres que le contrôleur CMC principal.

Ajout d'un utilisateur CMC

Pour ajouter un nouvel utilisateur à la configuration CMC, quelques commandes élémentaires sont disponibles. Procédez comme suit :

1. Définissez le nom d'utilisateur.
2. Définissez le mot de passe.
3. Définissez les privilèges utilisateur. Pour des informations supplémentaires sur les privilèges d'utilisateur, voir [Table 5-40](#), et [Table 5-41](#) dans le chapitre Propriétés de la base de données du *Guide de référence de la ligne de commande pour iDRAC6 et CMC*.
4. Activez l'utilisateur.

Exemple

L'exemple suivant décrit l'ajout d'un nouvel utilisateur appelé « Jean » avec un mot de passe « 123456 » et des privilèges d'ouverture de session CMC.

REMARQUE : consultez le tableau 3-1 du chapitre Propriétés de la base de données du *Guide de référence de la ligne de commande pour iDRAC6 et CMC* pour obtenir la liste des valeurs de masque binaire valides correspondant à des privilèges d'utilisateur spécifiques. La valeur de privilège par défaut est 0, indiquant que l'utilisateur n'a aucun privilège activé.

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

Pour vérifier qu'un utilisateur a bien été ajouté avec les privilèges corrects, utilisez l'une des commandes suivantes :

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

Utilisation de RACADM pour configurer l'authentification par clé publique sur SSH

Avant de commencer

Vous pouvez configurer jusqu'à 6 clés publiques pouvant être utilisées avec le nom d'utilisateur du service sur l'interface SSH. Avant d'ajouter ou de supprimer des clés publiques, veillez à utiliser la commande `view` pour voir les clés qui sont déjà configurées afin de ne pas écraser ou supprimer une clé accidentellement. Le nom d'utilisateur du service est un compte d'utilisateur spécial qui peut être utilisé lors de l'accès à CMC via SSH. Lorsque le PKA sur SSH est installé et utilisé correctement, vous ne devez pas entrer un nom d'utilisateur ou un mot de passe pour vous connecter à CMC. Cela peut être très utile pour créer des scripts automatisés afin d'exécuter des fonctions différentes.

Lorsque vous êtes prêt à configurer cette fonctionnalité, tenez compte des points suivants :

- 1 l'interface utilisateur n'est pas prise en charge pour la gestion de cette fonctionnalité ; vous ne pouvez utiliser que RACADM
- 1 lorsque vous ajoutez des clés publiques, vérifiez que les clés existantes ne figurent pas déjà dans l'index dans lequel la nouvelle clé sera ajoutée. CMC n'effectue aucun contrôle pour vérifier que les clés précédentes sont bien supprimées avant l'ajout d'une nouvelle clé. Dès qu'une nouvelle clé est ajoutée, elle est automatiquement effective tant que l'interface SSH est activée.
- 1 lorsque vous utilisez la section de commentaire de la clé publique, n'oubliez pas que seuls les 16 premiers caractères sont utilisés par CMC. Le commentaire de la clé publique est utilisé par CMC pour différencier les utilisateurs SSH lors de l'utilisation de la commande `getssninfo` RACADM car tous les utilisateurs PKA utilisent le nom d'utilisateur du service pour ouvrir une session.

Par exemple, si deux clés publiques sont configurées, l'une avec le commentaire PC1 et l'autre avec le commentaire PC2 :

```
racadm getssninfo

Type Utilisateur Adresse IP Date/heure de l'ouverture de session
SSH PC1 x.x.x.x 16/06/09 09:00:00
SSH PC2 x.x.x.x 16/06/09 09:00:00
```

Pour des informations supplémentaires sur la commande `sshpkauth`, voir le *Guide de référence de la ligne de commande pour iDRAC6 et CMC*.

Génération de clés publiques pour Windows

Avant d'ajouter un compte, le système qui accèdera à CMC sur SSH nécessite une clé publique. Deux méthodes sont possibles pour générer la paire de clés publique/privée : utiliser l'application PuTTY Key Generator pour les clients exécutant Windows ou la CLI ssh-keygen pour les clients exécutant Linux.

Cette section donne des instructions simples pour générer une paire de clés publique/privée pour les deux applications. Pour une utilisation supplémentaire ou avancée de ces outils, consultez 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. Saisissez le nombre de bits de la clé. Le nombre doit être compris entre 768 et 4 096.

 **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 essaieriez 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 saisir une phrase de passe pour sécuriser la clé. Veillez à bien enregistrer la clé privée.

4. Vous pouvez utiliser la clé publique de deux façons :
 - 1 enregistrer la clé publique dans un fichier à téléverser ultérieurement.
 - 1 copier/coller le texte de la fenêtre **Clé publique à coller...** lorsque vous ajoutez le compte à l'aide de l'option de texte.

Génération de clés publiques pour Linux

L'application ssh-keygen pour les clients Linux est un outil de ligne de commande sans interface utilisateur graphique. Ouvrez une fenêtre de terminal et tapez, 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 phrase de passe est facultative.

Suivez les instructions. Lorsque la commande s'est exécutée, utilisez le fichier public pour passer à RACADM en vue du téléversement du fichier.

Notes de syntaxe RACADM pour CMC

Lorsque vous utilisez la commande `racadm sshpkauth`, vérifiez les points suivants :

- 1 Pour l'option `-i`, le paramètre doit être `svcacct`. Tous les autres paramètres pour `-i` échouent dans CMC. Le `svcacct` est un compte spécial pour l'authentification à clé publique sur SSH dans CMC.
- 1 Pour se connecter à CMC, l'utilisateur doit être `service`. Les utilisateurs des autres catégories ont accès aux clés publiques entrées en utilisant la commande `sshpkauth`.

Affichage des clés publiques

Pour afficher les clés publiques que vous avez ajoutées à CMC, tapez :

```
racadm sshpkauth -i svcacct -k all -v
```

Pour afficher une seule clé à la fois, remplacez `all` par un nombre compris entre 1 et 6. Par exemple, pour afficher la clé 2, tapez :

```
racadm sshpkauth -i svcacct -k 2 -v
```

Ajout des clés publiques

Pour ajouter une clé publique à CMC à l'aide des options de téléversement de fichier (`-f`), tapez :

```
racadm sshpkauth -i svcacct -k 1 -p 0xffff -f <fichier de la clé publique>
```

 **REMARQUE** : vous pouvez uniquement utiliser l'option de téléversement de fichier avec RACADM distant. Pour plus d'informations, consultez [Accès à distance à RACADM](#) et les sections suivantes.

Pour connaître les privilèges de clé publique, consultez le tableau 3-1 du chapitre Propriétés de la base de données du *Guide de référence de l'administrateur de Dell Chassis Management Controller*.

Pour ajouter une clé publique à l'aide de l'option de téléversement de texte, tapez :

```
racadm sshpkauth -i svcacct -k 1 -p 0xffff -t "<texte de clé publique>"
```

Suppression des clés publiques

Pour supprimer une clé publique, tapez :

```
racadm sshpkauth -i svcacct -k 1 -d
```

Pour supprimer toutes les clés publiques, tapez :

```
racadm sshpkauth -i svcacct -k all -d
```

Ouverture de session avec l'authentification par clé publique

Une fois les clés publiques téléversées, vous pourrez ouvrir une session CMC sur SSH sans avoir à saisir un mot de passe. Vous avez également la possibilité d'envoyer une commande RACADM unique en tant qu'argument de ligne de commande à l'application SSH. Les options de ligne de commande se comportent comme RACADM distant car la session se termine une fois la commande exécutée. Par exemple :

Ouverture de session :

```
ssh service@<domaine>
```

Ou

```
ssh service@<adresse_IP>
```

où <adresse_IP> correspond à l'adresse IP de CMC.

Envoi de commandes racadm :

```
ssh service@<domaine> racadm getversion
```

```
ssh service@<domaine> racadm getsel
```

Lorsque vous ouvrez une session avec le compte de service, si une phrase de passe a été configurée lors de la création de la paire de clés publique/privée, vous pouvez être invité à saisir à nouveau cette phrase de passe. Si une phrase de passe est utilisée avec les clés, les clients Windows et Linux fournissent des méthodes pour automatiser aussi cette procédure. Pour les clients Windows, vous pouvez utiliser l'application Pageant. Elle s'exécute en arrière-plan et rend la saisie de la phrase de passe transparente. Pour les clients Linux, vous pouvez utiliser ssh-agent. Pour configurer et utiliser l'une de ces applications, voir la documentation fournie depuis cette application.

Activation d'un utilisateur CMC ayant des droits

Pour accorder des droits d'administration spécifiques (autorisation basée sur le rôle) à un utilisateur, commencez par rechercher un index utilisateur disponible en suivant les étapes indiquées dans [Avant de commencer](#). Ensuite, tapez les lignes de commande suivantes avec le nouveau nom d'utilisateur et le nouveau mot de passe.

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <index> <valeur de masque binaire du privilège d'utilisateur>
```

 **REMARQUE** : consultez le tableau 3-1 du chapitre Propriétés de la base de données du *Guide de référence de l'administrateur de Dell Chassis Management Controller* pour obtenir la liste des valeurs de masque binaire valides correspondant à des privilèges d'utilisateur spécifiques. La valeur de privilège par défaut est 0, indiquant que l'utilisateur n'a aucun privilège activé.

Désactivation d'un utilisateur CMC

À l'aide de l'interface RACADM, vous pouvez uniquement désactiver manuellement les utilisateurs CMC et de manière individuelle. Vous ne pouvez supprimer les utilisateurs à l'aide d'un fichier de configuration.

L'exemple suivant illustre la syntaxe de commande qui peut être utilisée pour supprimer un utilisateur CMC :

```
racadm config -g cfgUserAdmin -i 2 cfgUserAdminPrivilege 0x0
```

Configuration de l'envoi de notifications par e- mail ou d'alertes SNMP

Vous pouvez configurer CMC pour envoyer des interruptions d'événement SNMP et/ou des alertes par e-mail lorsque certains événements se produisent au niveau du châssis. Pour plus d'informations et d'instructions, voir [Configuration des alertes SNMP](#) et [Configuration des alertes par e-mail](#).

Vous pouvez spécifier les destinations d'interruptions sous la forme d'adresses numériques au format approprié (IPv6 ou IPv4) ou de noms de domaine pleinement qualifiés (FQDN). Choisissez un format compatible avec votre technologie de mise en réseau/infrastructure.

 **REMARQUE** : la fonctionnalité **INTERRUPTION test** ne détecte pas les choix incorrects en fonction de la configuration réseau actuelle. Par exemple, l'utilisation d'une destination IPv6 dans un environnement IPv4 uniquement.

Configuration de plusieurs CMC dans plusieurs châssis

À l'aide de RACADM, vous pouvez configurer un ou plusieurs CMC avec des propriétés identiques.

Lorsque vous effectuez une requête sur une carte CMC spécifique à l'aide de son numéro de groupe et du numéro de l'objet, RACADM crée le fichier de configuration `racadm.cfg` à partir des informations collectées. En exportant le 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 de CMC cible contenant la configuration appropriée.

 **REMARQUE** : le fichier de configuration généré est `monfichier.cfg`. Vous pouvez renommer ce fichier.

 **REMARQUE** : le fichier `.cfg` ne contient aucun mot de passe utilisateur. Lorsque le fichier `.cfg` est téléversé sur le nouveau CMC, tous les mots de passe doivent être à nouveau ajoutés.

2. Ouvrez une console texte Telnet/SSH sur CMC, ouvrez une session et tapez :

```
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. Pour plus d'informations, voir [Accès à distance à RACADM](#).

3. Modifiez le fichier de configuration à l'aide d'un éditeur de texte brut (optionnel). Tout caractère de formatage spécial dans le fichier de configuration peut corrompre la base de données RACADM.
4. Utilisez le fichier de configuration nouvellement créé pour modifier un CMC cible.

À l'invite de commande, entrez :

```
racadm config -f myfile.cfg
```

5. Réinitialisez le contrôleur CMC cible qui a été configuré. À l'invite de commande, entrez :

```
racadm reset
```

La sous-commande `getconfig -f myfile.cfg` (étape 1) demande la configuration CMC pour le contrôleur CMC principal et génère le fichier `myfile.cfg`. Si nécessaire, vous pouvez renommer le fichier ou l'enregistrer dans un emplacement différent.

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

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

La sous-commande `config` charge les informations sur les autres CMC. Server Administrator utilise la commande `config` pour synchroniser la base de données des noms d'utilisateur et mots de passe.

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 de texte brut. La commande vous permet de construire un fichier de configuration (similaire à un fichier `.ini`) et de configurer 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 si on le désigne par cette extension dans cette sous-section).

 **REMARQUE** : pour des informations supplémentaires sur la sous-commande `getconfig`, voir le *Guide de référence de la ligne de commande pour iDRAC6 et CMC*.

RACADM analyse le fichier `.cfg` lors de son premier chargement sur CMC afin de vérifier la présence de noms de groupes et d'objets valides et le respect de quelques règles simples de syntaxe. Les erreurs sont indiquées avec le numéro de ligne dans laquelle l'erreur a été détectée et un message explique le problème. Tout le fichier est analysé et toutes les erreurs sont affichées. Les commandes d'écriture ne sont pas transmises à CMC si une erreur est trouvée dans le fichier `.cfg`. Vous devez corriger toutes les erreurs avant que la configuration puisse avoir lieu.

Pour vérifier les erreurs avant de créer le fichier de configuration, utilisez l'option `-c` avec la sous-commande `config`. Avec l'option `-c`, `config` vérifie uniquement

la syntaxe et n'écrit *pas* sur CMC.

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

- 1 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 CMC de ce groupe. Les objets de ce groupe représentent des modifications lorsque CMC est configuré. Si un objet modifié représente un nouvel index, l'index est créé sur CMC pendant la configuration.

- 1 Vous ne pouvez pas choisir les index souhaités dans un fichier `.cfg`:

Les index peuvent être créés et supprimés. Au fil du temps, le groupe peut se fragmenter par suite des index utilisés et inutilisés. Si un index est présent, il est modifié. Si un index n'est pas présent, le premier index disponible est utilisé. Cette méthode permet une certaine flexibilité lors de l'ajout d'entrées indexées où il est inutile d'établir des correspondances d'index exactes entre tous les CMC gérés. Les nouveaux utilisateurs sont ajoutés au premier index disponible. Un fichier `.cfg` qui analyse et s'exécute correctement sur un CMC peut ne pas s'exécuter correctement sur un autre si tous les index sont remplis et qu'un nouvel utilisateur doit être ajouté.

- 1 Utilisez la sous-commande `racresetcfg` pour configurer les deux CMC avec des propriétés identiques.

Utilisez la sous-commande `racresetcfg` pour réinitialiser CMC à ses paramètres initiaux par défaut et exécutez ensuite la commande `racadm config -f <nom de fichier>.cfg`. Le fichier `.cfg` doit inclure tous les objets, utilisateurs, index et autres paramètres appropriés. Voir le chapitre Propriétés de la base de données du *Guide de référence de la ligne de commande pour iDRAC6 et CMC* pour une liste exhaustive des objets et des groupes.

PRÉCAUTION : utilisez la sous-commande `racresetcfg` pour réinitialiser la base de données et les paramètres de carte réseau CMC sur leurs paramètres par défaut d'origine, et supprimer tous les utilisateurs et toutes les configurations utilisateur. Pendant que l'utilisateur root est disponible, les paramètres par défaut des autres utilisateurs sont également réinitialisés.

Règles d'analyse

- 1 Les lignes qui commencent par le caractère de hachage « # » sont traitées comme des commentaires.

Une ligne de commentaire doit commencer dans la première colonne. Un caractère « # » dans toute autre colonne est traité comme un caractère #.

Certains paramètres de modem peuvent inclure les caractères # dans leurs chaînes de caractères. Un caractère d'échappement n'est pas requis. Vous pouvez générer un fichier `.cfg` à partir d'une commande `racadm getconfig -f <nom de fichier>.cfg`, puis exécuter une commande `racadm config -f <nom de fichier>.cfg` sur un autre CMC sans ajouter de caractères d'échappement.

Par exemple :

```
#
# Il s'agit d'un commentaire
[cfgUserAdmin]
cfgUserAdminPageModemInitString=<Init modem # n'est pas un commentaire>
```

- 1 Toutes les entrées de groupe doivent être entourées de crochets d'ouverture et de fermeture ([et]).

Le caractère « [» du début indiquant un nom de groupe *doit* commencer dans la colonne 1. Ce nom de groupe *doit* être spécifié avant n'importe quel objet dans ce groupe. Les objets auxquels aucun nom de groupe n'est associé génèrent une erreur. Les données de configuration s'organisent en groupes tel que défini dans le chapitre Propriétés de la base de données du *Guide de référence de la ligne de commande pour iDRAC6 et CMC*.

L'exemple suivant affiche un nom de groupe, un objet et la valeur de propriété de l'objet :

```
[cfgLanNetworking] - {nom de groupe}
cfgNicIpAddress=143.154.133.121 {nom de l'objet} {valeur de l'objet}
```

- 1 Tous les paramètres sont spécifiés en tant que paires « objet=valeur » sans espace entre l'objet, le signe = et la valeur.

Les espaces blancs qui sont inclus après la valeur sont ignorés. Un espace blanc à l'intérieur d'une chaîne de valeurs n'est pas modifié. Tout caractère à droite du symbole « = » est pris tel quel (par exemple, un deuxième « = », un « # », « [», «] », et ainsi de suite). Ces caractères sont des caractères de script de conversation de modem valides.

```
[cfgLanNetworking] - {nom de groupe}
cfgNicIpAddress=143.154.133.121 {nom d'objet}
```

- 1 L'analyseur `.cfg` ignore une entrée d'objet d'index.

Vous ne pouvez pas spécifier quel index est utilisé. Si l'index existe déjà, il est utilisé ou la 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, ce qui vous permet de visualiser les commentaires inclus.

REMARQUE : vous pouvez créer un groupe indexé manuellement en utilisant la commande suivante :

```
racadm config -g <Nomgroupe> -o <objet ancré> -i <index 1 à 16> <nom d'ancre unique>
```

- 1 La ligne d'un groupe indexé ne peut pas être supprimée d'un fichier `.cfg`. Si vous supprimez cette ligne à l'aide d'un éditeur de texte, RACADM interrompra son analyse du fichier de configuration et vous avertira de l'erreur.

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

```
racadm config -g <nom du groupe> -o <nom de l'objet> -i <index 1 à 16> ""
```

 **REMARQUE** : une chaîne de caractères nulle (identifiée par deux caractères ") demande à CMC de supprimer l'index du groupe spécifié.

Pour voir le contenu d'un groupe indexé, utilisez la commande suivante :

```
racadm getconfig -g <nom du groupe> -i <index 1 à 16>
```

- 1 Pour les groupes indexés, l'ancre d'objet doit être le premier objet après les crochets « [] ».

Voici des exemples de groupes indexés actuels :

```
[cfgUserAdmin]
cfgUserAdminUserName=<NOM_D'UTILISATEUR>
```

Si vous tapez `racadm getconfig -f <mon exemple>.cfg`, la commande construit un fichier `.cfg` pour la configuration CMC actuelle. Ce fichier de configuration peut être utilisé comme exemple et comme point de départ de votre fichier `.cfg` unique.

Modification de l'adresse IP CMC

Lorsque vous modifiez l'adresse IP CMC dans le fichier de configuration, supprimez toutes les entrées `<variable>=<valeur>` inutiles. Seul le nom du groupe variable actuel avec « [» et «] » est conservé, avec les deux entrées `<variable>=<valeur>` correspondant au changement d'adresse IP.

Exemple :

```
#
# Groupe d'objets « cfgLanNetworking »
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.10.110
cfgNicGateway=10.35.10.1
```

Ce fichier est mis à jour comme suit :

```
#
# Groupe d'objets « 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 <monfichier>.cfg` analyse le fichier et identifie toutes les erreurs par numéro de ligne. Un fichier correcte met à jour les bonnes entrées. En outre, vous pouvez utiliser la même commande `getconfig` utilisée dans l'exemple précédent pour confirmer la mise à jour.

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

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

Utilisation de RACADM pour configurer les propriétés sur iDRAC

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

- 1 `cfgLanNetworking`
- 1 `cfgIPV6LanNetworking`
- 1 `cfgRacTuning`
- 1 `cfgRemoteHosts`
- 1 `cfgSerial`
- 1 `cfgSessionManagement`

 **REMARQUE** : pour plus d'informations sur les valeurs et les plages de propriétés par défaut, consultez le *Guide d'utilisation d'Integrated Dell Remote Access Controller 6 (iDRAC6) Enterprise pour les serveurs lames*.

Si le micrologiciel sur le serveur ne prend pas une fonctionnalité en charge, la configuration d'une propriété liée à cette fonctionnalité entraîne l'affichage d'une erreur. Par exemple, l'utilisation de RACADM pour activer `syslog` distant sur un iDRAC non pris en charge entraîne l'affichage d'un message d'erreur.

De même, lors de l'affichage des propriétés iDRAC à l'aide de la commande `getconfig` de RACADM, les valeurs de propriétés sont affichées sous la forme - pour une fonctionnalité non prise en charge sur le serveur.

Par exemple :

```
$ racadm getconfig -g cfgSessionManagement -m server-1

# cfgSsnMgtWebServerMaxSessions=-

# cfgSsnMgtWebServerActiveSessions=-

# cfgSsnMgtWebServerTimeout=-

# cfgSsnMgtSSHMaxSessions=-

# cfgSsnMgtSSHActiveSessions=-

# cfgSsnMgtSSTimeout=-

# cfgSsnMgtTelnetMaxSessions=-

# cfgSsnMgtTelnetActiveSessions=-

# cfgSsnMgtTelnetTimeout=-
```

Dépannage

Le [Tableau 4-3](#) répertorie les problèmes courants liés à RACADM distant.

Tableau 4-3. Utilisation des commandes Serial/ RACADM : Foire aux questions

Question	Réponse
Après avoir réinitialisé CMC (avec la sous-commande <code>racreset</code> de RACADM), j'entre une commande et le message suivant s'affiche : <code>racadm <sous-commande> Transport: ERROR: (RC=-1)</code> Qu'est-ce que ce message signifie ?	Vous devez attendre que CMC soit complètement réinitialisé avant d'envoyer une autre commande.
Lorsque j'utilise les sous-commandes RACADM, je reçois des erreurs que je ne comprends pas.	Il se peut que vous rencontriez une ou plusieurs des erreurs suivantes lors de l'utilisation de RACADM : 1 Messages d'erreur locaux : problèmes de syntaxe, d'erreurs typographiques et de noms incorrects . Exemple : <code>ERROR: <message></code> Utilisez la sous-commande <code>help</code> RACADM pour afficher la syntaxe correcte et les informations d'utilisation. 1 Messages d'erreur liés à CMC : problèmes qui empêchent CMC d'effectuer une opération. Le message peut également indiquer « Échec d'une commande RACADM ». Tapez <code>racadm gettracelog</code> pour obtenir des informations de débogage.
Pendant l'utilisation de RACADM distant, l'invite s'est modifiée pour afficher « > » et je ne parviens pas à récupérer l'invite « \$ ».	Si vous tapez des guillemets doubles différents (") ou une citation simple différente (') dans la commande, l'interface utilisateur change vers l'invite « > » et met en file d'attente toutes les commandes. Pour revenir à l'invite « \$ », tapez <code><Ctrl>-d</code> .
Les commandes suivantes ont affiché le message d'erreur « Not Found » : <code>\$ logout</code> <code>\$ quit</code>	Les commandes « <code>logout</code> » et « <code>quit</code> » ne sont pas prises en charge dans l'interface de ligne de commande CMC.

[Retour à la page Contenu](#)

[Retour à la page Contenu](#)

Dépannage et récupération

Micrologiciel Dell Chassis Management Controller Version 3.1 Guide d'utilisation

- [Présentation](#)
- [Outils de surveillance du châssis](#)
- [Premières étapes de dépannage d'un système distant](#)
- [Surveillance de l'alimentation et exécution de commandes de contrôle de l'alimentation sur le châssis](#)
- [Dépannage de l'alimentation](#)
- [Affichage des résumés du châssis](#)
- [Affichage de la condition d'intégrité du châssis et des composants](#)
- [Affichage des journaux d'événements](#)
- [Utilisation de la console de diagnostic](#)
- [Réinitialisation des composants](#)
- [Résolution des erreurs de protocole de temps du réseau \(NTP\)](#)
- [Interprétation des couleurs des LED et séquences de clignotement](#)
- [Dépannage d'un contrôleur CMC qui ne répond pas](#)
- [Dépannage des problèmes de réseau](#)
- [Réinitialisation de mot de passe administrateur oublié](#)
- [Dépannage des alertes](#)

Présentation

Cette section détaille les tâches de récupération et de résolution des problèmes se produisant sur le système distant avec l'interface Web CMC.

- 1 Collecte des informations de configuration, d'état d'erreur et des journaux d'erreurs
- 1 Gestion de l'alimentation d'un système distant
- 1 Affichage des informations sur le châssis
- 1 Affichage des journaux d'événements
- 1 Utilisation de la console de diagnostic
- 1 Réinitialisation des composants
- 1 Dépannage des problèmes de protocole de temps du réseau (NTP)
- 1 Dépannage des problèmes de réseau
- 1 Dépannage des problèmes d'alerte
- 1 Réinitialisation de mot de passe administrateur oublié
- 1 Journaux et codes d'erreur

Outils de surveillance du châssis

Collecte des informations de configuration et d'état et journaux du châssis

La sous-commande **racdump** fournit une seule commande permettant d'obtenir la condition complète du châssis, des informations sur l'état de configuration et des journaux.

Utilisation

```
racadm racdump
```

La sous-commande **racdump** affiche les informations suivantes :

- 1 Informations générales sur le système/RAC
- 1 Informations sur CMC
- 1 Informations sur le châssis
- 1 Informations sur les sessions
- 1 Informations du capteur
- 1 Informations sur le numéro du micrologiciel

Interfaces prises en charge

- 1 CLI RACADM
- 1 RACADM distante

1 Telnet RACADM

La commande RACADM peut être exécutée à distance à partir de l'invite de commande d'une console série, Telnet ou SSH , ou d'une invite de commande normale.

Pour obtenir la liste des options de syntaxe et de ligne de commande des différentes sous-commandes RACDUMP, tapez :

```
aide racadm <racdump>
```

CLI RACDUMP

Racdump inclut les sous-systèmes suivants et regroupe les commandes RACADM suivantes :

Sous-système	Commande RACADM
Informations générales sur le système/sur le 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 de 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

Utilisation

```
racadm racdump
```

RACDUMP distante

RACADM distante est un utilitaire côté client qui peut être exécuté à partir d'une station de gestion via l'interface réseau hors bande. Une option de capacité d'accès à distance (-r) qui vous permet de vous connecter au système géré et d'exécuter les sous-commandes RACADM à partir d'une console distante ou d'une station de gestion est fournie. Pour utiliser la capacité d'accès à distance, il vous faut un nom d'utilisateur (option -u) et un mot de passe (option -p) valides, ainsi que l'adresse IP de CMC.

 **REMARQUE** : lorsque vous utilisez la capacité d'accès à distance de RACADM, vous devez posséder des droits d'écriture sur les dossiers sur lesquels vous utilisez les sous-commandes RACADM impliquant des opérations sur des fichiers, par exemple :

- o racadm getconfig -f <nom de fichier>
- o racadm sslcertdownload -t <type> [-f <nom de fichier>]

Utilisation RACDUMP distante

Pour utiliser la sous-commande RACDUMP à distance, tapez les commandes suivantes :

```
racadm -r <adresse IP CMC> -u <nom d'utilisateur> -p <mot de passe>
```

```
<sous-commande> <options de la sous-commande>
```

```
racadm -i -r <adresse IP CMC> <sous-commande> <options de
```

```
la sous-commande>
```

 **REMARQUE** : l'option -i ordonne à RACADM de demander le nom d'utilisateur et le mot de passe de manière interactive. Sans l'option -i, vous devez indiquer le nom d'utilisateur et le mot de passe dans la commande à l'aide des options -u et -p.

Par exemple :

```
racadm -r 192.168.0.120 -u root -p calvin racdump
```

```
racadm -i -r 192.168.0.120 racdump
```

Si le numéro de port HTTPS du CMC a été remplacé par un port personnalisé autre que le port par défaut (443), la syntaxe suivante doit être utilisée :

```
racadm -r <adresse IP CMC>:<port> -u <nom d'utilisateur> -p <mot de passe> <sous-commande> <options de la sous-commande>

racadm -i -r <adresse IP CMC>:<port> <sous-commande> <options de la sous-commande>
```

Telnet RACDUMP

RACADM SSH/Telnet est utilisée pour faire référence à l'utilisation de la commande RACADM à partir de l'invite SSH ou Telnet.

Pour plus d'informations sur RACDUMP, consultez la section [Utilisation de l'interface de ligne de commande RACADM](#) et le « *Guide de référence de l'administrateur de 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.

Utilisation de l'interface Web

Pour activer le clignotement d'une, de plusieurs ou de toutes les LED de composants :

1. Ouvrez une session sur l'interface Web de CMC.
2. Sélectionnez **Châssis** dans l'arborescence.
3. Cliquez sur l'onglet **Dépannage**.
4. Cliquez sur le sous-onglet **Identifier**. La page **Identifier** s'affiche et présente la liste de tous les composants du châssis.
5. Pour activer le clignotement d'une LED, cochez la case en regard du nom de périphérique, puis cliquez sur **Clignotement**.
6. Pour désactiver le clignotement d'une LED, cochez la case en regard du nom de périphérique, puis cliquez sur **Arrêter le clignotement**.

Utilisation de la RACADM

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

```
racadm setled -m <module> [-l <état du voyant>]
```

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

```
l server-n où n = 1-16
l switch-n où n = 1-6
l cmc-active
```

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

```
l 0 : aucun clignotement (par défaut)
l 1 : clignotement
```

Configuration des alertes SNMP

Les interruptions SNMP (protocole de gestion de réseau simple) ou les *interruptions d'événements* sont similaires aux alertes d'événement par e-mail. Elles sont utilisées par une station de gestion pour recevoir des données de CMC sans avoir à les demander.

Vous pouvez configurer CMC pour générer des interruptions d'événement. [Tableau 12-2](#) fournit un aperçu des événements déclencheurs des alertes SNMP et par e-mail. Pour plus d'informations sur les alertes par e-mail, voir [Configuration des alertes par e-mail](#).

 **REMARQUE** : dès la version 2.10 de CMC, SNMP bénéficie désormais de la capacité IPv6. Vous pouvez inclure une adresse IPv6 ou un nom de domaine pleinement qualifié (FQDN) dans la destination pour une alerte d'événement.

Tableau 12-2. Événements sur châssis susceptibles de générer des alertes SNMP et par e-mail

Événement	Description
Panne de sonde de ventilateur	Un ventilateur est trop lent ou ne fonctionne pas du tout.
Avertissement de capteur de batterie	Une batterie a cessé de fonctionner.
Avertissement de capteur de température	La température approche de ses limites excessivement hautes ou basses.
Panne de capteur de température	La température est trop haute ou trop basse pour un fonctionnement correct.
Redondance dégradée	La redondance des ventilateurs et/ou des blocs d'alimentation a été réduite.
Perte de la redondance	Les ventilateurs et/ou les blocs d'alimentation ne sont plus redondants.
Avertissement de bloc d'alimentation	Le bloc d'alimentation approche d'une condition de panne.
Panne de bloc d'alimentation	Le bloc d'alimentation est défaillant.
Bloc d'alimentation absent	Un bloc d'alimentation qui devrait être en place est manquant.
Erreur dans le journal du matériel	Le journal du matériel ne fonctionne pas.
Avertissement du journal du matériel	Le journal du matériel est presque plein.
Serveur absent	Un serveur qui devrait être présent est manquant.
Panne de serveur	Le serveur ne fonctionne pas.
KVM absent	Un module KVM qui devrait être présent est manquant.
Échec de KVM	Le module KVM ne fonctionne pas.
Module d'E/S absent	Un module d'E/S qui devrait être présent est manquant.
Panne de module d'E/S	Le module d'E/S ne fonctionne pas.
Non correspondance de version de micrologiciel	Il existe une incompatibilité du micrologiciel avec le châssis ou du serveur.
Erreur de limite de puissance du châssis	La consommation électrique au sein du châssis a atteint la limite de puissance d'entrée système.
CARTE SD absente	Aucun support ne se trouve dans le logement de carte SD (Secure Digital) de CMC et une fonctionnalité CMC configurée en a besoin.
Erreur de CARTE SD	Une erreur s'est produit lors de l'accès au support se trouvant dans le logement de carte SD (Secure Digital) de CMC.

Vous pouvez ajouter et configurer des alertes SNMP à l'aide de l'interface Web ou RACADM.

Utilisation de l'interface Web

 **REMARQUE** : vous devez disposer du privilège **Administrateur de configuration du châssis** pour ajouter ou configurer des alertes SNMP.

 **REMARQUE** : pour plus de sécurité, il est vivement recommandé de modifier le mot de passe par défaut du compte root (User 1). Le compte root est le compte d'administration par défaut fourni avec le contrôleur CMC. Pour modifier le mot de passe par défaut du compte root, cliquez sur la référence utilisateur 1 pour ouvrir la page **Configuration utilisateur**. L'aide relative à cette page est disponible via le lien **Aide** en haut à droite de la page.

- Ouvrez une session sur l'interface Web de CMC.
- Sélectionnez **Châssis** dans l'arborescence du système.
- Cliquez sur l'onglet **Alertes**. La page **Événements sur châssis** s'affiche.
- Activation des alertes :
 - Cochez les cases des événements pour lesquels vous souhaitez activer les alertes. Pour activer tous les événements pour les alertes, cochez la case **Sélectionner tout**.
 - Cliquez sur **Appliquer** pour enregistrer vos paramètres.
- Cliquez sur le sous-onglet **Paramètres d'interruptions**. La page **Destinations des alertes des événements sur châssis** s'affiche.
- Saisissez une adresse valide dans un champ **Destination** vide.

 **REMARQUE** : une adresse valide est une adresse qui reçoit les alertes d'interruptions. Utilisez le format IPv4 « à quatre points », la notation d'adresses IPv6 standard ou FQDN. Par exemple : 123.123.123.123 ou 2001:db8:85a3::8a2e:370:7334 ou dell.com

- Entrez la **chaîne de communauté SNMP** à laquelle appartient la station de gestion de destination.

 **REMARQUE** : les chaînes de communauté des pages **Destinations des alertes des événements sur châssis** et **Châssis → Réseau → Services** diffèrent. La chaîne de communauté des interruptions SNMP est celle utilisée par CMC pour les interruptions sortantes à destination des stations de gestion. La chaîne de communauté de la page **Châssis → Réseau → Services** correspond à la chaîne de communauté utilisée par les stations de gestion pour interroger le démon SNMP sur CMC.

- Cliquez sur **Appliquer** pour enregistrer les modifications.

Pour tester une interruption d'événement pour une destination d'alerte :

1. Ouvrez une session sur l'interface Web de CMC.
2. Sélectionnez **Châssis** dans l'arborescence du système.
3. Cliquez sur l'onglet **Alertes**. La page **Événements du châssis** s'affiche.
4. Cliquez sur l'onglet **Paramètres d'interruptions**. La page **Destinations des alertes des événements du châssis** s'affiche.
5. Cliquez sur **Envoyer** dans la colonne **Interruption de test** à côté de la destination.

 **REMARQUE** : spécifiez les destinations d'interruptions sous la forme d'adresses numériques au format approprié (IPv6 ou IPv4) ou de noms de domaine pleinement qualifiés (FQDN). Choisissez un format compatible avec votre technologie de mise en réseau/infrastructure. La fonctionnalité **Interruption de test** ne peut pas détecter les choix incorrects d'après la configuration réseau actuelle (par exemple, l'utilisation d'une destination IPv6 dans un environnement IPv4 uniquement).

Utilisation de la RACADM

1. Ouvrez une console texte série/Telnet/SSH d'accès à CMC, puis ouvrez une session.

 **REMARQUE** : seul un masque de filtre peut être défini pour les alertes SNMP et par e-mail. Vous pouvez passer l'étape 2 si vous avez déjà sélectionné le masque de filtre.

2. Activez des alertes en entrant :

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

3. Spécifiez les événements pour lesquels vous souhaitez que CMC génère des alertes en entrant :

```
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 secondes valeurs des différents masques (1, 2, 4, etc.) à l'aide de la touche <OR>.

Par exemple, pour activer les alertes d'interruptions pour l'avertissement de capteur de batterie (0x2), la panne de bloc d'alimentation (0x1000) et la panne de KVM (0x80000), tapez 2 <OR> 1000 <OR> 200000 et appuyez sur la touche <=>.

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

Tableau 12-3. Masques de filtre d'interruptions d'événements

Événement	Valeur du masque de filtre
Panne de sonde de ventilateur	0x1
Avertissement de capteur de batterie	0x2
Avertissement de capteur de température	0x8
Panne de capteur de température	0x10
Redondance dégradée	0x40
Perte de la redondance	0x80
Avertissement de bloc d'alimentation	0x800
Panne de bloc d'alimentation	0x1000
Bloc d'alimentation absent	0x2000
Erreur dans le journal du matériel	0x4000
Avertissement du journal du matériel	0x8000
Serveur absent	0x10000
Panne de serveur	0x20000
KVM absent	0x40000
Échec de KVM	0x80000
Module d'E/S absent	0x100000
Panne de module d'E/S	0x200000
Non correspondance de version de micrologiciel	0x00400000

Erreur de limite de puissance du châssis	0x01000000
CARTE SD absente	0x02000000
Erreur de CARTE SD	0x04000000
Erreur du groupe de châssis	0x80000000

4. Activez des alertes d'interruption en entrant :

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

où *<index>* est une valeur comprise entre 1 et 4. Le numéro d'index est utilisé par CMC pour distinguer jusqu'à quatre destinations configurables pour les alertes d'interruptions. Les destinations peuvent être spécifiées sous la forme d'adresses numériques au format approprié (IPv6 ou IPv4) ou de noms de domaine pleinement qualifiés (FQDN).

5. Spécifiez une adresse IP de destination pour la réception d'alertes d'interruption en entrant :

```
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 en entrant :

```
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 recevoir des alertes d'interruptions. Pour ajouter d'autres destinations, répétez les étapes 2 à 6.

 **REMARQUE** : les commandes des étapes 2 à 6 écrasent tout paramètre existant configuré pour l'index spécifié (1 à 4). Pour déterminer si des valeurs ont précédemment été configurées pour un index, entrez : `racadm get config -g cfgTraps -i <index>`. Si l'index a été configuré, des valeurs apparaîtront pour les objets `cfgTrapsAlertDestIPAddr` et `cfgTrapsCommunityName`.

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 de l'alerte à tester. Si vous n'êtes pas certain du numéro d'index, tapez :

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

Configuration des alertes 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.

Le [Tableau 12-2](#) fournit un aperçu des événements déclencheurs des alertes SNMP et par e-mail. Pour plus d'informations sur les alertes SNMP, voir [Configuration des alertes SNMP](#).

Vous pouvez ajouter et configurer des alertes par e-mail à l'aide de l'interface Web ou RACADM.

Utilisation de l'interface Web

 **REMARQUE** : vous devez disposer du privilège **Administrateur de configuration du châssis** pour ajouter ou configurer des alertes par e-mail.

- Ouvrez une session sur l'interface Web de CMC.
- Sélectionnez **Châssis** dans l'arborescence du système.
- Cliquez sur l'onglet **Alertes**. La page **Événements sur châssis** s'affiche.
- Activation des alertes :
 - Cochez les cases des événements pour lesquels vous souhaitez activer les alertes. Pour activer tous les événements pour les alertes, cochez la case **Sélectionner tout**.
 - Cliquez sur **Appliquer** pour enregistrer vos paramètres.
- Cliquez sur le sous-onglet **Paramètres des alertes par e-mail**. La page **Destination des alertes par e-mail** s'affiche.
- Spécifiez l'adresse IP du serveur SMTP :
 - Localisez le champ **Serveur SMTP (e-mail)**, puis entrez le nom d'hôte SMTP ou l'adresse IP.

 **REMARQUE** : vous devez configurer le serveur de messagerie SMTP pour accepter les e-mails transmis à partir de l'adresse IP de CMC, une fonctionnalité qui est normalement désactivée sur la plupart des serveurs de messagerie en raison des préoccupations de sécurité. Pour savoir comment procéder en toute sécurité, reportez-vous à la documentation qui accompagne votre serveur SMTP.

- b. Saisissez l'expéditeur de l'e-mail souhaité pour l'alerte ou laissez le champ vide pour utiliser l'expéditeur de l'e-mail par défaut. L'expéditeur par défaut est : `cmc@<adresse_IP>` où `<adresse_IP>` correspond à l'adresse IP de CMC. Si vous entrez une valeur, la syntaxe du nom de l'e-mail est : `<nom_e-mail>[<domaine>]`. Le nom du domaine est facultatif.

Lorsque `@<domaine>` n'est pas spécifié et qu'il existe un domaine de réseau CMC actif, l'adresse e-mail `<nom_e-mail>@<domaine_cmc>` est utilisée comme e-mail source. Si `@<domaine>` n'est pas spécifié et que CMC ne possède pas de domaine de réseau actif, l'adresse IP de CMC est utilisée (par exemple, `<nom_e-mail>@<adresse_IP>`).

- c. Cliquez sur **Appliquer** pour enregistrer vos modifications.

7. Spécifiez les adresses e-mail des destinataires des alertes :

- a. Saisissez une adresse e-mail valide dans un champ **Adresse e-mail de destination** vide.
- b. Entrez un **Nom** facultatif. Ce nom correspond au destinataire de l'e-mail. Le nom est ignoré si l'adresse e-mail correspondante n'est pas valide.
- c. Cliquez sur **Appliquer** pour enregistrer vos paramètres.

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

1. Ouvrez une session sur l'interface Web de CMC.
2. Sélectionnez **Châssis** dans l'arborescence du système.
3. Cliquez sur l'onglet **Alertes**. La page **Événements sur châssis** s'affiche.
4. Cliquez sur le sous-onglet **Paramètres des alertes par e-mail**. La page **Destination des alertes par e-mail** s'affiche.
5. Cliquez sur **Envoyer** dans la colonne **Adresse e-mail de destination** en regard de la destination.

Utilisation de la RACADM

1. Ouvrez une console texte série/Telnet/SSH d'accès à CMC, puis ouvrez une session.
2. Activez des alertes en entrant :

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

 **REMARQUE** : seul un masque de filtre peut être défini pour les alertes SNMP et par e-mail. Vous pouvez passer l'étape 3 si vous avez déjà défini un masque de filtre.

3. Spécifiez les événements pour lesquels vous souhaitez que CMC génère des alertes en entrant :

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

où `<valeur du masque>` correspond à une valeur hexadécimale comprise entre 0x0 et 0xffffffff devant commencer par les caractères 0x. Le [Tableau 12-3](#) fournit des masques de filtre pour chaque type d'événement. Pour des instructions sur le calcul de la valeur hexadécimale du masque de filtre à activer, voir l'étape 3 de la section [Utilisation de la RACADM](#).

4. Activez les alertes par e-mail en tapant :

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEnable 1 -i <index>
```

où `<index>` est une valeur comprise entre 1 et 4. Le numéro d'index est utilisé par CMC pour distinguer jusqu'à quatre adresses e-mail de destination configurables.

5. Spécifiez une adresse e-mail de destination des alertes par e-mail en tapant :

```
racadm config -g cfgEmailAlert -o cfgEmailAlertAddress <adresse e-mail> -i <index>
```

où `<adresse e-mail>` correspond à une adresse e-mail valide et `<index>` à la valeur de l'index spécifiée à l'[étape 4](#).

6. Spécifiez le nom du destinataire de l'alerte par e-mail en tapant :

```
racadm config -g cfgEmailAlert -o cfgEmailAlertEmailName <nom destinataire de l'e-mail> -i <index>
```

où `<nom de l'e-mail>` correspond au nom de la personne ou du groupe destinataire de l'alerte par e-mail et `<index>` à la valeur de l'index spécifiée à l'[étape 4](#) et à l'[étape 5](#). Le nom du destinataire de l'e-mail peut contenir jusqu'à 32 caractères alphanumériques, des tirets, des traits de soulignement et des points. Les espaces ne sont pas valides.

7. Définissez l'hôte SMTP en configurant la propriété de la base de données `cfgRhostsSmtServerIpAddr` en tapant :

```
racadm config -g cfgRemoteHosts -o cfgRhostsSmtServerIpAddr domaine.hôte
```

où `domaine.hôte` est un nom de domaine complet.

Vous pouvez configurer jusqu'à quatre adresses e-mail de destination des alertes par e-mail. Pour ajouter d'autres adresses e-mail, répétez les étapes de l'[étape 2](#) à l'[étape 6](#).

 **REMARQUE** : les commandes des étapes 2 à 6 écrasent tout paramètre existant configuré pour l'index spécifié (1 à 4). Pour déterminer si des valeurs ont été précédemment configurées pour un index, entrez : `racadm get config -g cfgEmailAlert -i <index>`. Si l'index a été configuré, des valeurs apparaîtront pour les objets `cfgEmailAlertAddress` et `cfgEmailAlertEmailName`.

Premières étapes de dépannage d'un système distant

Les questions suivantes aident souvent à dépanner les problèmes de haut niveau dans le système géré :

1. Le système est-il sous tension ou hors tension ?
2. S'il est sous tension, est-ce que le système d'exploitation fonctionne, est-il tombé en panne ou est-il seulement bloqué ?
3. S'il est hors tension, est-ce que l'alimentation a été coupée soudainement ?

Surveillance de l'alimentation et exécution de commandes de contrôle de l'alimentation sur le châssis

Vous pouvez utiliser l'interface Web ou RACADM pour :

1. Afficher l'état actuel de l'alimentation du système.
1. Effectuer un arrêt normal via le système d'exploitation lors du redémarrage et mettre sous tension puis hors tension le système.

Pour des informations concernant la gestion de l'alimentation sur CMC et la configuration du bilan de puissance, de la redondance et du contrôle de l'alimentation, voir [Gestion de l'alimentation](#).

Affichage de la condition du bilan de puissance

Pour des instructions sur l'affichage de la condition du bilan de puissance du châssis, des serveurs et des unités d'alimentation via l'interface Web ou RACADM, voir [Affichage de l'état de la consommation de puissance](#).

Exécution d'une opération de contrôle de l'alimentation

Pour des instructions sur la mise sous/hors tension, la réinitialisation, ou le cycle d'alimentation du système via l'interface Web CMC ou RACADM, voir [Exécution de tâches de contrôle de l'alimentation sur le châssis](#), [Exécution d'opérations de contrôle de l'alimentation sur un module d'E/S](#) et [Exécution de tâches de contrôle de l'alimentation sur un serveur](#).

Dépannage de l'alimentation

Utilisez les éléments ci-dessous pour vous aider à résoudre les problèmes inhérents au bloc d'alimentation et à l'alimentation :

- 1 **Problème** : politique de redondance d'alimentation configurée sur **Redondance de l'alimentation alternative**, et un événement de perte de redondance de bloc d'alimentation redondante est survenu.
 - o **Résolution A** : cette configuration nécessite qu'au moins un bloc d'alimentation du côté 1 (trois logements de gauche) et un bloc d'alimentation dans le côté 2 (trois logements de droite) soient présents et fonctionnels dans l'enceinte modulaire. En outre, la capacité de chaque côté doit être suffisante pour soutenir les allocations de puissances totales pour que le châssis maintienne la **redondance de l'alimentation alternative**. (Pour une opération de redondance de l'alimentation alternative complète, s'assurer qu'une configuration de bloc d'alimentation complète de six blocs d'alimentation est disponible.)
 - o **Résolution B** : vérifiez si tous les blocs d'alimentation sont correctement connectés aux deux réseaux AC ; les blocs d'alimentation du côté 1 doivent être connectés à un réseau de courant alternatif, ceux du côté 2 doivent être raccordés au réseau à courant alternatif, et les deux réseaux CA doivent fonctionner. La **redondance de l'alimentation alternative** est perdue lorsque l'un des réseaux d'alimentation alternative ne fonctionne pas.
- 1 **Problème** : l'état de l'unité d'alimentation s'affiche comme **Échoué (Pas d'alimentation alternative)**, même lorsqu'un cordon d'alimentation alternative est connecté et que l'unité de distribution d'alimentation produit une sortie d'alimentation alternative satisfaisante.
 - o **Résolution A** : vérifiez et remplacez le cordon d'alimentation alternative. Vérifiez et confirmez que l'unité de distribution électrique acheminant l'électricité vers le bloc d'alimentation fonctionne comme prévu. Si la panne persiste, appelez le service client de Dell en vue du remplacement du bloc d'alimentation.
 - o **Résolution B** : vérifiez que l'unité d'alimentation est connectée à la même tension que les autres. Si CMC détecte une unité d'alimentation sur une tension différente, celle-ci est désactivée et marquée comme défaillante.

- 1 **Problème** : l'enclenchement dynamique des blocs d'alimentation est activé, mais aucun des blocs d'alimentation ne s'affiche à l'état **Veille**.
 - o **Résolution A** : l'excédent d'électricité est insuffisant. Un ou plusieurs blocs d'alimentation sont placés en mode de veille seulement lorsque le surplus d'énergie disponible dans l'enceinte dépasse la capacité d'au moins un bloc d'alimentation.
 - o **Résolution B** : l'enclenchement dynamique des blocs d'alimentation ne peut être entièrement pris en charge avec les blocs d'alimentation présents dans l'enceinte. Pour vérifier si c'est le cas, utilisez l'interface Web pour couper l'enclenchement dynamique des blocs d'alimentation, puis rallumez-le. Un message s'affiche si l'enclenchement dynamique des blocs d'alimentation ne peut pas être pris en charge complètement.

- 1 **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.
 - o **Résolution A** : vérifiez le paramètre de limite de puissance d'entrée système ; il se peut qu'elle soit configurée sur un niveau trop faible pour permettre la mise sous tension de serveurs supplémentaires.
 - o **Résolution B** : vérifiez le fonctionnement 110 V. Si des blocs d'alimentation sont connectés à des circuits de dérivation 110V, vous devez reconnaître cette configuration comme valide avant que les serveurs soient autorisés à se mettre sous tension. Pour plus de détails, consultez les paramètres de configuration de la puissance.
 - o **Résolution C** : vérifiez le paramètre de conservation de la puissance max. S'il est défini, les serveurs sont autorisés à se mettre sous tension. Pour plus de détails, consultez les paramètres de configuration de la puissance.
 - o **Résolution B** : vérifiez la priorité de la puissance d'emplacement du serveur de l'emplacement associé au serveur récemment inséré et veillez à ce qu'elle ne soit pas inférieure à toute autre priorité de puissance d'emplacement du serveur.

- 1 **Problème** : la puissance disponible ne cesse d'évoluer, même lorsque la configuration de l'enceinte modulaire n'a pas changé
 - o **Résolution** : CMC 1.2 et les versions ultérieures intègrent la gestion dynamique de l'alimentation de ventilateur qui réduit les allocations de serveur brièvement si l'enceinte fonctionne à un niveau proche du seuil énergétique maximal configuré par l'utilisateur ; cela permet d'allouer de la puissance aux ventilateurs en réduisant les performances du serveur afin de maintenir le débit de puissance en dessous de la **limite de la puissance d'entrée système**. Ce comportement est normal.

- 1 **Problème** : 2000 W est signalé comme étant l'**excédent des performances maximales**.
 - o **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.

- 1 **Problème** : un sous-ensemble de serveurs n'est plus alimenté suite à une panne du réseau d'alimentation en CA, même si le châssis fonctionnait en mode de configuration **Redondance d'alimentation alternative** avec six blocs d'alimentation.
 - o **Résolution** : cette situation peut se produire si les blocs d'alimentation ne sont pas correctement connectés aux réseaux électriques C.A. redondants lorsque la panne de réseau électrique C.A. survient. La stratégie **Redondance d'alimentation alternative** exige que les trois blocs d'alimentation de gauche soient connectés à un réseau électrique C.A. et que les trois blocs d'alimentation de droite soient connectés à l'autre réseau électrique C.A. Si deux unités d'alimentation ne sont pas correctement connectées, par exemple si l'unité d'alimentation3 et l'unité d'alimentation4 sont connectées aux mauvais réseaux d'alimentation alternative, une panne de réseau d'alimentation alternative entraîne la perte d'alimentation vers les serveurs de priorité inférieure.

- 1 **Problème** : les serveurs de niveau de priorité le plus faible ne sont plus alimentés suite à une panne d'unité d'alimentation.
 - o **Résolution** : ce comportement est normal si la stratégie d'alimentation de l'enceinte a été configurée sur **Pas de redondance**. Pour éviter toute panne future du bloc d'alimentation entraînant la mise hors tension des serveurs, veillez à ce que le châssis dispose d'au moins quatre blocs d'alimentation et soit configuré pour la stratégie **Redondance du bloc d'alimentation** afin d'empêcher la panne d'unité d'alimentation d'affecter le fonctionnement du serveur.

- 1 **Problème** : les performances globales du serveur diminuent lorsque la température ambiante augmente dans le centre de données.
 - o **Résolution** : cette situation peut se produire si le paramètre **Limite de puissance d'entrée système** a été configuré sur une valeur entraînant un besoin accru de puissance pour les ventilateurs devant être réduits dans l'allocation de puissance vers les serveurs. L'utilisateur peut définir la **Limite de puissance d'entrée système** sur une valeur supérieure afin de permettre une allocation de puissance supplémentaire aux ventilateurs sans affecter les performances du serveur.

Affichage des résumés du châssis

CMC fournit des aperçus qui regroupent les informations relatives au châssis, aux contrôleurs CMC principal et de secours, à iKVM, aux ventilateurs, aux capteurs de température et aux modules d'E/S.

Utilisation de l'interface Web

Pour afficher les résumés du châssis, des contrôleurs CMC, du module iKVM et des modules d'E/S :

1. Ouvrez une session sur l'interface Web de CMC.
2. Sélectionnez **Chassis (Châssis)** dans l'arborescence.
3. Cliquez sur l'onglet **Résumé**. La page **Résumé du châssis** s'affiche.

Les [Tableau 12-4](#), [Tableau 12-5](#), [Tableau 12-6](#) et [Tableau 12-7](#) décrivent les informations affichées à la page **Résumé du châssis**.

Tableau 12-4. Résumé du châssis

Élément	Description
---------	-------------

Nom	Affiche le nom du châssis. Le nom identifie le châssis sur le réseau. Pour plus d'informations sur la définition du nom du châssis, voir Editing Slot Names .
Modèle	Affiche le modèle de châssis ou son fabricant. Par exemple, PowerEdge 2900.
Numéro de service	Affiche le numéro de service du châssis. Le numéro de service est un identifiant unique fourni par le fabricant pour le support et la maintenance.
Numéro d'inventaire	Affiche le numéro d'inventaire du châssis.
Emplacement	Affiche l'emplacement du châssis.
Basculement CMC disponible	Indique (Oui , Non) si le contrôleur CMC de secours (le cas échéant) est capable de prendre le relais en cas de basculement.
Condition de la puissance système	Affiche la condition de la puissance système.

Tableau 12-5. Résumé CMC

Élément	Description
Information de CMC actif	
Nom	Affiche le nom CMC. Par exemple, CMC actif ou CMC de secours.
Description	Fournit une brève description de l'utilisation à laquelle CMC est destiné.
Date/Heure	Affiche la date et l'heure actuellement définies sur le contrôleur CMC actif.
Emplacement du logement du contrôleur CMC actif	Affiche le logement sur le contrôleur CMC actif.
Mode de redondance	Indique si le contrôleur CMC de secours est présent dans le châssis.
Version du micrologiciel principale	Affiche la version du micrologiciel du contrôleur CMC actif.
Dernière mise à jour de micrologiciel	Indique la date de la dernière mise à jour du micrologiciel. Si aucune mise à jour n'a été effectuée, cette propriété affiche -.
Versión du matériel	Affiche la version matérielle du contrôleur CMC actif.
MAC Address (Adresse Mac)	Affiche l'adresse MAC de l'interface réseau de CMC. L'adresse MAC est un identificateur unique pour CMC sur le réseau.
Adresse IP	Affiche l'adresse IP de l'interface réseau de CMC.
Passerelle	Affiche la passerelle de l'interface réseau de CMC.
Masque de sous-réseau	Affiche le masque de sous-réseau de l'interface réseau de CMC.
Utiliser DHCP (pour l'adresse IP d'interface réseau)	Indique si CMC est activé pour demander et obtenir automatiquement une adresse IP auprès du serveur DHCP (protocole de configuration dynamique des hôtes) (Oui ou Non). Le paramètre par défaut de cette propriété est Non .
Serveur DNS principal	Indique le nom du serveur DNS principal.
Autre serveur DNS	Indique le nom du serveur DNS secondaire.
Utiliser DHCP pour le nom de domaine DNS	Indique l'utilisation de DHCP pour acquérir le nom de domaine DNS (Oui , Non).
Nom de domaine DNS	Affiche le nom de domaine DNS.
Informations sur le contrôleur CMC de secours	
Présent	Indique (Oui , Non) si un second contrôleur CMC (de secours) est installé.
Version du micrologiciel de secours	Affiche la version du micrologiciel CMC installé sur le contrôleur CMC de secours.

Tableau 12-6. Résumé du module iKVM

Élément	Description
Présent	Indique si le module iKVM est présent (oui ou non).
Nom	Affiche le nom iKVM. Le nom identifie le module iKVM sur le réseau.
Fabricant	Affiche le modèle iKVM ou son fabricant.
Numéro de pièce	Affiche le numéro de pièce d'iKVM. Le numéro de pièce est un identificateur unique fourni par le fournisseur. Les conventions d'attribution des noms des numéros de pièce diffèrent d'un fournisseur à l'autre.
Version du micrologiciel	Indique la version du micrologiciel iKVM.
Versión du matériel	Indique la version du micrologiciel iKVM.
État de l'alimentation	Indique l'état de l'alimentation d'iKVM : sous tension , hors tension ou N/A (absente).

USB/Vidéo du panneau avant activés	Indique si les connecteurs USB et VGA du panneau avant sont activés (Oui ou Non).
Autoriser l'accès à l'interface de ligne de commande CMC à partir du module iKVM	Indique que l'accès à l'interface de ligne de commande est activé sur le module iKVM (Oui ou Non).

Tableau 12-7. Résumé des modules d'E/S

Élément	Description
Emplacement	Indique les logements occupés par les modules d'E/S. Six logements sont identifiés par nom de groupe (A, B ou C) et par numéro de logement (1 ou 2). Noms des logements : A-1, A-2, B-1, B-2, C-1 ou C-2.
Présent	Indique si le module d'E/S est présent (oui ou non).
Nom	Affiche le nom du module.
Structure	Affiche le type de structure.
État de l'alimentation	Indique la condition de l'alimentation du module d'E/S : sous tension, hors tension ou N/A (absente).
Numéro de service	Affiche le numéro de service du module d'E/S. Le numéro de service est un identifiant unique fourni par le fabricant pour le support et la maintenance.

Utilisation de la RACADM

1. Ouvrez une console texte série/Telnet/SSH d'accès à CMC, puis ouvrez une session.

2. Pour afficher les résumés du châssis et CMC, entrez :

```
racadm getsysinfo
```

3. Pour afficher le résumé iKVM, tapez :

```
racadm getkvminfo
```

4. Pour afficher le résumé du module d'E/S, tapez :

```
racadm getioinfo
```

Affichage de la condition d'intégrité du châssis et des composants

Utilisation de l'interface Web

Pour afficher les résumés du châssis et d'intégrité des composants :

1. Ouvrez une session sur l'interface Web de CMC.

2. Sélectionnez **Chassis** (Châssis) dans l'arborescence. La page **Intégrité du châssis** s'affiche.

La section **Graphiques du châssis** fournit une vue avant et arrière du châssis. Cette représentation graphique fournit un aperçu des composants installés dans le châssis et de leur état correspondant.

Chaque graphique affiche une représentation en temps réel des composants installés. L'état du composant est indiqué par la couleur du sous-graphique de composant.

- 1 Aucune couleur : le composant est présent, sous tension et communique avec CMC, aucune indication d'événement indésirable.
- 1 Panneau orange : indique que seules des alertes sont émises et que des mesures correctives doivent être prises.
- 1 Croix rouge : indique qu'au moins une condition de panne est présente. Cela signifie que CMC peut toujours communiquer avec le composant et que la condition d'intégrité signalée est critique.
- 1 Grisé : indique que le composant est présent et n'est pas sous tension. Il ne communique pas avec CMC et il n'y a aucune indication de condition indésirable.

Un champ textuel ou un infobulle correspondant au composant s'affiche lorsque vous placez le curseur sur le sous-graphique de ce dernier. L'état du composant est mis à jour de manière dynamique et les couleurs du sous-graphique correspondant, ainsi que les champs textuels sont automatiquement modifiés.

En cliquant sur le sous-graphique du composant, vous sélectionnez les renseignements sur ce composant et les Liens rapides pour afficher sous les graphiques du châssis.

La section Journal du matériel CMC fournit les 10 dernières entrées du Journal du matériel CMC à des fins de référence (voir Affichage du journal du matériel).

Utilisation de la RACADM

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

```
racadm getmodinfo
```

Affichage des journaux d'événements

Les pages **Journal du matériel** et **Journal CMC** affichent les événements critiques pour le système qui surviennent sur le système géré.

Affichage du journal du matériel

CMC génère un journal du matériel pour les événements qui surviennent sur le châssis. Vous pouvez afficher le journal du matériel à l'aide de l'interface Web et de la RACADM distante.

 **REMARQUE** : vous devez disposer du privilège **Administrateur d'effacement des journaux** pour effacer le journal du matériel.

 **REMARQUE** : vous pouvez configurer CMC de manière à envoyer des e-mails ou des interruptions SNMP lorsque des événements spécifiques se produisent. Pour des informations sur la configuration CMC concernant l'envoi des alertes, voir [Configuration des alertes SNMP](#) et [Configuration des alertes par e-mail](#).

Exemples d'entrées du journal du matériel

```
critical System Software event: redundancy lost

Wed May 09 15:26:28 2007 normal System Software event: log cleared was asserted

Wed May 09 16:06:00 2007 warning System Software event: predictive failure was asserted

Wed May 09 15:26:31 2007 critical System Software event: log full was asserted

Wed May 09 15:47:23 2007 unknown System Software event: unknown event
```

Utilisation de l'interface Web

Vous pouvez afficher le journal du matériel, l'enregistrer dans un fichier texte et l'effacer via l'interface Web CMC.

Le [Tableau 12-8](#) décrit les informations fournies sur la page **Journal du matériel** de l'interface Web CMC.

Pour afficher le journal du matériel :

1. Ouvrez une session sur l'interface Web de CMC.
2. Sélectionnez **Châssis** dans l'arborescence.
3. Cliquez sur l'onglet **Journaux**.
4. Cliquez sur le sous-onglet **Journal du matériel**. La page **Journal du matériel** s'affiche.

Pour enregistrer une copie du journal du matériel sur votre station de gestion ou sur le réseau :

1. Cliquez sur **Enregistrer le journal**.
Une boîte de dialogue s'ouvre.
2. Sélectionnez un emplacement pour un fichier texte du journal.

 **REMARQUE** : les images graphiques utilisées pour indiquer la gravité dans l'interface utilisateur n'apparaissent pas dans le journal car ce dernier est enregistré en tant que fichier texte. Dans ce fichier texte, la gravité est indiquée par les termes OK, Informatif, Inconnu, Avertissement et Grave. Les entrées de date et d'heure apparaissent dans l'ordre ascendant. Si <DÉMARRAGE SYSTÈME> apparaît dans la colonne Date et heure, cela signifie que l'événement s'est produit à l'arrêt ou au démarrage de l'un des modules, lorsqu'aucune date ou heure n'est disponible.

Pour effacer le journal de matériel, cliquez sur **Effacer le journal**.

 **REMARQUE** : CMC crée une nouvelle entrée du journal qui indique que celui-ci a été effacé.

Tableau 12-8. Informations du journal du matériel

Élément	Description	
Sévérité	 OK	Indique un événement normal qui ne nécessite pas d'actions correctives.
	 Informatif	Indique une entrée informative relative à un événement pour lequel la condition Gravité n'a pas été modifiée.
	 Inconnu	Indique un événement non critique pour lequel des actions correctives doivent être effectuées rapidement pour éviter les pannes système.
	 Avertissement	Indique un événement critique nécessitant des actions correctives immédiates pour éviter les pannes système.
	 Grave	Indique un événement critique nécessitant des mesures correctives immédiates pour éviter les pannes système.
Date/Heure	Indique la date et l'heure exactes auxquelles l'événement s'est produit (par exemple, en anglais Wed May 02 16:26:55 2007). Si les champs de la date et de l'heure sont vides, cela signifie que l'événement s'est produit au démarrage du système.	
Description	Fournit une brève description, générée par CMC, de l'événement (par exemple, Perte de redondance, Serveur inséré).	

Utilisation de la RACADM

1. Ouvrez une console texte série/Telnet/SSH d'accès à CMC, puis ouvrez une session.

2. Pour afficher le journal du matériel, entrez :

```
racadm getsel
```

Pour effacer le journal du matériel, tapez :

```
racadm clrsel
```

Affichage du journal CMC

CMC génère un journal des événements liés au châssis.

 **REMARQUE** : vous devez disposer du privilège **Administrateur d'effacement des journaux** pour effacer le journal du matériel.

Utilisation de l'interface Web

Vous pouvez afficher le journal CMC, l'enregistrer dans un fichier texte et l'effacer via l'interface Web CMC.

Le journal peut être à nouveau trié par source, date et heure ou description en cliquant sur l'en-tête de colonne correspondant. Pour inverser le tri, il vous suffit de cliquer de nouveau sur les en-têtes de colonne.

Le [Tableau 12-9](#) décrit les informations de la page **Journal CMC** de l'interface Web CMC.

Pour afficher le journal CMC :

1. Ouvrez une session sur l'interface Web de CMC.
2. Sélectionnez **Châssis** dans l'arborescence.
3. Cliquez sur l'onglet **Journaux**.

4. Cliquez sur le sous-onglet **Journal CMC**. La page **Journal CMC** s'affiche.
5. Cliquez sur **Enregistrer le journal** pour enregistrer une copie du journal CMC sur votre station de gestion ou sur le réseau.

La boîte de dialogue s'ouvre. Choisissez l'emplacement d'enregistrement du fichier texte du journal.

Tableau 12-9. Informations du journal CMC

Commande	Résultat
Source	Indique l'interface (par exemple CMC) ayant provoqué l'événement.
Date/Heure	Indique la date et l'heure exactes auxquelles l'événement s'est produit (par exemple, en anglais Wed May 02 16:26:55 2007).
Description	Fournit une brève description de l'action, telle qu'une ouverture ou fermeture de session, un échec d'ouverture de session ou l'effacement des journaux. Les descriptions sont générées par CMC.

Utilisation de la RACADM

1. Ouvrez une console texte série/Telnet/SSH d'accès à CMC, puis ouvrez une session.

2. Pour afficher le journal du matériel, entrez :

```
racadm gettraclog
```

Pour effacer le journal du matériel, tapez :

```
racadm clrtraclog
```

Utilisation de la console de diagnostic

La page **Console de diagnostic** permet à un utilisateur avancé ou à un utilisateur sous la supervision du support technique de diagnostiquer les problèmes matériels du châssis à l'aide de commandes CLI.

 **REMARQUE** : vous devez disposer du privilège **Administrateur de commandes de débogage** pour modifier ces paramètres.

Pour accéder à la page **Console de diagnostic** :

1. Ouvrez une session sur l'interface Web de CMC.
2. Sélectionnez **Châssis** dans l'arborescence.
3. Cliquez sur l'onglet **Dépannage**.
4. Cliquez sur le sous-onglet **Diagnostic**. La page **Console de diagnostic** s'affiche.

Pour exécuter une commande CLI de diagnostic, tapez la commande dans le champ **Saisir une commande RACADM**, puis cliquez sur **Envoyer** pour exécuter la commande de diagnostic. La page Résultats des diagnostics apparaît.

Pour retourner à la page **Console de diagnostic**, cliquez sur **Retour à la page Console de diagnostic** ou sur **Actualiser**.

La console de diagnostic prend en charge les commandes répertoriées dans le [Tableau 12-10](#) ainsi que les commandes RACADM.

Tableau 12-10. Commandes de diagnostic prises en charge

Commande	Résultat
arp	Affiche le contenu de la table du protocole de résolution d'adresses (ARP). Les entrées ARP ne peuvent être ni ajoutées, ni supprimées.
ifconfig	Affiche le contenu de la table d'interface réseau.
netstat	Imprime le contenu du tableau de routage.
ping <adresse IP>	Vérifie que l'<adresse IP> de destination est accessible à partir de CMC avec le contenu actuel du tableau de routage. Vous devez saisir une adresse IP de destination dans le champ situé à droite de cette option. Un paquet d'écho du protocole de contrôle des messages sur Internet (ICMP) est envoyé à l'adresse IP de destination en fonction du contenu actuel de la table de routage.
gettracelog	Affiche le journal de suivi (cette opération peut prendre quelques secondes). La commande gettracelog -i renvoie le nombre d'enregistrements figurant dans le journal de suivi.

REMARQUE : pour des informations supplémentaires sur la commande gettracelog, voir la section de la commande gettracelog dans le *Guide de référence de ligne de commande pour iDRAC6 et CMC*.

Réinitialisation des composants

La page **Réinitialiser les composants** permet aux utilisateurs de réinitialiser le contrôleur CMC actif, ou de réattribuer virtuellement un siège aux serveurs, les obligeant ainsi à se comporter comme s'ils avaient été retirés et réinsérés. Si le châssis intègre un contrôleur CMC de secours, la réinitialisation de CMC actif entraîne un basculement et le contrôleur CMC de secours devient alors actif.

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

Pour accéder à la page **Console de diagnostic** :

1. Ouvrez une session sur l'interface Web de CMC.
2. Sélectionnez **Châssis** dans l'arborescence.
3. Cliquez sur l'onglet **Dépannage**.
4. Cliquez sur le sous-onglet **Réinitialiser les composants**. La page **Réinitialiser les composants** s'affiche. La section **Résumé CMC** de la page **Réinitialiser les composants** affiche les informations suivantes :

Tableau 12-11. Résumé CMC

Attribut	Description	
Intégrité	 OK	CMC est présent et communique avec ses composants.
	 Informatif	Affiche des informations sur CMC en l'absence de modification de la condition de l'intégrité (OK, Avertissement, Grave).
	 Avertissement	Des alertes d'avertissement ont été émises et des actions correctives doivent être effectuées . Si aucune action corrective n'est effectuée, des pannes critiques ou graves susceptibles d'affecter l'intégrité de CMC peuvent se produire.
	 Grave	Au moins une alerte de panne a été générée. L'état grave représente une panne système de CMC et une action corrective doit être effectuée immédiatement .
Date/Heure		Affiche la date et l'heure de CMC au format <i>MM/JJ/AAAA</i> , où <i>MM</i> correspond au mois, <i>JJ</i> à la date et <i>AAAA</i> à l'année.
Emplacement du logement du contrôleur CMC actif		Affiche le logement sur le contrôleur CMC actif.
Mode de redondance		Affiche Redondant si un contrôleur CMC de secours est présent dans le châssis, et Pas de redondance si aucun contrôleur CMC de secours n'est présent dans le châssis.

5. La section **Réattribuer virtuellement un siège aux serveurs** de la page **Réinitialiser les composants** affiche les informations suivantes :

Tableau 12-12. Réattribuer virtuellement un siège aux serveurs

Attribut	Description	
Ordre de priorité	Indique le logement occupé par le serveur du châssis. Les noms de logement sont des ID séquentiels, allant de 1 à 16, permettant d'identifier l'emplacement du serveur au sein du châssis.	
Nom	Affiche le nom du serveur dans chaque logement.	
Présent	Indique si le serveur est présent dans le logement (Oui ou Non).	
Intégrité	 OK	Le serveur est présent et communique avec CMC. En cas de perte de la communication entre CMC et le serveur, CMC ne pourra pas obtenir ni afficher la condition d'intégrité du serveur.

		Informatif	Affiche des informations sur le serveur en l'absence de modification de l'état de l'intégrité (OK, Avertissement, Grave).
		Avertissement	Des alertes d'avertissement ont été émises et des actions correctives doivent être effectuées . Si aucune action corrective n'est effectuée, des pannes critiques ou graves susceptibles d'affecter l'intégrité du serveur peuvent se produire.
		Grave	Au moins une alerte de panne a été générée. L'état grave représente une panne système de CMC et une action corrective doit être effectuée immédiatement .
Condition iDRAC			<p>Affiche la condition du contrôleur de gestion intégré iDRAC du serveur :</p> <ul style="list-style-type: none"> 1 N/A : le serveur n'est pas présent ou le châssis n'est pas sous tension. 1 Prêt : l'iDRAC est prêt et fonctionne normalement. 1 Corrompu : le micrologiciel iDRAC est corrompu. Utilisez l'utilitaire de mise à jour du micrologiciel iDRAC pour réparer le micrologiciel. 1 Échec : impossible de communiquer avec iDRAC. Cochez la case Réattribuer virtuellement un siège pour supprimer l'erreur. Si cette opération échoue, retirez et remplacez manuellement le serveur pour supprimer l'erreur. 1 Mise à jour du micrologiciel : la mise à jour du micrologiciel iDRAC est en cours ; attendez que la mise à jour se termine avant de tenter une action quelconque. 1 Initialisation : la réinitialisation iDRAC est en cours ; attendez que la mise sous tension du contrôleur se termine avant de tenter une action quelconque.
État de l'alimentation			<p>Affiche la condition de l'alimentation du serveur :</p> <ul style="list-style-type: none"> 1 N/A : CMC n'a pas déterminé l'état d'alimentation du serveur. 1 Désactivé : le serveur ou le châssis est hors tension. 1 Activé : le châssis et le serveur sont sous tension. 1 Activation : état temporaire entre le mode Désactivé et Activé. Lorsque le cycle d'activation est terminé, l'état d'alimentation passe en mode Activé. 1 Mise hors tension : état temporaire entre le mode Activé et Désactivé. Lorsque le cycle de désactivation est terminé, l'état d'alimentation passe en mode Désactivé.
Réattribuer virtuellement un siège			Cochez la case pour réattribuer virtuellement un siège à ce serveur.

6. Pour réattribuer virtuellement un siège à un serveur, cochez la case des serveurs dont le siège sera réattribué, puis sélectionnez **Appliquer les sélections**. Cette opération oblige les serveurs à se comporter comme s'ils avaient été retirés et réinsérés.
7. Sélectionnez **Réinitialisation/Basculement de CMC** pour entraîner la réinitialisation de CMC actif. Si un contrôleur CMC de secours est présent et qu'un châssis est pleinement redondant, un basculement se produit, amenant le contrôleur CMC de secours à devenir actif.

Résolution des erreurs de protocole de temps du réseau (NTP)

Après avoir configuré CMC afin qu'il synchronise son horloge avec un serveur de temps distant sur le réseau, un délai de 2 à 3 minutes peut s'écouler avant qu'une modification de la date et du temps ne se produise. Si aucun changement n'a eu lieu une fois ce délai écoulé, il peut être nécessaire de procéder à un dépannage d'un problème. CMC peut ne pas être en mesure de synchroniser son horloge pour plusieurs raisons :

- 1 Un problème lié aux paramètres du serveur NTP 1, du serveur NTP 2 et du serveur NTP 3 a pu se produire.
- 1 Un nom d'hôte ou une adresse IP non valide a pu être entré(e) par erreur.
- 1 Un problème de connectivité réseau empêchant CMC de communiquer avec l'un des serveurs NTP configurés a pu se produire.
- 1 Un problème de DNS empêchant la résolution de l'un des noms d'hôte de serveur NTP a pu se produire.

CMC fournit des outils de dépannage de ces problèmes ; la principale source d'informations de dépannage étant le journal de suivi CMC. Ce journal contient un message d'erreur concernant les pannes inhérentes à NTP. Si le CMC n'est pas en mesure d'effectuer la synchronisation avec l'un des serveurs NTP distants ayant été configurés, il dérive alors sa synchronisation de l'horloge système local.

Si le CMC est synchronisé sur l'horloge système local plutôt que sur un serveur de temps distant, le journal de suivi contient une entrée similaire à la suivante :

```
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 gettractime -n
```

Si aucun « * » n'est affiché par rapport à l'un des serveurs configurés, il est possible qu'un élément ne soit pas configuré correctement. La sortie de la commande ci-dessus contient également des statistiques NTP détaillées qui peuvent faciliter le débogage du problème de non-synchronisation du serveur. Si vous tentez de configurer un serveur NTP basé sur Windows, il peut s'avérer utile d'augmenter le paramètre MaxDist pour ntpd. Avant de modifier ce paramètre, il convient de bien lire et de bien comprendre toutes les implications que cela comporte, tout particulièrement car le paramètre par défaut doit être suffisamment élevé pour pouvoir être accepté par la majorité des serveurs NTP. Pour modifier le type de paramètre, tapez la commande suivante :

```
racadm config -g cfgRemoteHosts -o cfgRhostsNtpMaxDist 32
```

Après avoir effectué la modification, redémarrez ntpd en désactivant NTP, en attendant entre 5 et 10 secondes, puis en réactivant NTP.

 **REMARQUE** : NTP peut avoir besoin de 3 minutes de plus pour se synchroniser.

Pour désactiver NTP, tapez :

```
racadm config -g cfgRemoteHosts -o cfgRhostsNtpEnable 0
```

Pour activer NTP, tapez :

```
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.

D'autres entrées du journal de suivi inhérentes à NTP peuvent vous aider dans votre entreprise de dépannage. S'il s'agit d'un problème de configuration incorrecte de l'adresse IP du serveur NTP, une entrée similaire à la suivante risque de s'afficher :

```
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 du 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
```

Voir [Utilisation de la console de diagnostic](#) pour plus d'informations sur la façon d'entrer la commande `gettracelog` pour passer en revue le journal de suivi à l'aide de l'interface utilisateur graphique de CMC.

Interprétation des couleurs des LED et séquences de clignotement

Les LED du châssis fournissent des informations selon leur couleur et leur clignotement ou absence de clignotement :

- 1 Une LED verte permanente indique que le composant est sous tension. Si une LED verte clignote, cela indique un événement critique mais de routine, comme par exemple le téléversement du micrologiciel, au cours duquel l'unité est indisponible. Cela n'indique pas une panne.
- 1 Une LED orange qui clignote pour un module indique une panne de ce module.
- 1 L'utilisateur peut configurer les LED bleues clignotantes et les utiliser pour l'identification (voir [Configuration des LED pour l'identification des composants du châssis](#)).

Tableau 12-13. Couleurs 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	Mode Veille
Module 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

	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
Bloc d'alimentation	(Oval) Vert, continu	Alimentation en courant alternatif OK
	(Oval) Vert, clignotant	Inutilisé
	(Oval) Vert, foncé	Alimentation en courant alternatif défectueuse
	Orange, continu	Inutilisé
	Orange, clignotant	Panne
	Orange, foncé	Pas de panne
	(Cercle) Vert, continu	Alimentation en courant continu OK
	(Cercle) Vert, foncé	Alimentation en courant continu défectueuse

Dépannage d'un contrôleur CMC qui ne répond pas

 **REMARQUE** : il est impossible de se connecter sur le contrôleur CMC de secours à l'aide d'une console série.

Si vous ne pouvez pas ouvrir une session sur CMC via l'une des interfaces (interface Web, Telnet, SSH, RACADM distante ou série), vérifiez la fonctionnalité CMC en observant les LED de CMC, en obtenant les informations de récupération via le port série DB-9 ou en récupérant l'image du micrologiciel CMC.

Observation des LED afin d'isoler le problème

Lorsque vous faites face à CMC tel qu'il est installé dans le châssis, vous verrez deux LED du côté gauche de la carte.

LED du haut : la LED verte supérieure indique l'état de l'alimentation. Si celle-ci n'est PAS allumée :

1. Vérifiez qu'une alimentation secteur est présente sur au moins l'un des blocs d'alimentation.
2. Vérifiez que la carte CMC est correctement insérée. Vous pouvez tirer sur la poignée d'éjection, retirer la carte CMC et la réinstaller en vous assurant qu'elle est insérée complètement et que le loquet se ferme correctement.

LED du bas : la LED inférieure est multicolore. Lorsque le contrôleur CMC est actif et en cours de fonctionnement, et lorsqu'il n'y a pas de problème, la LED inférieure est bleue. Si elle est orange, une panne a été détectée. Cette panne peut avoir été causée par l'un des trois événements suivants :

- 1 Une panne du noyau. Dans ce cas, la carte CMC doit être remplacée.
- 1 Un échec de l'auto-test. Dans ce cas, la carte CMC doit être remplacée.
- 1 Une corruption de l'image. Dans ce cas, vous pouvez récupérer la carte CMC en téléversant l'image du micrologiciel CMC.

 **REMARQUE** : plus d'une minute est nécessaire pour amorcer/réinitialiser normalement CMC sur le système d'exploitation concerné avant de pouvoir ouvrir une session. La LED bleue est activée sur le CMC actif. Dans une configuration redondante comprenant deux CMC, seule la LED supérieure verte est activée sur le contrôleur CMC de secours.

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

Lorsque la LED inférieure est orange, les informations de récupération doivent être disponibles via le port série DB-9 situé à l'avant de CMC.

Pour obtenir les informations de récupération :

1. Installez un câble de modem NULL entre CMC et un ordinateur client.
2. Ouvrez le logiciel d'émulation de terminal de votre choix (comme par exemple HyperTerminal ou Minicom). Configurez les paramètres suivants : 8 bits, aucune parité, aucun contrôle du débit, 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 **récupération** s'affiche, des informations supplémentaires sont disponibles. L'invite indique le numéro d'emplacement CMC et le type de panne.

Pour afficher la cause de la panne ainsi que la syntaxe de quelques commandes, tapez

```
recover
```

puis appuyez sur <Entrée>. Exemples d'invites :

```
recover1[self test] CMC 1 self test failure
```

```
recover2[Bad FW images] CMC2 has corrupted images
```

- 1 Si l'invite indique un échec de l'auto-test, il n'y a pas de composant réparable sur CMC. CMC est défectueux et doit être renvoyé à Dell.
- 1 Si l'invite indique **Bad FW Images**, suivez les étapes fournies dans la section [Récupération de l'image du micrologiciel](#) pour résoudre le problème.

Récupération de l'image du micrologiciel

CMC entre en mode de récupération lorsqu'un démarrage normal du système d'exploitation CMC n'est pas possible. En mode de récupération, un sous-ensemble réduit de commandes est disponible qui vous permet de reprogrammer les périphériques Flash en téléversant le fichier de mise à jour du micrologiciel, `firmimg.cmc`. Il s'agit du même fichier image de micrologiciel que celui utilisé pour les mises à jour normales du micrologiciel. La procédure de récupération affiche les opérations en cours et redémarre le système d'exploitation de CMC lorsqu'elle a terminé.

Lorsque vous tapez la commande `recover` et que vous appuyez ensuite sur <Entrée> à l'invite **de récupération**, la cause de la récupération et les sous-commandes disponibles s'affichent. Voici un exemple de séquence de récupération :

```
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 situé le plus à gauche

 **REMARQUE** : en mode récupération, vous ne pouvez pas utiliser normalement la commande ping sur CMC car aucune pile réseau n'est active. La commande de récupération `ping <IP serveur TFTP>` vous permet d'utiliser la commande ping sur le serveur TFTP afin de vérifier la connexion au réseau local. Sur certains systèmes, vous devrez peut-être utiliser la commande `recover reset` après la commande `setniccfg`.

Dépannage des problèmes de réseau

Le journal de suivi CMC interne vous permet de déboguer les problèmes d'alerte et de réseau CMC. Vous pouvez accéder au journal de suivi via l'interface Web CMC (voir [Utilisation de la console de diagnostic](#)) ou la RACADM (voir [Utilisation de l'interface de ligne de commande RACADM](#)) et la section relative à la commande `gettracelog` du *Guide de référence de la ligne de commande pour iDRAC et CMC*.

Le journal de suivi enregistre les informations suivantes :

- 1 DHCP : effectue le suivi des paquets envoyés à un serveur DHCP et reçus de celui-ci.
- 1 DDNS : effectue le suivi des requêtes et des réponses de mise à jour du DNS.
- 1 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 de mot de passe administrateur oublié

 **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 d'entretien 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.

Un utilisateur doit disposer de privilèges Administrateur pour réaliser des opérations de gestion. Le logiciel CMC possède une fonctionnalité de protection du mot de passe de compte utilisateur qui peut être désactivée en cas d'oubli du mot de passe du compte administrateur. En cas d'oubli du mot de passe du compte administrateur, ce dernier peut être récupéré via le cavalier PASSWORD_RST sur la carte CMC.

La carte CMC possède un connecteur de réinitialisation du mot de passe à deux fiches comme décrit dans la [Figure 12-1](#). Si un cavalier est installé dans le connecteur de réinitialisation, le mot de passe et le compte d'administrateur par défaut sont activés et définis sur les valeurs par défaut suivantes : **nom d'utilisateur : root** et **mot de passe : calvin**. Le compte d'administrateur est réinitialisé sans tenir compte de la suppression du compte ou de la modification du mot de passe.

 **REMARQUE** : assurez-vous que le module CMC est en mode passif avant de démarrer.

Un utilisateur doit disposer de privilèges Administrateur pour réaliser des opérations de gestion. En cas d'oubli du mot de passe du compte administrateur, ce dernier peut être récupéré via le cavalier PASSWORD_RST sur la carte CMC.

Le cavalier PASSWORD_RST utilise un connecteur à deux broches comme indiqué dans la [Figure 12-1](#).

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 blocage de CMC situé sur la poignée et faites pivoter la poignée à l'opposé du panneau avant du module. Faites glisser le module CMC hors de l'enceinte.

 **REMARQUE** : les décharges électrostatiques peuvent affecter le CMC. Sous certaines conditions, les décharges électrostatiques peuvent s'accumuler dans votre organisme ou dans un objet, puis être transmises à un autre objet, comme votre CMC. Pour éviter les dommages liés aux décharges électrostatiques, vous devez prendre des précautions pour décharger l'électricité statique de votre corps lors de la manipulation et de l'accès au CMC en dehors du châssis.

2. Retirez la fiche de cavalier du connecteur de réinitialisation du mot de passe, puis insérez la fiche à deux broches afin d'activer le compte Administrateur par défaut. Pour identifier l'emplacement du cavalier de mot de passe sur la carte CMC, voir [Figure 12-1](#).

Figure 12-1. Emplacement du cavalier de réinitialisation du mot de passe

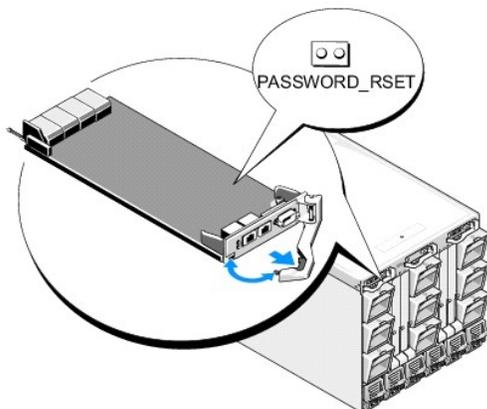


Tableau 12-14. Paramètres du cavalier de mot de passe CMC

PASSWORD_RSET	 (par défaut)	La fonction de réinitialisation du mot de passe est désactivée.
		La fonction de réinitialisation du mot de passe est activée.

- Faites glisser le module CMC dans l'enceinte. Rebranchez les câbles qui ont été débranchés.

 **REMARQUE** : veillez à ce que le module CMC branché par cavaliers devienne le module actif et le reste jusqu'à ce que les étapes restantes soient terminées.

- Si le module CMC branché par cavaliers est le seul module CMC, il vous suffit d'attendre qu'il ait fini de redémarrer. En cas de présence de CMC redondants dans votre châssis, effectuez un changement pour rendre actif le module CMC branché par cavaliers. Sur l'interface utilisateur :

- Naviguez jusqu'à la page du **Châssis**, cliquez sur l'onglet **Alimentation** → sous-onglet **Contrôle**.
- Sélectionnez le bouton **Réinitialiser le CMC (démarrage à chaud)**.
- Cliquez sur **Appliquer**.

Le CMC bascule automatiquement sur le module redondant qui devient maintenant actif.

- Connectez-vous au CMC actif à l'aide du nom d'utilisateur Administrateur par défaut (**root**) et du mot de passe (**calvin**), puis restaurez (le cas échéant) les paramètres de compte utilisateur. Les comptes et les mots de passe existants ne sont pas désactivés et restent actifs.
- Effectuez toutes les actions de gestion nécessaires, y compris la création d'un nouveau mot de passe administrateur à la place de celui oublié.
- Retirez le cavalier PASSWORD_RST à 2 broches, puis replacez la fiche de cavalier.
 - Appuyez sur le loquet de blocage de CMC situé sur la poignée et faites pivoter la poignée à l'opposé du panneau avant du module. Faites glisser le module CMC hors de l'enceinte.
 - Retirez la fiche de cavalier à 2 broches puis replacez la fiche de cavalier.
 - Faites glisser le module CMC dans l'enceinte. Rebranchez les câbles qui ont été débranchés. Répétez l'[étape 4](#) pour faire du module CMC non cavalier le CMC actif.

Dépannage des alertes

Utilisez le journal CMC et le journal de suivi pour dépanner les alertes CMC. Le succès ou l'échec de chaque tentative d'envoi d'e-mail et/ou interruption SNMP est enregistré dans le journal CMC. Le journal de suivi contient lui des informations complémentaires sur les erreurs spécifiques. Cependant, étant donné que SNMP ne confirme pas la livraison des interruptions, utilisez un analyseur réseau ou un outil tel que, **snmputil** de Microsoft pour effectuer le suivi des paquets sur le système géré.

Vous pouvez configurer les alertes SNMP à l'aide de l'interface Web. Pour plus d'informations, voir [Configuration des alertes SNMP](#).

[Retour à la page Contenu](#)

[Retour à la page Contenu](#)

Utilisation de l'interface Web de CMC

Micrologiciel Dell Chassis Management Controller Version 3.1 Guide d'utilisation

- [Accès à l'interface Web CMC](#)
- [Configuration des paramètres CMC de base](#)
- [Page Intégrité du châssis](#)
- [Utilisation du groupe du châssis](#)
- [Résumé des composants du châssis](#)
- [Informations sur le composant sélectionné](#)
- [Surveillance de la condition d'intégrité du système](#)
- [Affichage de l'état du panneau LCD](#)
- [Affichage des ID de nom mondial/Contrôle de l'accès aux médias \(WWN/MAC\)](#)
- [Configuration des propriétés du réseau CMC](#)
- [Configuration des réseaux locaux virtuels \(VLAN\)](#)
- [Ajout et configuration d'utilisateurs CMC](#)
- [Configuration et gestion des certificats Microsoft Active Directory](#)
- [Gestion des certificats Active Directory](#)
- [Fichier Keytab Kerberos](#)
- [Configuration et gestion des services LDAP génériques](#)
- [Sélection de vos serveurs LDAP](#)
- [Gestion des paramètres de groupe LDAP](#)
- [Gestion des certificats de sécurité LDAP](#)
- [Sécurisation des communications CMC à l'aide de certificats SSL et numériques](#)
- [Gestion des sessions](#)
- [Configuration des services](#)
- [Configuration des bilans de puissance](#)
- [Gestion des mises à jour du micrologiciel](#)
- [Gestion iDRAC](#)
- [FlexAddress](#)
- [Partage de fichiers distants](#)
- [Questions les plus fréquentes](#)
- [Dépannage du CMC](#)

CMC intègre une interface Web qui vous permet de configurer les propriétés et les utilisateurs CMC, d'effectuer les tâches de gestion à distance et de dépanner un système (géré) distant en cas de problème. Pour la gestion quotidienne du châssis, utilisez l'interface Web de CMC. Ce chapitre fournit des informations sur la manière d'effectuer les tâches de gestion courantes du châssis à l'aide de l'interface Web de CMC.

Vous pouvez également effectuer l'ensemble des tâches de configuration à l'aide de commandes RACADM locales ou de consoles de ligne de commande (console série, Telnet ou SSH). Pour plus d'informations sur l'utilisation de RACADM en local, voir [Utilisation de l'interface de ligne de commande RACADM](#). Pour des informations sur l'utilisation des consoles de ligne de commande, voir [Configuration de CMC pour utiliser des consoles de ligne de commande](#).

 **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.

Accès à l'interface Web CMC

Pour accéder à l'interface Web CMC sur IPv4 :

1. Ouvrez une fenêtre d'un navigateur Web pris en charge.

Pour les dernières informations relatives aux navigateurs Web pris en charge, consultez la *Matrice de prise en charge des logiciels des systèmes Dell* sur le site Web du support de Dell à l'adresse support.dell.com/manuals.

2. Entrez l'adresse URL suivante dans le champ Adresse, puis appuyez sur <Entrée> :

```
https://<adresse IP CMC>
```

Si le numéro de port HTTPS par défaut (port 443) a été modifié, entrez :

```
https://<adresse IP CMC>:<numéro de port>
```

où <adresse IP CMC> est l'adresse IP CMC et <numéro de port> le numéro de port HTTPS.

La page **Ouverture de session CMC** s'affiche.

Pour accéder à l'interface Web CMC sur IPv6 :

1. Ouvrez une fenêtre d'un navigateur Web pris en charge.

Pour les dernières informations relatives aux navigateurs Web pris en charge, consultez la *Matrice de prise en charge des logiciels des systèmes Dell* sur le site Web du support de Dell à l'adresse support.dell.com/manuals.

2. Entrez l'adresse URL suivante dans le champ Adresse, puis appuyez sur <Entrée> :

```
https://[<adresse IP CMC>]
```

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

Le numéro de port HTTPS dans l'URL est facultatif si vous utilisez toujours la valeur par défaut (443). Sinon, vous devez spécifier le numéro de port. La syntaxe de l'URL CMC IPv6 avec le numéro de port spécifié est la suivante :

```
https://[<adresse IP CMC>]:<numéro de port>
```

où <adresse IP CMC> est l'adresse IP CMC et <numéro de port> le numéro de port HTTPS.

La page **Ouverture de session CMC** s'affiche.

Ouverture de session

-  **REMARQUE** : pour ouvrir une session CMC, vous devez posséder un compte CMC doté du privilège **Ouverture de session CMC**.
-  **REMARQUE** : par défaut, le nom d'utilisateur est **root** et le mot de passe **calvin**. Le compte root est le compte d'administration par défaut fourni avec le contrôleur CMC. Pour plus de sécurité, Dell recommande fortement de modifier le mot de passe par défaut du compte root lors de la procédure de configuration initiale.
-  **REMARQUE** : 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.
-  **REMARQUE** : 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.

Vous pouvez ouvrir une session en tant qu'utilisateur CMC ou en tant qu'utilisateur Active Directory.

Pour ouvrir une session :

1. Dans le champ **Nom d'utilisateur**, entrez votre nom d'utilisateur :
 - | Nom d'utilisateur du contrôleur CMC : *<nom d'utilisateur>*
 - | Nom d'utilisateur Active Directory : *<domaine>\<nom d'utilisateur>*, *<domaine>/<nom d'utilisateur>* OU *<utilisateur>@<domaine>*.
 - | Nom d'utilisateur LDAP : *<nom d'utilisateur>* **REMARQUE** : ce champ est sensible à la casse.
2. Dans le champ **Mot de passe**, entrez votre mot de passe d'utilisateur pour le contrôleur CMC ou pour Active Directory. **REMARQUE** : ce champ est sensible à la casse.
3. Facultativement, sélectionnez un délai de session. C'est la durée pendant laquelle vous pouvez rester connecté sans activité avant d'être automatiquement déconnecté. La valeur par défaut est définie comme le délai d'inactivité du service Web. Voir Configuration des services pour plus de détails.
4. Cliquez sur **OK** ou appuyez sur <Entrée>.

Fermeture de session

Lorsqu'une session est ouverte dans l'interface Web, vous pouvez à tout moment la fermer en cliquant sur **Fermer la session** dans le coin supérieur droit de chaque page.

-  **REMARQUE** : veillez à appliquer (enregistrer) les paramètres ou les informations entrés sur une page. Si vous fermez la session ou quittez cette page sans appliquer vos modifications, celles-ci seront perdues.

Configuration des paramètres CMC de base

Définition du nom du châssis

Vous pouvez définir le nom utilisé pour identifier le châssis sur le réseau. (Le nom par défaut est « Dell Rack System »). Par exemple, une requête SNMP sur le nom du châssis renvoie le nom que vous avez configuré.

Pour définir le nom du châssis :

1. Ouvrez une session sur l'interface Web de CMC. La page **Intégrité du châssis** s'affiche.
2. Cliquez sur l'onglet **Configuration**. La page **Paramètres généraux du châssis** s'affiche.
3. Entrez le nouveau nom dans le champ **Nom du châssis**, puis cliquez sur **Appliquer**.

Définition de la date et de l'heure sur 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).

1. Ouvrez une session sur l'interface Web de CMC. La page **Intégrité du châssis** s'affiche.
2. Cliquez sur l'onglet **Configuration**. La page **Paramètres généraux du châssis** s'affiche.
3. Cliquez sur le sous-onglet **Date/Heure**. La page **Date et heure** s'affiche.
4. Pour synchroniser la date et l'heure avec un serveur NTP (Network Time Protocol), cochez **Activer NTP** et spécifiez jusqu'à trois serveurs NTP.
5. Pour définir manuellement la date et l'heure, décochez **Activer NTP** et modifiez les champs **Date** et **Heure**, sélectionnez le **Fuseau horaire** dans le menu déroulant, puis cliquez ensuite sur **Appliquer**.

Pour définir la date et l'heure en utilisant l'interface de ligne de commande, consultez les sections de la commande `config` et du groupe de propriétés de base de données `cfgRemoteHosts` dans le *Guide de référence de la ligne de commande pour l'iDRAC6 et le contrôleur CMC*.

Page Intégrité du châssis

Quand vous vous connectez au contrôleur CMC, la page **Intégrité du châssis (Présentation du châssis → Propriétés → Intégrité)** s'affiche. Les informations et actions les plus souvent requises sont disponibles sur cette page. Si votre châssis est configuré en tant que Chef de groupe, la page **Intégrité du châssis** s'affiche après la connexion. Pour des informations supplémentaires, voir [Utilisation du groupe du châssis](#).

La page **Intégrité du châssis** affiche une vue graphique du châssis et de ses composants, ainsi que les détails des composants. Selon le composant sélectionné, différentes actions ou liens vers d'autres pages sont disponibles. En outre, les derniers événements du journal du matériel de CMC sont également affichés.

Toutes les informations sont mises à jour dynamiquement sur la page **Intégrité du châssis**. Cette page contient deux sections : **Résumé des composants du châssis** en haut, suivi de la liste **Événements récents du journal de matériel de CMC**.

La section **Résumé des composants du châssis** (également intitulée « Intégrité du châssis » lorsque les informations générales sur le châssis sont affichées) affiche les graphiques et leurs informations associées. Vous pouvez masquer cette section en cliquant sur l'icône **Fermer**.

La partie gauche de la section **Résumé des composants du châssis** affiche les graphiques et les liens rapides du châssis. La moitié droite affiche des informations, liens et actions liés à l'élément sélectionné. Cliquez sur la représentation graphique d'un composant pour sélectionner le composant. Le graphique devient bleu une fois sélectionné.

La liste **Événements récents du journal de matériel de CMC** affiche les 10 derniers événements de ce journal. Le contenu de cette section est mis à jour dynamiquement et présente les derniers événements en haut de la liste. Pour plus d'informations sur les entrées de journal matériel de CMC, voir [Affichage des journaux d'événements](#).

Utilisation du groupe de châssis

Le contrôleur CMC permet de contrôler plusieurs châssis depuis un seul châssis chef. À l'activation d'un groupe de châssis, le contrôleur CMC du châssis chef génère un affichage graphique de l'état du châssis chef et de tous les châssis membres au sein du groupe de châssis.

Fonctionnalités du groupe de châssis

La page GUI des groupes de châssis affiche des images qui représentent l'arrière et l'avant de chaque châssis, un ensemble pour le châssis chef et un ensemble pour chaque châssis membre.

Des problèmes liés à l'intégrité du chef et des membres d'un groupe sont affichées en couleur rouge ou jaune accompagnés d'une croix X ou d'un ! sur le composant présentant des problèmes. Des détails sont visibles sous l'image du châssis lorsque vous cliquez sur cette dernière ou sur le bouton **Détails**.

Un groupe de châssis peut contenir jusqu'à huit membres. De plus, un chef ou un membre ne peut appartenir qu'à un seul groupe. Un châssis, chef ou membre, faisant partie d'un groupe ne peut pas être ajouté à un autre groupe. Il peut être supprimé d'un groupe, puis ajouté à un autre groupe ultérieurement.

Configuration d'un groupe de châssis

Le groupe de châssis est configuré avec l'interface GUI :

1. Connectez-vous au châssis chef à l'aide des privilèges administrateur.
2. Cliquez sur **Configuration → Administration des groupes**.
La page Groupe de châssis s'affiche.
3. Dans la page Groupe du châssis, sélectionnez **Chef** sous **Rôle**.
Un champ permettant d'ajouter le nom du groupe s'affiche.
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 u groupe.

L'interface GUI devient automatiquement la page GUI du groupe du châssis une fois le groupe du châssis créé. L'arborescence du système affiche le groupe par son nom de groupe et le châssis chef ainsi que le châssis membre non peuplé.

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

1. Connectez-vous au châssis chef à l'aide des privilèges administrateur.
2. Sélectionnez le châssis chef 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 utilisateur** du châssis membre, saisissez un nom utilisateur à l'aide des privilèges administrateur du châssis.
6. Saisissez le mot de passe correspondant dans le champ **Mot de passe**.
7. Sélectionnez le bouton **Appliquer**.
8. Répétez les étapes, de l'[étape 4](#) à l'[étape 7](#) pour ajouter jusqu'à huit membres.

Les noms de châssis des nouveaux membres s'affichent dans la boîte de dialogue libellée **Membres**.

L'état du nouveau membre s'affiche lorsque le groupe est sélectionné dans l'arborescence. Cliquez sur l'image du châssis ou sur le bouton **Détails** pour afficher des détails.

 **REMARQUE** : lorsqu'elles sont saisies, les références d'un membre sont transmises de manière sécuritaire au châssis membre afin d'établir une relation de confiance entre le membre et le châssis chef. Les références ne restent sur aucun des châssis et ne sont plus échangées après l'établissement initial de la relation de confiance.

Retrait d'un membre du châssis chef

Vous pouvez supprimer un membre du groupe du châssis chef. Pour supprimer un membre :

1. Connectez-vous au châssis chef à l'aide des privilèges administrateur.
2. Sélectionnez le châssis chef 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 chef communique au membre ou aux membres sélectionnés qu'ils ont été supprimés du groupe. Le nom du membre est supprimé de la boîte de dialogue. Le châssis membre ne pourra pas recevoir le message si un problème de réseau empêche la communication entre le chef et le membre. Dans ce cas, désactivez le membre depuis le châssis membre pour terminer le processus de retrait. Voir la sous-section « Désactivation d'un membre individuel depuis le châssis membre » pour la procédure.

Dissolution d'un groupe du châssis

Il est également possible de dissoudre complètement un groupe depuis le châssis chef. Pour ce faire :

1. Connectez-vous au châssis chef à l'aide des privilèges administrateur.
2. Sélectionnez le châssis chef dans l'arborescence.
3. Cliquez sur **Configuration** → **Administration des groupes**.
4. Dans la page du groupe du châssis, sous **Rôle**, sélectionnez **Aucun**, puis cliquez sur **Appliquer**.

Le châssis chef communique alors avec tous les membres qui ont été supprimés pour leur faire savoir qu'ils ont été supprimés du groupe. Enfin, le châssis chef ne tient plus ce rôle. Il peut maintenant être affecté en tant que membre ou chef d'un autre groupe.

Le châssis membre ne pourra pas recevoir le message si un problème de réseau empêche la communication entre le chef et le membre. Dans ce cas, désactivez le membre depuis le châssis membre pour terminer le processus de retrait. Voir la sous-section « Désactivation d'un membre individuel depuis le châssis membre » pour la procédure.

Désactivation d'un membre individuel depuis le châssis membre

Il arrive qu'un membre ne puisse pas être supprimé d'un groupe par le châssis chef. Cela peut se produire si la connectivité réseau du membre est perdue. Un membre peut être supprimé d'un groupe depuis le châssis membre :

1. Connectez-vous au châssis membre à l'aide des privilèges administrateur.
2. Cliquez sur **Configuration** → **Administration des groupes**.
3. Sélectionnez **Aucun**, puis cliquez sur **Appliquer**.

Résumé des composants du châssis

Graphiques du châssis

Le châssis est représenté par les vues avant et arrière (image supérieure et image inférieure, respectivement). Les serveurs et l'écran LCD sont affichés dans la vue avant et les autres composants sont affichés dans la vue arrière. La sélection des composants est indiquée par une dominante bleue et est contrôlée en cliquant sur l'image du composant requis. Quand un composant est présent dans le châssis, une icône de ce type de composant est affichée dans le graphique du logement où le composant a été installé. Les logements vides sont affichés sur un fond gris anthracite. L'icône du composant indique visuellement l'état du composant. L'icône de serveur est utilisée au Tableau 5-1 comme exemple. D'autres composants affichent des icônes qui représentent visuellement le composant physique. Les icônes de serveurs et de modules d'E/S s'étendent sur plusieurs logements lorsqu'un élément de taille double est installé. En survolant un composant, vous afficherez une info-bulle avec plus d'informations sur ce composant.

Tableau 5-1. États d'icône 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.
	Aucun serveur présent.

Les Liens rapides du châssis sont affichés sous les graphiques du châssis.

Tableau 5-2. Liens rapides du châssis

Champ	Description
Configurer les utilisateurs	Accédez à Présentation du châssis→ Authentification utilisateur→ Utilisateurs locaux
Configuration du réseau	Accédez à Présentation du châssis→ Réseau→ Réseau
Configuration de l'alimentation	Accédez à Présentation du châssis→ Alimentation→ Configuration
Mise à jour de micrologiciel	Accédez à Présentation du châssis→ Mise à jour→ Mise à jour du micrologiciel

Intégrité du châssis

Lorsque la première page s'affiche, la droite de la page contient des informations au niveau du châssis et des alertes. Toutes les alertes actives critiques et non critiques sont affichées.

En cliquant sur un composant, vous remplacez les informations au niveau du châssis par l'affichage des informations associées au composant sélectionné. Pour restaurer les informations au niveau du châssis, cliquez sur **Retourner à l'intégrité du châssis** dans le coin supérieur droit.

Tableau 5-3. Informations de la page du châssis

Champ	Description
Modèle	Affiche le modèle du panneau LCD du châssis.
Micrologiciel	Affiche la version du micrologiciel du contrôleur CMC actif.
Numéro de service	Affiche le numéro de service du châssis. Le numéro de service est un identifiant unique fourni par le fabricant pour le support et la maintenance.
Numéro d'inventaire	Affiche le numéro d'inventaire du châssis.
Alimentation d'entrée	Alimentation que le châssis consomme actuellement.
Seuil énergétique	Puissance d'entrée maximale définie par l'utilisateur pour la consommation. Lorsque le châssis atteint cette limite, les serveurs ralentissent pour éviter une nouvelle augmentation dans la puissance d'entrée requise.
Stratégie d'alimentation	Préférence définie par l'utilisateur pour la coordination des multiples unités d'alimentation.
Intégrité	Affiche l'intégrité générale du sous-système d'alimentation du châssis.

Informations sur le composant sélectionné

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

1 Intégrité, Performances et Propriétés

Les événements actifs critiques et non critiques tels que ceux figurant dans les journaux de matériel sont affichés ici, le cas échéant. Les données de performances qui peuvent varier avec le temps sont également présentées ici.

1 Propriétés

Les propriétés des composants qui ne varient pas avec le temps ou qui changent rarement sont affichées ici.

1 Liens rapides

La section Liens rapides fournit un moyen commode de navigation pour les pages les plus souvent consultées, ainsi que les actions les plus fréquemment effectuées. Seuls les liens applicables à l'élément sélectionné sont affichés dans cette section.

Tableau 5-4. Informations sur l'intégrité et les performances - Serveurs

Élément	Description
État de l'alimentation	État Sous tension/Hors tension du serveur. Voir Tableau 5-23 pour plus de détails sur les différents types d'états d'alimentation.
Intégrité	Affiche l'équivalent texte de l'icône d'intégrité.
Consommation électrique	Quantité d'énergie que consomme le serveur à l'heure actuelle.
Alimentation allouée	Quantité d'alimentation allouée au serveur.
Température	Température lue par le capteur de température du serveur.

Tableau 5-5. Propriétés du serveur

Élément	Description
Nom	Nom de logement attribué par l'utilisateur.
Modèle	Modèle du serveur, par exemple « PowerEdge M600 » ou « PowerEdge M605 ».
Numéro de service	Le numéro de service du serveur. Le numéro de service est un identifiant unique fourni par le fabricant pour le support et la maintenance. Si le serveur est absent, ce champ est vide.
SE	Système d'exploitation du serveur.
Nom de l'hôte	Nom du serveur, tel qu'établi par le système d'exploitation.
iDRAC	Version du micrologiciel iDRAC sur le serveur.
BIOS	Version du BIOS du serveur.
CPLD	Affiche le numéro de version du circuit logique programmable complexe (CPLD) du serveur.

Tableau 5-6. Liens rapides - Serveurs

Élément	Description
Condition du serveur	Accéder à Présentation des serveurs → <serveur sélectionné> → Propriétés → Condition
Lancez la console distante	Invoque une session clavier-écran-souris sur le serveur si le serveur prend en charge cette opération.
Lancer l'interface utilisateur iDRAC	Invoque une console de gestion iDRAC pour le serveur.
Mettre le serveur sous tension	Appliquer la tension à un serveur qui est hors tension.
Mettre le serveur hors tension	Couper l'alimentation d'un serveur qui est sous tension.
Partage de fichiers à distance	Accéder à Présentation des serveurs → Configuration → Partage de fichiers à distance
Déployer le réseau iDRAC	Accéder à Présentation des serveurs → Configuration → iDRAC (Déployer iDRAC)

Tableau 5-7. Intégrité et performances de module d'E/S

Élément	Description
État de l'alimentation	Affiche l'état de l'alimentation du module d'E/S : sous tension, hors tension ou inconnu (absent).
Rôle	Affiche l'adhésion à l'empilage du module d'E/S lorsque les modules sont reliés. Maître : le module fait partie d'un ensemble de piles. Membre : le module est un point d'accès principal.

Tableau 5-8. Propriétés du module d'E/S

Élément	Description
Modèle	Affiche le nom de produit du module d'E/S.
Numéro de service	Affiche le numéro de service du module d'E/S. Le numéro de service est un identifiant unique fourni par Dell pour le support et la maintenance.

Tableau 5-9. Liens rapides - Modules d'E/S.

Élément	Description
Condition du module d'E/S	Accéder à Modules d'E/S → <module d'E/S sélectionné> → Propriétés → Condition
Lancer l'interface utilisateur du module d'E/S	Si l'icône d'un module d'E/S spécifique est présente, un clic sur cette icône lance la console de gestion de ce module d'E/S dans une nouvelle fenêtre de navigateur ou sous un nouvel onglet.

Tableau 5-10. Intégrité et performances du contrôleur CMC actif

Élément	Description
---------	-------------

Mode de redondance	Affiche le basculement disponible du contrôleur CMC de secours. Si le micrologiciel CMC ne correspond pas ou si CMC n'est pas câblé correctement au réseau de gestion, la redondance apparaît comme non disponible
MAC Address (Adresse Mac)	Affiche l'adresse MAC de l'interface réseau de CMC. L'adresse MAC est un identificateur unique pour CMC sur le réseau.
IPv4	Affiche l'adresse IPv4 de l'interface réseau de CMC.
IPv6	Affiche l'adresse IPv6 de l'interface réseau de CMC.

Tableau 5-11. Propriétés de CMC

Élément	Description
Micrologiciel	Affiche la version du micrologiciel du contrôleur CMC actif.
Micrologiciel :	Affiche la version du micrologiciel CMC installé sur le contrôleur CMC de secours. Si vous n'avez pas installé un deuxième contrôleur CMC, ce champ affiche N/A.
Dernière mise à jour	Indique la date de la dernière mise à jour du micrologiciel. Si aucune mise à jour ne s'est produite, ce champ affiche N/A.
Matériel	Affiche la version matérielle du contrôleur CMC actif.

Tableau 5-12. Liens rapides - CMC

Élément	Description
Condition CMC	Accéder à Contrôleur du châssis → Propriétés → Condition
Mise en réseau	Accéder à Présentation du châssis → Réseau → Réseau
Mise à jour de micrologiciel	Accéder à Présentation du châssis → Mise à jour → Mise à jour du micrologiciel

Tableau 5-13. Intégrité et performances du module iKVM

Élément	Description
Console OSCAR	Indique si le connecteur du panneau arrière VGA est activé (Oui ou Non) pour l'accès à CMC.

Tableau 5-14. Propriétés du module iKVM

Élément	Description
Nom	Affiche le nom iKVM.
Numéro de pièce	Affiche le numéro de pièce d'iKVM. Le numéro de pièce est un identificateur unique fourni par le fournisseur. Les conventions d'attribution des noms des numéros de pièce diffèrent d'un fournisseur à l'autre.
Micrologiciel	Indique la version du micrologiciel iKVM.
Matériel	Indique la version du micrologiciel iKVM.

Tableau 5-15. Liens rapides - iKVM

Élément	Description
Condition iKVM	Accéder à iKVM → Propriétés → Condition
Mise à jour de micrologiciel	Accéder à Présentation du châssis → Mise à jour → Mise à jour du micrologiciel

Tableau 5-16. Intégrité et performances du ventilateur

Élément	Description
Vitesse	Indique la vitesse du ventilateur en tours par minute (tr/min).

Tableau 5-17. Propriétés du ventilateur

Élément	Description
Seuil critique inférieur	Vitesse en dessous de laquelle le ventilateur est considéré comme étant en panne.
Seuil critique supérieur	Vitesse au-dessus de laquelle le ventilateur est considéré comme étant en panne.

Tableau 5-18. Liens rapides - Ventilateur

Élément	Description
Condition du ventilateur	Accéder à Ventilateurs→ Propriétés→ Condition

Tableau 5-19. Intégrité et performances de l'unité d'alimentation

Élément	Description
État de l'alimentation	Indique l'état d'alimentation des blocs d'alimentation (un seul à la fois) : En cours d'initialisation, En ligne, Veille, Test de diagnostic, Échec, Mise à jour, Hors ligne ou Inconnu.

Tableau 5-20. Propriétés de l'unité d'alimentation

Élément	Description
Capacité	Affiche la capacité de l'unité d'alimentation (en watts).

Tableau 5-21. Liens rapides - Unité d'alimentation

Élément	Description
État du bloc d'alimentation	Accéder à Blocs d'alimentation→ Propriétés→ Condition
Consommation électrique	Accéder à Présentation du châssis→ Alimentation→ Consommation électrique
Bilan de puissance du système	Accéder à Présentation du châssis→ Alimentation→ Condition du bilan de puissance

Tableau 5-22. Intégrité et performances du panneau LCD

Élément	Description
Condition du panneau LCD	Affiche la présence et la condition du panneau LCD.
Intégrité du châssis	Affiche la description texte de l'intégrité du châssis.

Il n'existe aucun lien rapide pour le panneau LCD.

Surveillance de la condition d'intégrité du système

Affichage des résumés relatifs au châssis et aux composants

La page de CMC **Intégrité du châssis** contient une représentation graphique du châssis, fournissant une présentation visuelle des composants installés. La page **Intégrité du châssis** est mise à jour de manière dynamique. Les couleurs du sous-graphique des composants et les champs textuels sont automatiquement modifiés.

Figure 5-1. Exemple de graphiques du châssis dans l'interface Web



La page **Intégrité du châssis** fournit une condition générale de l'intégrité du châssis, des modules CMC principal et de secours, des modules de serveur, des modules d'E/S, des ventilateurs, du module iKVM, des blocs d'alimentation et du panneau LCD. Des informations plus détaillées sur chaque composant s'affichent en cliquant sur le composant. Pour des instructions sur l'affichage des résumés du châssis et de ses composants, voir [Affichage des résumés du châssis](#).

Affichage de la condition du bilan de puissance

La page **Condition du bilan de puissance** affiche la condition du bilan de puissance pour le châssis, les serveurs et les unités d'alimentation du châssis.

Pour des instructions sur l'affichage de la condition du bilan de puissance, voir [Affichage de l'état de la consommation de puissance](#). Pour plus d'informations sur la gestion de l'alimentation de CMC, voir [Gestion de l'alimentation](#).

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

Le nom du modèle et le numéro de service de chaque serveur peuvent être obtenus instantanément en procédant comme suit :

- 1 Extension des serveurs dans l'arborescence du système. Tous les serveurs (1 à 16) s'affichent dans la liste développée Serveurs. Le nom de logement sans serveur est estompé.
- 1 Le passage du curseur sur le nom du logement ou du numéro de logement d'un serveur fait apparaître une info-bulle avec le nom du modèle du serveur et le numéro de service (si disponible).

Affichage de la condition d'intégrité de l'ensemble des serveurs

Vous pouvez consulter la condition d'intégrité de tous les serveurs depuis la section **Graphiques du châssis** de la page **Intégrité du châssis** ou **Condition des serveurs**.

La page **Graphiques du châssis** fournit un aperçu graphique de tous les serveurs installés dans le châssis.

Pour consulter la condition d'intégrité des serveurs à l'aide des graphiques du châssis :

1. Ouvrez une session sur l'interface Web de CMC.

La page **Intégrité du châssis** s'affiche. La section située au centre de la page **Graphiques du châssis** représente une vue de face du châssis et contient la condition d'intégrité de tous les serveurs. La condition d'intégrité du serveur est indiquée par la couleur du sous-graphique du serveur :

- 1 Aucune couleur : le composant est présent, sous tension et communique avec le contrôleur CMC. Il n'existe aucune indication d'événement indésirable.
- 1 Panneau orange : indique que seules des alertes sont émises et que des mesures correctives doivent être prises.
- 1 Croix rouge : indique qu'au moins une condition de panne est présente. Cela signifie que CMC peut toujours communiquer avec le composant et que la condition d'intégrité signalée est critique.
- 1 Grisé : indique que le composant est présent et n'est pas sous tension. Il ne communique pas avec CMC et il n'y a aucune indication d'événement indésirable.

La page **Condition des serveurs** fournit un aperçu des serveurs du châssis. Pour afficher la condition d'intégrité de tous les serveurs en utilisant la page **Condition des serveurs** :

1. Ouvrez une session sur l'interface Web de CMC.
2. Cliquez sur **Présentation des serveurs** dans l'arborescence. La page **État des serveurs** s'affiche.

Tableau 5-23. Informations relatives à la condition de l'ensemble des serveurs

--	--

Élément	Description	
Ordre de priorité	Affiche l'emplacement du serveur. Le numéro de logement est un numéro séquentiel qui identifie le serveur en fonction de son emplacement dans le châssis.	
Nom	Indique le nom du serveur, qui est par défaut désigné par le nom de son logement (SLOT01 à SLOT-16). REMARQUE : vous pouvez changer le nom du serveur par défaut. Pour des instructions, voir Modification du nom d'un logement .	
Modèle	Affiche le nom du modèle du serveur. Si ce champ est vide, le serveur n'est pas présent. Si ce champ affiche Extension de n° (où la valeur de n° est comprise entre 1 et 8), le n° correspond au logement principal d'un serveur à plusieurs logements.	
Intégrité	 OK	Indique que le serveur est présent et qu'il communique avec CMC. En cas de perte de la communication entre CMC et le serveur, CMC ne pourra pas obtenir ni afficher la condition d'intégrité du serveur.
	 Informatif	Affiche des informations sur les serveurs en l'absence de modification de l'état de l'intégrité (OK, Avertissement, Critique).
	 Avertissement	Indique que des alertes d'avertissement seules ont été émises et que <i>des actions correctives doivent être effectuées</i> . Si aucune action corrective n'est effectuée, des pannes critiques susceptibles d'affecter l'intégrité du serveur peuvent se produire.
	 Critique	Indique qu'au moins une alerte de panne a été générée. La condition Critique représente une panne système du serveur et des <i>actions correctives doivent être effectuées immédiatement</i> .
	Aucune valeur	Lorsque le serveur est absent du logement, les informations d'intégrité ne sont pas fournies.
Lancez la console distante	<p>Cliquez ici pour lancer une session clavier-écran-souris sur le serveur dans une nouvelle fenêtre ou un nouvel onglet. Cette icône n'est affichée pour un serveur que si toutes les conditions suivantes sont remplies :</p> <ul style="list-style-type: none"> 1 Le serveur est PowerEdge M610, M610X, M710, M710HD ou M910. 1 Le châssis est sous tension. 1 L'interface de réseau local sur le serveur est activée. 1 La version d'iDRAC est 2.20 ou ultérieure. <p>Cette fonctionnalité s'exécute correctement si les conditions suivantes sont remplies :</p> <ul style="list-style-type: none"> 1 Le système hôte dispose du JRE (Java Runtime Environment) 6 Update 16 ou ultérieur. 1 Le navigateur sur le système hôte autorise les fenêtres contextuelles (le blocage des fenêtres contextuelles est désactivé). 	
Lancer l'interface utilisateur iDRAC	<p>Cliquez-gauche sur l'icône pour lancer la console de gestion iDRAC pour un serveur dans une nouvelle fenêtre ou un nouvel onglet du navigateur. Cette icône n'est affichée pour un serveur que si toutes les conditions suivantes sont remplies :</p> <ul style="list-style-type: none"> 1 Le serveur est présent. 1 Le châssis est sous tension. 1 L'interface de réseau local sur le serveur est activée. <p>Cette fonctionnalité fonctionne correctement si la condition suivante est remplie :</p> <ul style="list-style-type: none"> 1 Le navigateur sur le système hôte autorise les fenêtres contextuelles (le blocage des fenêtres contextuelles est désactivé). <p>REMARQUE : si le serveur est retiré du châssis, l'adresse IP d'iDRAC est modifiée ou s'il existe un problème de connexion de réseau sur iDRAC, un clic sur l'icône Lancer l'interface utilisateur iDRAC risque d'afficher une page d'erreur sur l'interface de réseau local d'iDRAC.</p>	
État de l'alimentation	<p>Affiche l'état d'alimentation du serveur :</p> <ul style="list-style-type: none"> 1 - : CMC n'a pas encore déterminé l'état d'alimentation du serveur. 1 Désactivé : le serveur ou le châssis est hors tension. 1 Activé : le châssis et le serveur sont sous tension. 1 Activation : état temporaire entre le mode Désactivé et Activé. Lorsque l'action est terminée, l'État d'alimentation est activé. 1 Mise hors tension : état temporaire entre le mode Activé et Désactivé. Lorsque l'action est terminée, l'État d'alimentation est désactivé. 	
Numéro de service	Affiche le numéro de service du serveur. Le numéro de service est un identifiant unique fourni par le fabricant pour le support et la maintenance. Si le serveur est absent, ce champ est vide.	

Pour des informations sur la procédure de lancement de la console de gestion iDRAC et les stratégies de signature unique, voir [Lancement d'iDRAC en utilisant une signature unique](#).

Modification du nom d'un logement

La page **Noms des logements** vous permet de mettre à jour les noms des logements du châssis. Les noms de logements sont utilisés pour identifier des serveurs individuels. Pour le choix des noms de logements, les règles suivantes s'appliquent :

- 1 Les noms peuvent contenir un **maximum de 15 caractères ASCII non étendus** (codes ASCII de 32 à 126).
- 1 Les noms de logements doivent être uniques au sein d'un châssis. Le nom de chaque logement doit être unique.
- 1 Les chaînes de caractères ne sont pas sensibles à la casse. *Serveur-1*, *serveur-1* et *SERVEUR-1* sont des noms équivalents.
- 1 Les noms de logements ne doivent pas commencer par les chaînes de caractères suivantes :

- 1 Switch-
- 1 Fan-
- 1 PS-
- 1 KVM (clavier/écran/souris)
- 1 DRAC-
- 1 MC-
- 1 Châssis
- 1 Housing-Left
- 1 Housing-Right
- 1 Housing-Center

- 1 Les chaînes de caractères *Server-1* à *Server-16* peuvent être utilisées, mais uniquement pour le logement correspondant. Par exemple, *Server-3* est un nom valide pour le logement 3 mais pas pour le logement 4. Il convient de noter que *Server-03* est un nom valide pour n'importe quel logement.

- REMARQUE : pour modifier le nom du logement, vous devez avoir le privilège d'**Administrateur de configuration du châssis**.
- REMARQUE : la configuration du nom du logement dans l'interface Web réside uniquement sur CMC. Si un serveur est retiré du châssis, le paramètre du nom du logement ne s'applique plus au serveur.
- REMARQUE : le paramètre du nom du logement n'est pas étendu au module iKVM optionnel. Les informations du nom du logement sont disponibles via l'unité remplaçable sur site du module iKVM.
- REMARQUE : la configuration du nom d'un logement dans l'interface Web CMC supprime toujours les modifications apportées au nom d'affichage dans l'interface iDRAC.

Pour modifier le nom d'un logement :

1. Ouvrez une session sur l'interface Web de CMC.
2. Sélectionnez **Présentation des serveurs** dans le menu **Châssis** de l'arborescence du système.
3. Cliquez sur **Configuration** → **Noms des logements**. La page **Noms des logements** s'affiche.
4. Entrez le nom modifié ou le nouveau nom d'un logement dans le champ **Nom de logement**. Répétez cette action pour chaque logement que vous souhaitez renommer.
5. Cliquez sur **Appliquer**.
6. Pour restaurer le nom du logement par défaut (de **SLOT-01** à **SLOT-16**, basé sur la place du logement du serveur) sur le serveur, appuyez sur **Restaurer la valeur par défaut**.

Utilisation du nom d'hôte du serveur comme nom de logement

La page **Noms des logements** permet de remplacer les noms de logements statiques par le nom d'hôte du serveur (ou nom du système), si disponible. Pour ce faire, l'agent OMSA doit être installé sur le serveur. Consultez le *Guide utilisateur de Dell OpenManage Server Administrator* pour plus de détails sur l'agent OMSA.

Pour utiliser le nom d'hôte du serveur en tant que nom de logement :

1. Ouvrez une session sur l'interface Web de CMC.
2. Sélectionnez **Présentation des serveurs** dans le menu **Châssis** de l'arborescence du système.
3. Cliquez sur **Configuration** → **Noms des logements**. La page **Noms des logements** s'affiche.
4. Cochez la case **Utiliser le nom d'hôte comme nom de logement**.
5. Cliquez sur **Appliquer**.

Définition du premier périphérique d'amorçage pour les serveurs

La page **Périphérique de démarrage initial** vous permet de spécifier le périphérique d'amorçage de chaque serveur. Il est possible qu'il ne s'agisse pas du périphérique d'amorçage initial réel du serveur ou même d'un périphérique présent dans ce serveur, mais il est utilisé par CMC en tant que périphérique d'amorçage initial associé à ce serveur.

Vous pouvez définir le périphérique d'amorçage par défaut, mais aussi indiquer un périphérique d'amorçage qui ne sera utilisé qu'une seule fois pour démarrer le système à partir d'une image spécifique. Cette image peut vous permettre, par exemple, d'effectuer des tâches telles que l'exécution de diagnostics, la réinstallation d'un système d'exploitation, etc.

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

Tableau 5-24. 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	Permet de démarrer à partir du lecteur de disquette virtuel. Le lecteur de disquette (ou l'image d'une disquette) se trouve sur un autre ordinateur du réseau de gestion et est connecté à l'aide du visualiseur de console de l'interface utilisateur iDRAC.
CD/DVD virtuel	Permet de démarrer à partir d'un lecteur de CD/DVD virtuel ou d'une image ISO sur CD/DVD. Le lecteur optique ou le fichier de l'image ISO se trouve sur un autre ordinateur ou un autre disque disponible sur le réseau de gestion et est connecté à l'aide du visualiseur de console de l'interface utilisateur iDRAC.
iSCSI	Permet de démarrer à partir d'un périphérique Internet SCSI (interface système pour micro-ordinateur).
Carte SD locale	Démarrage à partir de la carte SD locale : pour les systèmes M610/M710/M805/M905 uniquement.
Disquette	Démarrage à partir d'une disquette insérée dans le lecteur local de disquette.

 **REMARQUE** : pour définir le premier périphérique d'amorçage pour les serveurs, vous devez avoir des privilèges d'administrateur du serveur ou des privilèges d'administrateur de configuration du châssis et des privilèges de connexion iDRAC.

Pour définir le premier périphérique d'amorçage pour certains serveurs ou pour tous les serveurs du châssis :

1. Ouvrez une session sur l'interface Web de CMC.
2. Cliquez sur **Présentation des serveurs** dans l'arborescence, puis sur **Configuration** → **Déployer le premier périphérique d'amorçage**. Une liste de serveurs s'affiche, un serveur par ligne.
3. Sélectionnez le périphérique d'amorçage que vous souhaitez utiliser pour chaque serveur.
4. Si vous voulez que le serveur démarre à partir du périphérique sélectionné à chaque amorçage, décochez la case **Démarrer une fois** correspondant à ce serveur.

Si vous souhaitez que le serveur démarre à partir du périphérique sélectionné au prochain démarrage uniquement, cochez la case **Démarrer une fois** correspondant à ce serveur.
5. Cliquez sur **Appliquer**.

Affichage de la condition d'intégrité d'un serveur spécifique

Vous pouvez consulter la condition d'intégrité d'un serveur de deux manières : à partir de la section **Graphiques du châssis** sur la page **Intégrité du châssis** ou sur la page **Condition du serveur**.

La page **Intégrité du châssis** fournit une représentation graphique d'un serveur spécifique installé dans le châssis.

Pour consulter la condition d'intégrité des serveurs à l'aide des graphiques du châssis :

1. Ouvrez une session sur l'interface Web de CMC.

La page **Intégrité du châssis** s'affiche. La section située au centre de la page **Graphiques du châssis** représente une vue de face du châssis et contient la condition d'intégrité de tous les serveurs. La condition d'intégrité du serveur est indiquée par la couleur du sous-graphique du serveur :

1. Aucune couleur : le serveur est présent, sous tension et communique avec CMC, aucune indication d'événement indésirable.
1. Panneau orange : indique que seules des alertes sont émises et que des mesures correctives doivent être prises.
1. Croix rouge : indique qu'au moins une condition de panne est présente. Cela signifie que CMC peut toujours communiquer avec le composant et que la condition d'intégrité signalée est critique.
1. Grisé : indique que le composant est présent et n'est pas sous tension. Il ne communique pas avec CMC et il n'y a aucune indication d'événement indésirable.

2. Déplacez le curseur pour parcourir un sous-graphique de serveur individuel.

Une astuce textuelle correspondante est affichée. Le champ textuel fournit des informations complémentaires sur ce serveur.

3. Cliquez sur le sous-graphique du serveur pour sélectionner les informations du serveur et afficher les Liens rapides sur la droite des graphiques du châssis.

La page **Condition du serveur** (à ne pas confondre avec la page **Condition des serveurs**) fournit un aperçu du serveur et un point de lancement d'iDRAC (micrologiciel utilisé pour gérer le serveur) vers l'interface Web.

 **REMARQUE** : vous devez posséder un nom d'utilisateur et un mot de passe iDRAC pour utiliser l'interface utilisateur iDRAC. Pour plus d'informations sur iDRAC et l'utilisation de l'interface Web iDRAC, consultez le *Guide d'utilisation du micrologiciel Integrated Dell Remote Access Controller*.

Pour afficher la condition d'intégrité d'un serveur spécifique :

1. Ouvrez une session sur l'interface Web de CMC.
2. Développez **Présentation des serveurs** dans l'arborescence. Tous les serveurs (1 à 16) s'affichent dans la liste développée **Serveurs**.
3. Cliquez sur le (logement de) serveur que vous souhaitez afficher. La page **Condition du serveur** s'affiche.

Vous pouvez également consulter la page d'état du serveur en cliquant sur le lien d'état dans les liens rapides du serveur sur le côté droit de la page.

Tableau 5-25. Condition d'un serveur spécifique : Propriétés

Élément	Description		
Ordre de priorité	Indique le logement occupé par le serveur du châssis. Les numéros de logement sont des ID séquentiels, qui vont de 1 à 16 (16 logements sont disponibles dans le châssis) et qui permettent d'identifier l'emplacement du serveur dans le châssis.		
Nom de logement	Indique le nom du logement où réside le serveur.		
Présent	Indique si le serveur est présent dans le logement (Oui ou Non). Lorsque le serveur est absent, l'intégrité, l'état de l'alimentation et le numéro de service du serveur sont inconnus (ne s'affichent pas).		
Intégrité		OK	Indique que le serveur est présent et qu'il communique avec CMC. En cas de perte de la communication entre CMC et le serveur, CMC ne pourra pas obtenir ni afficher la condition d'intégrité du serveur.
		Informatif	Affiche des informations sur les serveurs en l'absence de modification de l'état de l'intégrité (OK, Avertissement, Critique).
		Avertissement	Indique que des alertes d'avertissement seules ont été émises et que <i>des actions correctives doivent être effectuées</i> . Si aucune action corrective n'est effectuée, des pannes critiques susceptibles d'affecter l'intégrité du serveur peuvent se produire.
		Critique	Indique qu'au moins une alerte de panne a été générée. La condition Critique représente une panne système du serveur et <i>des actions correctives doivent être effectuées immédiatement</i> .
	Aucune valeur	Lorsque le serveur est absent du logement, les informations d'intégrité ne sont pas fournies.	
Modèle du serveur	Indique le modèle du serveur qui se trouve dans le châssis. Exemples : PowerEdge M600, PowerEdge M605.		
Numéro de service	Affiche le numéro de service du serveur. Le numéro de service est un identifiant unique fourni par le fabricant pour le support et la maintenance. Si le serveur est absent, ce champ est vide.		
Micrologiciel iDRAC	Indique la version d'iDRAC actuellement installée sur le serveur.		
Version du CPLD	Affiche le numéro de version du circuit logique programmable complexe (CPLD) du serveur.		
Version du BIOS	Indique la version du BIOS qui se trouve sur le serveur.		
Système d'exploitation	Indique le système d'exploitation installé sur le serveur.		

Tableau 5-26. Condition du serveur : journal des événements système iDRAC

Élément	Description	
Sévérité	OK	Indique un événement normal qui ne nécessite pas d'actions correctives.

		
	Informatif	Indique une entrée informative relative à un événement pour lequel la condition Gravité n'a pas été modifiée.
	Inconnu	Indique un événement inconnu/non classifié.
	Avertissement	Indique un événement non critique pour lequel des actions correctives doivent être effectuées rapidement pour éviter les pannes système.
	Critique	Indique un événement critique nécessitant des actions correctives immédiates pour éviter les pannes système.
Date/Heure	Indique la date et l'heure exactes auxquelles l'événement s'est produit (par exemple, en anglais Wed May 02 16:26:55 2007).	
Description	Fournit une brève description de l'événement.	

Tableau 5-27. Condition du serveur spécifique : paramètres réseau d'iDRAC

Élément	Description
Activé sur le LAN	Indique si le canal de réseau local est activé (Oui) ou désactivé (Non).

Tableau 5-28. Condition du serveur : paramètres réseau iDRAC IPv4

Élément	Description
Activé	Indique si le protocole IPv4 est utilisé sur le réseau local (Oui). Si le serveur ne prend pas en charge IPv6, le protocole IPv4 est toujours activé et ce paramètre n'est pas affiché.
DHCP activé	Indique si le protocole DHCP (Dynamic Host Configuration Protocol) est activé (Oui) ou désactivé (Non). Si cette option est activée (Oui), le serveur récupère automatiquement la configuration IP (adresse IP, masque de sous-réseau et passerelle) auprès d'un serveur DHCP de votre réseau. Le serveur utilise toujours une adresse IP unique allouée sur votre réseau.
IPMI sur le réseau local activé	Indique si le canal réseau local IPMI est activé (Oui) ou désactivé (Non).
Adresse IP	Indique l'adresse IP de l'interface réseau d'iDRAC.
Masque de sous-réseau	Indique le masque de sous-réseau de l'interface réseau d'iDRAC.
Passerelle	Indique la passerelle de l'interface réseau d'iDRAC.

Tableau 5-29. Condition du serveur : paramètres réseau iDRAC IPv6

Élément	Description
Activé	Indique si le protocole IPv6 est utilisé sur le réseau local (Oui).
Configuration automatique activée	Indique si la configuration automatique pour IPv6 est activée (Oui). Si la configuration automatique est activée, le serveur récupère automatiquement la configuration IPv6 (Adresse IPv6, Longueur du préfixe et Passerelle IPv6) auprès d'un routeur IPv6 de votre réseau. Le serveur disposera toujours d'une adresse IPv6 unique sur votre réseau et pourra avoir jusqu'à 16 adresses IPv6.
Adresse locale de liaison	Adresse IPv6 assignée à CMC d'après l'adresse MAC de CMC.
Passerelle	Affiche la passerelle IPv6 de l'interface réseau d'iDRAC.
Adresse IPv6	Affiche une adresse IPv6 pour l'interface réseau iDRAC. Ces adresses peuvent être au nombre de 16 au maximum. La longueur du préfixe, si elle est différente de zéro, est indiquée après une barre oblique (« / »).

Tableau 5-30. Condition d'un serveur spécifique : adresse WWN/MAC

--	--

Élément	Description
Ordre de priorité	Indique le ou les logements occupés par le serveur du châssis.
Emplacement	Affiche l'emplacement occupé par les modules d'entrée/sortie. Les six emplacements sont identifiés par une combinaison du nom du groupe (A, B ou C) et le numéro de logement (1 ou 2). Les noms de logement sont les suivants : A1, A2, B1, B2, C1 et C2.
Structure	Affiche le type de structure d'E/S.
Attribuée par le serveur	Affiche les adresses WWN/MAC attribuées par le serveur qui sont incorporées au matériel du contrôleur. Les adresses WWN/MAC affichant « - » indiquent que l'interface d'une structure spécifique n'a pas été installée.
Attribuée par le châssis	Affiche les adresses WWN/MAC attribuées par le châssis qui sont utilisées pour ce logement particulier. Les adresses WWN/MAC affichant « - » indiquent que la fonctionnalité FlexAddress n'a pas été installée. REMARQUE : une coche verte dans la colonne Attribuée par le serveur ou dans la colonne Attribuée par le châssis indique le type de adresses actives. REMARQUE : lorsque FlexAddress est activé, les logements sans serveurs installés affichent l'attribution MAC/WWN attribuée par le châssis pour les contrôleurs Ethernet incorporés (Structure A). Les adresses attribuées par le châssis pour les structures B et C affichent « - », à moins que ces structures soient en cours d'utilisation sur des serveurs dans les logements occupés. On assume que les mêmes types de structure seront déployés dans les logements inoccupés.

Pour des informations sur la procédure de lancement de la console de gestion iDRAC et les stratégies de signature unique, voir [Lancement d'iDRAC en utilisant une signature unique](#).

Affichage de la condition d'intégrité des modules d'E/S

Vous pouvez consulter la condition d'intégrité des modules d'E/S de deux manières : à partir de la section **Résumé des composants du châssis** sur la page **Intégrité du châssis** ou sur la page **Condition des modules d'E/S**. La page **Intégrité du châssis** fournit une représentation graphique des modules d'E/S installés dans le châssis.

Pour consulter la condition d'intégrité des modules d'E/S à l'aide des graphiques du châssis :

1. Ouvrez une session sur l'interface Web de CMC.

La page **Intégrité du châssis** s'affiche. La section située au centre de la page **Graphiques du châssis** représente une vue de face du châssis et contient la condition d'intégrité des modules d'E/S. La condition d'intégrité des modules d'E/S est indiquée par la couleur du sous-graphique des modules d'E/S :

1. Aucune couleur : le composant est présent, sous tension et communique avec le contrôleur CMC. Il n'existe aucune indication d'événement indésirable.
1. Panneau orange : indique que seules des alertes sont émises et que des mesures correctives doivent être prises.
1. Croix rouge : indique qu'au moins une condition de panne est présente. Cela signifie que CMC peut toujours communiquer avec le composant et que la condition d'intégrité signalée est critique.
1. Grisé : indique que le module est présent et n'est pas sous tension. Il ne communique pas avec CMC et il n'y a aucune indication d'événement indésirable.

2. Déplacez le curseur pour parcourir un sous-graphique du module d'E/S individuel.

Une astuce textuelle correspondante est affichée. Le champ textuel fournit des informations complémentaires sur le module d'E/S.

3. En cliquant sur le sous-graphique du module d'E/S, vous sélectionnez les informations du module d'E/S et ses Liens rapides pour les afficher à droite des graphiques du châssis.

La page **Condition des modules d'E/S** présente l'ensemble des modules d'E/S associés au châssis. Pour des instructions sur l'affichage de l'intégrité des modules d'E/S via l'interface Web ou RACADM, voir [Surveillance de l'intégrité des modules d'E/S](#).

Affichage de la condition d'intégrité des ventilateurs

 **REMARQUE** : lorsqu'une mise à jour du micrologiciel d'un contrôleur CMC ou d'un module iDRAC est en cours sur un serveur, une partie ou l'ensemble des unités de ventilation du châssis fonctionne à 100 %. Ce comportement est normal.

Vous pouvez consulter la condition d'intégrité des modules d'E/S de deux manières : à partir de la section **Résumé des composants du châssis** sur la page **Intégrité du châssis** ou sur la page **Condition des ventilateurs**. La page **Intégrité du châssis** fournit une représentation graphique de tous les ventilateurs installés dans le châssis.

Pour consulter la condition d'intégrité des ventilateurs à l'aide des **graphiques du châssis** :

1. Ouvrez une session sur l'interface Web de CMC.

La page **Intégrité du châssis** s'affiche. La section située au centre de la page **Graphiques du châssis** représente une vue arrière du châssis et contient la condition d'intégrité des modules d'E/S. La condition d'intégrité du ventilateur est indiquée par la couleur du sous-graphique du ventilateur :

- 1 Aucune couleur : le ventilateur est présent et en cours d'exécution ; aucune indication d'événement indésirable.
- 1 Panneau orange : indique que seules des alertes sont émises et que des mesures correctives doivent être prises.
- 1 Croix rouge : indique qu'au moins une condition de panne est présente. Cela signifie que la condition d'intégrité est signalée comme critique.
- 1 Grisé : indique que le ventilateur est présent et n'est pas sous tension. Aucune condition défavorable n'est indiquée.

2. Déplacez le curseur pour survoler un sous-graphique de ventilateur individuel.

Une astuce textuelle correspondante est affichée. Le champ textuel fournit des informations complémentaires sur le ventilateur.

3. En cliquant sur le sous-graphique du module d'E/S, vous sélectionnez les informations du ventilateur et ses Liens rapides pour les afficher à droite des graphiques du châssis.

La page **Condition des ventilateurs** fournit la condition et les mesures de vitesse en tours par minute (tr/min) des ventilateurs du châssis. Celui-ci peut comporter un ou plusieurs ventilateurs.

CMC, qui contrôle les vitesses des ventilateurs, augmente ou diminue automatiquement ces dernières sur la base des événements qui surviennent à l'échelle du système. CMC génère une alerte et augmente les vitesses des ventilateurs lorsque les événements suivants se produisent :

- 1 Le seuil de température ambiante de CMC est dépassé.
- 1 Un ventilateur est défaillant.
- 1 Un ventilateur est retiré du châssis.

Pour afficher la condition d'intégrité des ventilateurs :

1. Ouvrez une session sur l'interface Web de CMC.
2. Sélectionnez **Ventilateurs** dans l'arborescence du système. La page **Condition des ventilateurs** s'affiche.

Vous pouvez également consulter la page **Condition du ventilateur** en cliquant sur le lien d'état dans les liens rapides des informations du ventilateur sur le côté droit de la page.

Tableau 5-31. Informations relatives à la condition d'intégrité des ventilateurs

Élément	Description	
Nom	Affiche le nom du ventilateur au format FAN-n , où <i>n</i> correspond au numéro du ventilateur.	
Présent	Indique si le ventilateur est présent (Oui ou Non).	
Intégrité		OK Indique que l'unité de ventilateur est présente et communique avec CMC. En cas de perte des communications entre CMC et l'unité de ventilateur, CMC ne pourra pas obtenir ni afficher l'état de l'intégrité du ventilateur.
		Critique Indique qu'au moins une alerte de panne a été générée. La condition Critique indique une panne du système au niveau du ventilateur nécessitant une réparation immédiate afin d'éviter toute surchauffe et/ou arrêt du système.
		Inconnu Affiché lorsque le châssis est mis sous tension pour la première fois. En cas de perte des communications entre CMC et l'unité de ventilateur, CMC ne pourra pas obtenir ni afficher l'état de l'intégrité du ventilateur.
Vitesse	Indique la vitesse du ventilateur en tr/min.	

Affichage de la condition d'iKVM

Le module KVM d'accès local destiné à votre châssis de serveur Dell M1000e est appelé Avocent Integrated KVM Switch Module, soit iKVM. La condition d'intégrité d'iKVM associé au châssis peut être consultée sur la page **Intégrité du châssis**.

Pour consulter la condition d'intégrité des ventilateurs à l'aide des **graphiques du châssis** :

1. Ouvrez une session sur l'interface Web de CMC.

La page **Intégrité du châssis** s'affiche. La section située au centre de la page **Graphiques du châssis** représente une vue arrière du châssis et contient la condition d'intégrité du module iKVM. La condition d'intégrité d'iKVM est indiquée par la couleur du sous-graphique d'iKVM :

- 1 Aucune couleur : iKVM est présent, sous tension et communique avec le contrôleur CMC. Il n'existe aucune indication d'événement indésirable.

- 1 Panneau orange : indique que seules des alertes sont émises et que des mesures correctives doivent être prises.
- 1 Croix rouge : indique qu'au moins une condition de panne est présente. Cela signifie que CMC peut toujours communiquer avec iKVM et que la condition d'intégrité signalée est critique.
- 1 Grisé : indique que le module iKVM est présent et n'est pas sous tension. Il ne communique pas avec CMC et il n'y a aucune indication d'événement indésirable.

2. Utilisez le curseur pour survoler le sous-graphique iKVM.

Une astuce textuelle correspondante est affichée. Le texte du champ fournit des informations complémentaires sur cet iKVM.

3. En cliquant sur le sous-graphique d'iKVM, vous sélectionnez les informations du ventilateur et ses Liens rapides pour les afficher à droite des graphiques du châssis.

Vous pouvez également consulter la page **Condition d'iKVM** en cliquant sur le lien d'état dans les liens rapides des informations du ventilateur sur le côté droit de la page.

Pour des instructions sur l'affichage de la condition du module iKVM et la définition de ses propriétés, voir :

- 1 [Affichage de la condition et des propriétés d'iKVM](#)
- 1 [Activation ou désactivation du panneau avant](#)
- 1 [Activation de la console Dell CMC via iKVM](#)
- 1 [Mise à jour du micrologiciel du module iKVM](#)

Pour plus d'informations sur iKVM, voir [Utilisation du module iKVM](#).

Affichage de la condition d'intégrité des unités d'alimentation

Vous pouvez consulter la condition d'intégrité des unités d'alimentation de deux manières : à partir de la section **Résumé des composants du châssis** de la page **Intégrité du châssis** ou de la page **Condition du bloc d'alimentation**. La page **Intégrité du châssis** fournit une représentation graphique de toutes les unités d'alimentation installées dans le châssis.

Pour consulter la condition d'intégrité des unités d'alimentation à l'aide des **graphiques du châssis** :

1. Ouvrez une session sur l'interface Web de CMC.

La page **Intégrité du châssis** s'affiche. La section située au bas de la page **Graphiques du châssis** représente une vue arrière du châssis et contient la condition d'intégrité de toutes les unités d'alimentation. L'état d'intégrité des unités d'alimentation est indiqué par la couleur du sous-graphique des unités d'alimentation :

- 1 Aucune couleur : unité d'alimentation est présente, sous tension et communique avec le contrôleur CMC. Il n'existe aucune indication d'événement indésirable.
- 1 Panneau orange : indique que seules des alertes sont émises et que des mesures correctives doivent être prises.
- 1 Croix rouge : indique qu'au moins une condition de panne est présente. Cela signifie que CMC peut toujours communiquer avec l'unité d'alimentation et que la condition d'intégrité signalée est critique.
- 1 Grisé : indique que l'unité d'alimentation est présente et n'est pas sous tension. Il ne communique pas avec CMC et il n'y a aucune indication d'événement indésirable.

2. Placez le curseur sur le sous-graphique d'une unité d'alimentation spécifique pour afficher le champ textuel ou l'info bulle correspondant. Le champ textuel fournit des informations complémentaires sur l'unité d'alimentation.

3. En cliquant sur le sous-graphique de l'unité d'alimentation, vous sélectionnez les informations de celle-ci et ses Liens rapides pour les afficher à droite des graphiques du châssis.

La page **Condition du bloc d'alimentation** affiche la condition et les mesures des unités d'alimentation associées au châssis. Pour plus d'informations sur la gestion de l'alimentation de CMC, voir [Gestion de l'alimentation](#).

Pour afficher la condition d'intégrité des unités d'alimentation :

- 1. Ouvrez une session sur l'interface Web de CMC.
- 2. Sélectionnez **Blocs d'alimentation** dans l'arborescence du système. La page **État du bloc d'alimentation** s'affiche.

Vous pouvez également consulter la page **Condition des unités d'alimentation** en cliquant sur le lien d'état dans les liens rapides des informations du ventilateur sur le côté droit de la page.

Tableau 5-32. Informations relatives à la condition d'intégrité des blocs d'alimentation

--	--

Élément	Description	
Nom		Affiche le nom de l'unité d'alimentation au format <i>PS-n</i> , où <i>n</i> correspond au numéro du bloc d'alimentation.
Présent		Indique si le bloc d'alimentation est présent (oui ou non).
Intégrité	 OK	Indique que l'unité d'alimentation est présente et qu'elle communique avec CMC. Indique que l'intégrité de l'unité d'alimentation est OK. En cas de perte des communications entre CMC et l'unité de ventilateur, CMC ne pourra pas obtenir ni afficher l'état de l'intégrité de l'unité d'alimentation.
	 Critique	Indique que l'unité d'alimentation est en panne et que l'intégrité est critique. Une action corrective doit être effectuée immédiatement. Le non respect de cette consigne peut entraîner l'arrêt du composant en raison d'une panne de courant.
	 Inconnu	Affiché lorsque le châssis est mis sous tension pour la première fois. En cas de perte des communications entre CMC et l'unité d'alimentation, CMC ne pourra pas obtenir ni afficher l'état de l'intégrité de l'unité d'alimentation.
État de l'alimentation		Indique l'état de l'alimentation de l'unité d'alimentation : Connecté , Éteint ou Logement vide .
Capacité		Affiche la capacité d'alimentation en watts.

Tableau 5-33. Condition de la puissance système

Élément	Description
Intégrité globale énergétique	Indique la condition d'intégrité (OK , Non critique , Critique , Non récupérable , Autre , Inconnu) de la gestion de l'alimentation pour tout le châssis.
Condition de la puissance système	Affiche la condition de l'alimentation (Activé, Désactivé, Mis sous tension, Mis hors tension) du châssis.
Redondance	Indique la condition de la redondance des blocs d'alimentation. Les valeurs sont les suivantes : Non : les blocs d'alimentation ne sont pas redondants. Oui : une redondance totale est appliquée.

Affichage de la condition des capteurs de température

La page **Condition des capteurs de température** affiche l'état et les lectures des capteurs de température sur le châssis entier (châssis et serveurs).

 **REMARQUE** : la valeur des capteurs de température ne peut pas être modifiée. Toute modification au-delà du seuil génère une alerte qui affecte la vitesse du ventilateur. Par exemple, si le capteur de température ambiante de CMC excède le seuil, la vitesse des ventilateurs du châssis augmente.

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

1. Ouvrez une session sur l'interface Web de CMC.
2. Sélectionnez **Capteurs de température** dans l'arborescence du système. La page **Condition des capteurs de température** s'affiche.

Tableau 5-34. Informations relatives à la condition d'intégrité des capteurs de température

Élément	Description	
ID		Affiche l'emplacement du capteur de température.
Nom		Affiche le nom de chaque capteur de température pour le châssis et les serveurs.
Présent		Indique si le module est présent (Oui) ou absent (Non) dans le châssis.
Intégrité	 OK	Indique que le module est présent et qu'il communique avec CMC. En cas de perte de la communication entre CMC et le serveur, CMC ne pourra pas obtenir ni afficher la condition d'intégrité du serveur.
	 Avertissement	Indique que des alertes d'avertissement seules ont été émises et que des actions correctives doivent être effectuées. Si aucune action corrective n'est effectuée, des pannes critiques susceptibles d'affecter l'intégrité du serveur peuvent se produire.

	Grave	Indique qu'au moins une alerte de panne a été générée. La condition Critique représente une panne système du module et des actions correctives doivent être effectuées immédiatement.
	Inconnu	Indique que la communication avec le module n'a pas été établie. C'est généralement parce que le châssis est éteint ou qu'il n'a pas terminé l'initialisation.
Lecture	Indique la température actuelle en degrés Celsius et Fahrenheit.	
Seuil maximal	Indique la température la plus élevée, en degrés Celsius et Fahrenheit, à laquelle une alerte de panne est générée.	

Affichage de l'état du panneau LCD

Vous pouvez consulter la condition d'intégrité du panneau LCD en utilisant les graphiques du châssis associés avec le châssis sur la page **Intégrité du châssis**.

Pour afficher la condition d'intégrité du panneau LCD :

1. Ouvrez une session sur l'interface Web de CMC.

La page **Intégrité du châssis** s'affiche. La partie supérieure des graphiques du châssis représente la façade du châssis. La condition d'intégrité de l'écran LCD est indiquée par la couleur du sous-graphique du LCD :

- 1. Aucune couleur : le LCD est présent, sous tension, et communique avec CMC. Aucune indication d'événement indésirable.
- 1. Panneau orange : indique que seules des alertes sont émises et que des mesures correctives doivent être prises.
- 1. Croix rouge : indique qu'au moins une condition de panne est présente. La condition d'intégrité est critique.
- 1. Grisé : indique que le LCD est présent et n'est pas sous tension. Il ne communique pas avec CMC et il n'y a aucune indication d'événement indésirable.

2. Déplacez le curseur sur le sous-graphique du panneau LCD. L'astuce textuelle ou à l'écran correspondante, qui fournit des informations supplémentaires sur le panneau LCD, est affichée.
3. Cliquez sur le sous-graphique LCD pour sélectionner les informations sur le LCD et les afficher sur le côté droit des graphiques du châssis.

Affichage des ID de nom mondial/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 de structure d'entrée/sortie installée dans les structures A, B et C. Une coche verte indique que la structure est activée pour FlexAddress. La fonctionnalité FlexAddress permet le déploiement des adresses WWN/MAC de logement persistantes et attribuées par le châssis, dans plusieurs structures et plusieurs logements de ce dernier. Cette fonctionnalité est activée sur une base par structure et par logement.

 **REMARQUE** : voir [Utilisation de FlexAddress](#) pour plus d'informations sur la fonctionnalité FlexAddress.

Adresses WWN/MAC

La section **Adresse WWN/MAC** affiche les informations des adresses WWN/MAC qui sont attribuées à tous les serveurs, même si les logements de serveurs sont actuellement vides. **Emplacement** : affiche l'emplacement du logement occupé par les modules d'E/S. Les six logements sont identifiés par la combinaison d'un nom de groupe (A, B ou C) et d'un numéro de logement (1 ou 2) : noms des logements A1, A2, B1, B2, C1 ou C2. iDRAC représente le contrôleur de gestion intégré du serveur. **Structure** affiche le type de structure d'E/S. **Attribuée par le serveur** affiche les adresses WWN/MAC attribuées par le serveur et incorporées au matériel du contrôleur. **Attribuée par le châssis** affiche les adresses WWN/MAC attribuées par le châssis à ce logement spécifique. Une coche verte dans la colonne **Attribuée par le serveur** ou **Attribuée par le châssis** indique le type des adresses actives. Les adresses attribuées par le châssis sont attribuées lorsque FlexAddress est activée sur le châssis et représentent les adresses de logement persistantes. Lorsque les adresses attribuées par le châssis sont cochées, elles seront utilisées même si un serveur est remplacé par un autre.

Configuration des propriétés du réseau CMC

 **REMARQUE** : les modifications apportées à la configuration réseau peuvent entraîner la perte de connectivité pendant la session réseau actuelle.

Configuration de l'accès initial à CMC

Avant de pouvoir commencer à configurer CMC, vous devez d'abord configurer les paramètres réseau CMC afin de permettre la gestion à distance de CMC. Cette configuration initiale définit les paramètres de mise en réseau TCP/IP qui permettent l'accès à CMC.

 **REMARQUE** : vous devez disposer de privilèges **Administrateur de configuration du châssis** pour configurer les paramètres réseau CMC.

1. Connectez-vous à l'interface Web.
2. Cliquez sur **Présentation du châssis** dans l'arborescence.
3. Cliquez sur l'onglet **Réseau**. La page **Configuration réseau** s'affiche.
4. Activez ou désactivez DHCP pour CMC en cochant ou en décochant la case **Utiliser DHCP (pour l'adresse IP de l'interface réseau CMC)**.
5. Si vous avez désactivé le protocole DHCP, entrez l'adresse IP, la passerelle et le masque de sous-réseau.
6. Cliquez sur **Appliquer les changements** au bas de la page.

Configuration des paramètres du réseau local

 **REMARQUE** : vous devez disposer de privilèges **Administrateur de configuration du châssis** pour configurer les paramètres réseau CMC.

 **REMARQUE** : les paramètres de la page **Configuration réseau**, tels que la chaîne de communauté et l'adresse IP du serveur SMTP, affectent à la fois CMC et les paramètres externes du châssis.

 **REMARQUE** : si vous disposez de deux modules CMC (principal et de secours) sur le châssis et qu'ils sont tous les deux connectés au réseau, le contrôleur CMC de secours récupère automatiquement les paramètres réseau en cas de défaillance du contrôleur CMC principal.

Pour configurer les paramètres LAN du réseau :

1. Connectez-vous à l'interface Web.
2. Cliquez sur l'onglet **Réseau**.
3. Configurez les paramètres réseau CMC décrits du [Tableau 5-35](#) au [Tableau 5-37](#).
4. Cliquez sur **Appliquer les modifications**.

Pour configurer les paramètres de plage et de blocage IP, cliquez sur le bouton **Paramètres avancés** (voir [Configuration des paramètres de sécurité réseau CMC](#)).

Pour actualiser le contenu de la page **Configuration réseau**, cliquez sur **Actualiser**.

Pour imprimer le contenu de la page **Configuration réseau**, cliquez sur **Imprimer**.

Tableau 5-35. Paramètres réseau

Paramètre	Description
Adresse MAC de CMC	Affiche l'adresse MAC du châssis, qui est un identificateur unique du châssis sur le réseau.
Activer l'interface réseau de CMC	Active l'interface réseau de CMC Par défaut : activé. Si cette option est cochée : <ul style="list-style-type: none">1 CMC est accessible via le réseau d'ordinateurs avec lequel il communique.1 Les interfaces Web, de ligne de commande (RACADM distant), WSMAN, Telnet et SSH associées à CMC sont disponibles. Si cette option n'est pas cochée : <ul style="list-style-type: none">1 L'interface réseau de CMC ne peut pas communiquer sur le réseau.1 La communication avec le châssis via CMC n'est pas disponible.1 Les interfaces Web, de ligne de commande (RACADM distant), WSMAN, Telnet et SSH associées à CMC ne sont pas disponibles.1 L'interface Web iDRAC du serveur, l'interface de ligne de commande locale, les modules d'E/S et iKVM sont toujours accessibles.1 Les adresses réseau d'iDRAC et de CMC peuvent être obtenues dans ce cas à partir de l'écran LCD du châssis. REMARQUE : l'accès aux autres composants du châssis accessibles via le réseau n'est pas affecté en cas de désactivation ou de perte du réseau sur le châssis.

Enregistrer CMC sur DNS	<p>Cette propriété enregistre le nom CMC sur le serveur DNS.</p> <p>Par défaut : Décoché (désactivé)</p> <p>REMARQUE : certains serveurs DNS ne peuvent enregistrer que des noms de 31 caractères maximum. Assurez-vous que le nom désigné respecte la limite DNS.</p>
Nom CMC DNS	<p>Affiche le nom CMC uniquement lorsque l'option Enregistrer CMC sur DNS est sélectionnée. Le nom CMC par défaut est <i>CMC_numéro_de_service</i>, où <i>numéro de service</i> est le numéro de service du châssis, par exemple : CMC-00002. Il peut comporter jusqu'à 63 caractères. Le premier caractère doit être une lettre (a-z, A-Z) et doit être suivi de caractères alphanumériques (a-z, A-Z, 0-9) ou de tirets (-).</p>
Utiliser DHCP pour le nom de domaine DNS	<p>Utilise le nom de domaine DNS par défaut. Cette case est active uniquement lorsque l'option Utiliser DHCP (pour l'adresse IP de l'interface réseau de CMC) est sélectionnée.</p> <p>Par défaut : activé</p>
Nom de domaine DNS	<p>Le nom de domaine DNS par défaut est un caractère vide. Ce champ est modifiable uniquement lorsque la case Utiliser DHCP pour le nom de domaine DNS est cochée.</p>
Négociation automatique (1 Go)	<p>Détermine si CMC définit automatiquement le mode duplex et la vitesse réseau en communiquant avec le routeur ou le commutateur le plus proche (activé) ou vous permet de définir manuellement le mode duplex et la vitesse réseau (désactivé).</p> <p>Par défaut : activé</p> <p>Si la négociation automatique est activée, CMC communique automatiquement avec le routeur ou commutateur le plus proche et fonctionne à une vitesse de 1 Go.</p> <p>Lorsque l'option Négociation automatique est désactivée, vous devez définir manuellement le mode duplex et la vitesse réseau.</p>
Vitesse du réseau	<p>Définissez la vitesse réseau sur 100 Mbits/s ou 10 Mbits/s en fonction de votre environnement réseau.</p> <p>REMARQUE : le paramètre Vitesse réseau doit correspondre à votre configuration réseau afin de garantir l'efficacité du débit du réseau. Si la vitesse réseau que vous paramétrez est inférieure à la vitesse de votre configuration réseau, la consommation de bande passante augmente et les communications réseau ralentissent. Déterminez si votre réseau prend en charge les vitesses réseau ci-dessus et paramétrez-le en conséquence. Si votre configuration réseau ne correspond à aucune de ces valeurs, Dell vous recommande d'utiliser la négociation automatique ou de contacter le fabricant de votre équipement réseau.</p> <p>REMARQUE : pour utiliser les vitesses de 1 000 Mo ou 1 Go, sélectionnez Négociation automatique.</p>
Mode duplex	<p>Définissez le mode duplex sur Total ou Semi en fonction de votre environnement réseau.</p> <p>Conséquences : si l'option Négociation automatique est activée pour un périphérique mais non pour l'autre, alors le périphérique qui utilise la négociation automatique peut déterminer la vitesse réseau de l'autre périphérique, mais non le mode duplex. Dans ce cas, le mode duplex utilisé par défaut pendant la négociation automatique est le mode Semi duplex. Cette différence de mode duplex entraîne un ralentissement des connexions réseau.</p> <p>REMARQUE : les paramètres Vitesse réseau et Mode duplex ne sont pas disponibles si la négociation automatique est activée.</p>
MTU	<p>Définit la taille de l'unité de transmission maximale (MTU) ou le paquet le plus volumineux pouvant être transmis via l'interface.</p> <p>Plage de configuration : 576 à 1 500.</p> <p>Par défaut : 1 500.</p> <p>REMARQUE : IPv6 requiert une MTU minimale de 1 280. Si IPv6 est activé et que <code>cfgNetTuningMtu</code> est défini sur une valeur inférieure, CMC utilisera une MTU de 1 280.</p>

Tableau 5-36. Paramètres IPv4

Paramètre	Description
Activer IPv4	<p>Permet à CMC d'utiliser le protocole IPv4 pour communiquer sur le réseau. Le fait de décocher cette case n'empêche pas la mise en réseau IPv6. Par défaut : coché (activé).</p>
Activation DHCP	<p>Permet à CMC de demander et d'obtenir automatiquement une adresse IP auprès du serveur DHCP (protocole de configuration dynamique des hôtes) IPv4. Par défaut : coché (activé).</p> <p>Si cette option est cochée, CMC récupère automatiquement la configuration IPv4 (adresse IP, masque de sous-réseau et passerelle) auprès d'un serveur DHCP de votre réseau. CMC utilise toujours une adresse IP unique allouée sur votre réseau.</p> <p>REMARQUE : lorsque cette fonctionnalité est activée, les champs des propriétés Adresse IP statique, Masque de sous-réseau statique et Passerelle statique (situés immédiatement après cette option dans la page Configuration réseau) sont désactivés et toutes les valeurs précédemment saisies pour ces propriétés sont ignorées.</p>

	Si cette option n'est pas cochée, vous devez entrer manuellement l'adresse IP statique, le masque de sous-réseau statique et la passerelle statique dans les champs de texte qui suivent immédiatement cette option sur la page Configuration réseau .
Adresse IP statique	Affiche l'adresse IPv4 de l'interface réseau de CMC.
Masque de sous-réseau statique	Spécifie le masque de sous-réseau IPv4 statique de l'interface réseau de CMC.
Passerelle statique	Affiche la passerelle IPv4 de l'interface réseau de CMC. REMARQUE : les champs Adresse IP statique , Masque de sous-réseau statique et Passerelle statique sont actifs uniquement si l'option Activation DHCP (le champ de propriété précédant ces champs) est désactivée (décochée). Dans ce cas, vous devez entrer manuellement l'adresse IP statique, le masque de sous-réseau statique et la passerelle statique pour que CMC puisse les utiliser sur le réseau. REMARQUE : les champs Adresse IP statique , Masque de sous-réseau statique et Passerelle statique s'appliquent uniquement au périphérique du châssis. Ils n'affectent pas les autres composants de la solution du châssis accessibles sur le réseau tels que le réseau du serveur, l'accès local, les modules d'E/S et iKVM.
Utiliser DHCP pour obtenir des adresses de serveur DNS	Obtient les adresses de serveur DNS principales et secondaires du serveur de DHCP au lieu des paramètres statiques. Par défaut : coché (activé) par défaut REMARQUE : si l'option Utiliser DHCP (pour l'adresse IP de l'interface réseau de CMC) est activée, activez la propriété Utiliser DHCP pour obtenir des adresses de serveur DNS . Si cette option est cochée , CMC récupère automatiquement son adresse IP DNS auprès d'un serveur DHCP sur votre réseau. REMARQUE : lorsque cette propriété est activée, les champs de propriété Serveur DNS statique préféré et Autre serveur DNS statique (situés immédiatement après cette option dans la page Configuration réseau) sont désactivés et toutes les valeurs précédemment entrées pour ces propriétés sont ignorées. Si cette option n'est pas sélectionnée, CMC récupère l'adresse IP DNS auprès du serveur DNS statique préféré et du serveur DNS statique alternatif. Les adresses de ces serveurs sont spécifiées dans les champs de texte qui suivent immédiatement cette option sur la page Configuration réseau .
Serveur DNS statique préféré	Spécifie l'adresse IP statique du serveur DNS préféré. Le serveur DNS statique préféré est uniquement mis en œuvre lorsque l'option Utiliser DHCP pour obtenir des adresses de serveur DNS est désactivée.
Autre serveur DNS statique	Spécifie l'adresse IP statique du serveur DNS auxiliaire. L'autre serveur DNS statique est uniquement mis en œuvre lorsque l'option Utiliser DHCP pour obtenir des adresses de serveur DNS est désactivée. Si vous ne disposez pas d'un serveur DNS alternatif, entrez l'adresse IP 0.0.0.0.

Tableau 5-37. Paramètres IPv6

Paramètre	Description
Activer IPv6	Permet à CMC d'utiliser le protocole IPv6 pour communiquer sur le réseau. Le fait de décocher cette case n'empêche pas la mise en œuvre IPv4. Par défaut : coché (activé).
Activation de la configuration automatique	Permet à CMC d'utiliser le protocole IPv6 pour obtenir l'adresse IPv6 et les paramètres de la passerelle auprès d'un routeur IPv6 configuré pour fournir ces informations. CMC dispose alors d'une adresse IPv6 unique sur votre réseau. Par défaut : coché (activé). REMARQUE : lorsque cette fonctionnalité est activée, les champs des propriétés Adresse IPv6 statique , Longueur de préfixe statique et Passerelle statique (situés immédiatement après cette option dans la page Configuration réseau) sont désactivés et toutes les valeurs précédemment saisies pour ces propriétés sont ignorées. Si cette option n'est pas cochée, vous devez taper manuellement l'adresse IPv6 statique, la longueur de préfixe statique et la passerelle statique dans les champs de texte qui suivent immédiatement cette option sur la page Configuration réseau .
Adresse IPv6 statique	Spécifie l'adresse IPv6 de l'interface réseau de CMC lorsque la configuration automatique n'est pas activée.
Longueur de préfixe statique	Spécifie la longueur du préfixe IPv6 de l'interface réseau de CMC lorsque la configuration automatique n'est pas activée.
Passerelle statique	Spécifie la passerelle IPv6 statique de l'interface réseau de CMC lorsque la configuration automatique n'est pas activée. REMARQUE : les champs Adresse IPv6 statique , Longueur de préfixe statique et Passerelle statique sont actifs uniquement si l'option Activation de la configuration automatique (le champ de propriété précédant ces champs) est désactivée (décochée). Dans ce cas, vous devez entrer manuellement l'adresse IPv6 statique, la longueur de préfixe statique et la passerelle statique pour que CMC puisse les utiliser sur le réseau IPv6. REMARQUE : les champs Adresse IPv6 statique , Longueur de préfixe statique et Passerelle statique s'appliquent uniquement au

	périphérique du châssis. Ils n'affectent pas les autres composants de la solution du châssis accessibles sur le réseau tels que le réseau du serveur, l'accès local, les modules d'E/S et iKVM.
Serveur DNS statique préféré	Spécifie l'adresse IPv6 statique du serveur DNS préféré. Le serveur DNS statique préféré est uniquement mis en œuvre lorsque l'option Utiliser DHCP pour obtenir des adresses de serveur DNS est désactivée ou décochée. Les deux zones de configuration IPv4 et IPv6 comportent une entrée pour ce serveur.
Autre serveur DNS statique	Spécifie l'adresse IPv6 statique du serveur DNS alternatif. Si vous ne disposez pas d'un serveur DNS alternatif, saisissez l'adresse IPv6 « :: ». L'entrée du serveur DNS statique alternatif est uniquement prise en compte lorsque l'option Utiliser DHCP pour obtenir des adresses de serveur DNS est désactivée ou décochée. Les deux zones de configuration IPv4 et IPv6 comportent une entrée pour ce serveur.

Configuration des paramètres de sécurité réseau CMC

 **REMARQUE** : pour effectuer les étapes suivantes, vous devez disposer des privilèges **Administrateur de configuration du châssis**.

1. Connectez-vous à l'interface Web.

2. Cliquez sur l'onglet **Réseau**.

La page **Configuration réseau** s'affiche.

3. Cliquez sur le bouton **Paramètres avancés**.

La page **Sécurité réseau** s'affiche.

4. Configurez les paramètres de sécurité réseau CMC.

Le [Tableau 5-38](#) décrit les **paramètres** de la page **Sécurité réseau**.

 **REMARQUE** : les paramètres Plage IP et Blocage IP s'appliquent uniquement à IPv4.

Tableau 5-38. Paramètres de la page Sécurité réseau

Paramètres	Description
Plage IP activée	Active la fonctionnalité de vérification de la plage IP, qui définit une plage d'adresses IP spécifique pouvant accéder à CMC.
Adresse de la plage IP	Détermine l'adresse IP de base pour la vérification de la plage.
Masque de la plage IP	Définit une plage d'adresses IP spécifique pouvant accéder à CMC : ce processus est appelé vérification de la plage IP. La vérification de la plage IP permet uniquement l'accès à CMC à partir des clients ou des stations de gestion dont les adresses IP appartiennent à la plage spécifiée par l'utilisateur. Toutes les autres ouvertures de session sont refusées. Par exemple : Masque de plage IP : 255.255.255.0 (11111111.11111111.11111111.00000000) Adresse de la plage IP : 192.168.0.255 (11000000.10101000.00000000.11111111) La plage d'adresses IP résultante correspond à n'importe quelle adresse contenant 192.168.0, c'est-à-dire toute adresse comprise entre 192.168.0.0 et 192.168.0.255.
Blocage IP activé	Active la fonctionnalité de blocage d'une adresse IP, qui limite le nombre de tentatives de connexion ayant échoué à partir d'une adresse IP spécifique pour une durée présélectionnée.
1 Nombre d'échecs avant blocage IP	Définit le nombre d'échecs de tentatives d'ouverture de session à partir d'une adresse IP avant que les tentatives d'ouverture de session ne soient rejetées à partir de cette adresse.
1 Plage d'échecs avant blocage IP	Détermine la période, en secondes, pendant laquelle doit se produire le nombre d'échecs avant blocage IP pour déclencher la période de pénalité du bloc IP.
1 Période de pénalité avant blocage IP	Période en secondes pendant laquelle les tentatives d'ouverture de session à partir d'une adresse IP avec un nombre d'échecs excessif sont rejetées. REMARQUE : les champs Nombre d'échecs avant blocage d'adresse IP, Plage d'échecs avant blocage d'adresse IP et Période de pénalité avant blocage d'adresse IP sont actifs uniquement si la case Blocage d'adresse IP activé (le champ de propriétés précédant ces champs) est cochée (activée). Dans ce cas, vous devez entrer manuellement les propriétés Nombre d'échecs avant blocage d'adresse IP, Plage d'échecs avant blocage d'adresse IP et Période de pénalité avant blocage d'adresse IP.

5. Cliquez sur **Appliquer** pour enregistrer vos paramètres.

Pour actualiser le contenu de la page **Sécurité réseau**, cliquez sur **Actualiser**.

Pour imprimer le contenu de la page **Sécurité réseau**, cliquez sur **Imprimer**.

Configuration des réseaux locaux virtuels (VLAN)

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

1. Connectez-vous à l'interface Web.
2. Cliquez sur l'onglet **Réseau** → sous-onglet **VLAN**.

La page **Paramètres des numéros VLAN** apparaît. Les numéros VLAN correspondent aux propriétés du châssis. Ils demeurent associés au châssis, même en cas de retrait d'un composant.

3. Configurez les paramètres VLAN CMC/iDRAC.

Le [Tableau 5-39](#) décrit les **paramètres** de la page **Sécurité réseau**.

Tableau 5-39. Paramètres des numéros VLAN

Paramètre	Description
Ordre de priorité	Indique le logement occupé par le serveur du châssis. Les logements sont des ID séquentiels, qui vont de 1 à 16 (pour les 16 logements disponibles dans le châssis), qui permettent d'identifier l'emplacement du serveur dans le châssis.
Nom	Affiche le nom du serveur dans chaque logement.
Activé	Active VLAN si la case est cochée. VLAN est désactivé par défaut.
Priorité	Indique le niveau de priorité de la trame, qui peut être utilisé pour établir la priorité des différents types de trafic (voix, vidéo et données). Les priorités valides sont comprises entre 0 et 7, où 0 (priorité par défaut) correspond à la priorité inférieure et 7 à la priorité supérieure.
ID	Affiche l'ID VLAN (identification). Les ID VLAN valides sont les suivants : 1 à 4 000 et 4 021 à 4 094. L'ID VLAN par défaut est 1.

4. Cliquez sur **Appliquer** pour enregistrer les paramètres.

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

Ajout et configuration d'utilisateurs CMC

Pour gérer votre système avec CMC et maintenir la sécurité du système, créez des utilisateurs uniques et octroyez-leur des droits d'administration spécifiques (ou *autorité basée sur les rôles*). Pour une sécurité supplémentaire, vous pouvez aussi configurer des alertes qui sont envoyées par e-mail à des utilisateurs spécifiques quand un événement système spécifique se produit.

Types d'utilisateurs

Il existe deux types d'utilisateurs : les utilisateurs CMC et les utilisateurs iDRAC. Les utilisateurs CMC sont également appelés « utilisateurs châssis ». Étant donné qu'iDRAC réside sur le serveur, les utilisateurs iDRAC sont également appelés « utilisateurs du serveur ».

Les utilisateurs CMC peuvent être des utilisateurs locaux ou des utilisateurs Active Directory. Les utilisateurs iDRAC peuvent également être des utilisateurs locaux ou Active Directory.

Sauf si un utilisateur CMC possède des privilèges **administrateur de serveur**, les privilèges octroyés à un utilisateur CMC ne sont pas automatiquement transférés à ce même utilisateur sur un serveur car les utilisateurs du serveur sont créés indépendamment des utilisateurs CMC. En d'autres termes, les utilisateurs CMC Active Directory et les utilisateurs iDRAC Active Directory résident sur deux branches différentes de l'arborescence Active Directory. Pour créer un utilisateur local du serveur, l'administrateur de configuration des utilisateurs doit directement ouvrir une session sur le serveur. Les utilisateurs de configuration ne peuvent pas créer un utilisateur de serveur depuis CMC, et vice versa. Cette règle protège la sécurité et l'intégrité des serveurs.

Tableau 5-40. Types d'utilisateurs

Privilège	Description
Ouverture de session utilisateur CMC	L'utilisateur peut se connecter à CMC et afficher toutes les données de CMC, mais ne peut pas ajouter ou modifier des données ou exécuter des commandes. Un utilisateur peut posséder d'autres privilèges sans nécessairement posséder le privilège d'ouverture de session sur CMC. Cette fonctionnalité est utile lorsqu'un utilisateur n'a temporairement plus le droit d'ouvrir une session. Lorsque le privilège

	d'ouverture de session sur CMC de cet utilisateur est rétabli, l'utilisateur conserve tous les autres privilèges précédemment octroyés.
Administrateur de configuration du châssis	<p>L'utilisateur peut ajouter ou modifier des données qui :</p> <ul style="list-style-type: none"> 1 Identifie le châssis, telles que le nom du châssis et son emplacement. 1 Sont attribuées spécifiquement au châssis, tel que le mode IP (statique ou DHCP), l'adresse IP statique, la passerelle statique et le masque de sous-réseau statique. 1 Fournissent des services au châssis, tels que la date et heure, la mise à jour de micrologiciel et la réinitialisation CMC. 1 Sont associées au châssis, par exemple, le nom de logement et la priorité du logement. Bien que ces propriétés s'appliquent aux serveurs, ce sont strictement des propriétés du châssis qui concernent les logements plutôt que les serveurs eux-mêmes. C'est pourquoi, les noms de logement et les priorités de logement peuvent être ajoutés ou modifiés, que les serveurs soient présents dans les logements ou non. <p>Lorsqu'un serveur est déplacé vers un châssis différent, il hérite du nom et de la priorité du logement affectés au logement qu'il occupe dans le nouveau châssis. Le nom et la priorité du logement précédent restent avec le châssis précédent.</p>
Administrateur de configuration des utilisateurs	<p>L'utilisateur peut :</p> <ul style="list-style-type: none"> 1 Ajouter un nouvel utilisateur 1 Supprimer un utilisateur existant 1 Modifier le mot de passe d'un utilisateur 1 Modifier les privilèges d'un utilisateur 1 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 d'effacement des journaux	L'utilisateur peut effacer le journal matériel et le journal CMC.
Administrateur de contrôle du châssis (contrôle de l'alimentation)	<p>Les utilisateurs CMC qui disposent du privilège Administrateur de l'alimentation du châssis peuvent effectuer toutes les opérations liées à l'alimentation :</p> <ul style="list-style-type: none"> 1 Contrôler les opérations d'alimentation du châssis, y compris la mise sous tension, la mise hors tension et le cycle d'alimentation.
Server Administrator	<p>Les droits d'administrateur de serveur sont des droits permanents qui autorisent l'utilisateur CMC à effectuer des opérations sur n'importe quel serveur présent dans le châssis.</p> <p>Lorsqu'un utilisateur doté du privilège d'administrateur du serveur émet une action à effectuer sur un serveur, le micrologiciel CMC envoie la commande au serveur cible sans vérifier les privilèges de cet utilisateur sur le serveur. Autrement dit, les droits d'administrateur de serveur annulent toute absence de droits d'administrateur sur le serveur.</p> <p>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 :</p> <ul style="list-style-type: none"> 1 Le même nom d'utilisateur est utilisé sur le serveur 1 Le même nom d'utilisateur doit avoir exactement le même mot de passe sur le serveur 1 L'utilisateur doit avoir le droit d'exécuter la commande <p>Lorsqu'un utilisateur CMC qui ne dispose pas du privilège Administrateur de serveur émet une action à effectuer sur un serveur, CMC envoie une commande au serveur cible accompagnée du nom de connexion et du mot de passe de l'utilisateur. Si l'utilisateur n'existe pas sur le serveur ou si le mot de passe ne correspond pas, l'utilisateur se voit dans l'impossibilité d'effectuer l'action.</p> <p>Si l'utilisateur existe sur le serveur cible et si le mot de passe correspond, le serveur répond avec les privilèges accordés à l'utilisateur sur le serveur. Selon les privilèges renvoyés par le serveur, le micrologiciel CMC décide si l'utilisateur a le droit d'effectuer l'action.</p> <p>Nous avons répertorié ci-dessous les privilèges et les actions serveur auxquels l'administrateur du serveur a droit. Ces droits sont appliqués uniquement lorsque l'utilisateur du châssis ne dispose pas de droits d'administration serveur sur le châssis.</p>
Administrateur du serveur (suite)	<p>Administrateur et configuration du serveur :</p> <ul style="list-style-type: none"> 1 Définir l'adresse IP 1 Définir la passerelle 1 Définir le masque de sous-réseau 1 Définir le périphérique de démarrage initial <p>Configurer les utilisateurs :</p> <ul style="list-style-type: none"> 1 Définir le mot de passe racine iDRAC 1 Réinitialisation d'iDRAC <p>Administrateur et contrôle du serveur :</p> <ul style="list-style-type: none"> 1 Mise sous tension 1 Hors tension 1 Cycle d'alimentation 1 Arrêt normal 1 Redémarrage du serveur
Utilisateur de tests d'alertes	L'utilisateur peut envoyer des messages d'alerte d'essai.
Administrateur et 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 B1 ou B2 des logements d'E/S.
Administrateur de structure C	L'utilisateur peut définir et configurer le module d'E/S de la structure C, qui réside dans le logement C1 ou C2 des logements

C	d'E/S.
Super utilisateur	L'utilisateur a un accès racine à CMC et a des privilèges d'administrateur de configuration des utilisateurs et de connexion à l'utilisateur CMC. Seuls les utilisateurs avec des privilèges Super utilisateur peuvent accorder aux utilisateurs nouveaux ou existants des privilèges d'Administrateur de commande de débogage et de Super utilisateur.

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, puis que vous ajoutez ou supprimez un privilège du jeu prédéfini, le groupe CMC devient automatiquement Personnalisé.

Tableau 5-41. Privilèges de groupe CMC

Groupe d'utilisateurs	Privilèges octroyés
Administrateur	<ul style="list-style-type: none"> Ouverture de session utilisateur CMC Administrateur de configuration du châssis Administrateur de configuration des utilisateurs Administrateur d'effacement des journaux Server Administrator Utilisateur de tests d'alertes Administrateur et commandes de débogage Administrateur de structure A Administrateur de structure B Administrateur de structure C
Utilisateur privilégié	<ul style="list-style-type: none"> Connexion Administrateur d'effacement des journaux Administrateur de contrôle du châssis (contrôle de l'alimentation) Server Administrator Utilisateur de tests d'alertes Administrateur de structure A Administrateur de structure B Administrateur de structure C
Utilisateur invité	Connexion
Personnalisé	Sélectionnez n'importe quelle combinaison des autorisations suivantes : <ul style="list-style-type: none"> Ouverture de session utilisateur CMC Administrateur de configuration du châssis Administrateur de configuration des utilisateurs Administrateur d'effacement des journaux Administrateur de contrôle du châssis (contrôle de l'alimentation) Super utilisateur Server Administrator Utilisateur de tests d'alertes Administrateur et commandes de débogage Administrateur de structure A Administrateur de structure B Administrateur de structure C
None (Aucune)	Aucune autorisation n'a été attribuée.

Tableau 5-42. Comparaison des privilèges des administrateurs CMC, des utilisateurs privilégiés et des utilisateurs invités

Privilège défini	Droits d'administrateur	Utilisateur privilégié Autorisations	Utilisateur invité Autorisations
Ouverture de session utilisateur CMC	✓	✓	✓
Administrateur de configuration du châssis	✓	✗	✗
Administrateur de configuration des utilisateurs	✓	✗	✗
Administrateur d'effacement des journaux	✓	✓	✗
Administrateur de contrôle du châssis (contrôle de l'alimentation)			

	✓	✓	✗
Super utilisateur	✓	✗	✗
Server Administrator	✓	✓	✗
Utilisateur de tests d'alertes	✓	✓	✗
Administrateur et commandes de débogage	✓	✗	✗
Administrateur de structure A	✓	✓	✗
Administrateur de structure B	✓	✓	✗
Administrateur de structure C	✓	✓	✗

Ajout et gestion des utilisateurs

À partir des pages **Utilisateurs** et **Configuration utilisateur** de l'interface Web, vous pouvez afficher les informations relatives aux utilisateurs CMC, ajouter un nouvel utilisateur et modifier les paramètres d'un utilisateur existant.

Vous pouvez configurer jusqu'à 16 utilisateurs locaux. Si des utilisateurs supplémentaires sont nécessaires et que votre entreprise utilise Microsoft Active Directory ou les services LDAP, vous pouvez le configurer pour permettre l'accès à CMC. La configuration d'Active Directory vous permet d'ajouter des privilèges d'utilisateur CMC à vos utilisateurs existants dans votre logiciel Active Directory et de les contrôler, en plus des 16 utilisateurs locaux. Pour plus d'informations, voir [Utilisation du service d'annuaire CMC](#). Pour plus d'informations sur LDAP, consultez la section « Utilisation de CMC avec les services Lightweight Directory Access Protocol ».

La session de l'utilisateur peut être ouverte via l'interface Web, ou encore via une session Telnet, série, SSH ou iKVM. Un maximum de 22 sessions actives (interface Web, Telnet, série, SSH et iKVM, dans n'importe quelle combinaison) peuvent être partagées par les utilisateurs.

 **REMARQUE** : pour plus de sécurité, il est vivement recommandé de modifier le mot de passe par défaut du compte root (User 1). Le compte root est le compte d'administration par défaut fourni avec le contrôleur CMC. Pour modifier le mot de passe par défaut de ce compte, cliquez sur **User ID 1** (ID utilisateur 1) afin d'ouvrir la page **User Configuration** (Configuration des utilisateurs). L'aide relative à cette page est disponible via le lien **Aide en haut à droite** de la page.

Pour ajouter et configurer des utilisateurs CMC :

 **REMARQUE** : vous devez disposer du privilège de **configuration des utilisateurs** pour effectuer les étapes suivantes.

1. Connectez-vous à l'interface Web.
2. Cliquez sur l'onglet **Authentification utilisateur**. La page **Utilisateurs locaux** s'affiche, répertoriant l'ID, le nom d'utilisateur, les privilèges CMC et l'état d'ouverture de session de chaque utilisateur, y compris ceux de l'utilisateur racine. Aucune information utilisateur n'est affichée pour les ID utilisateur disponibles pour la configuration.

3. Cliquez sur un numéro d'ID utilisateur disponible. La page **Configuration utilisateur** s'affiche.

Pour actualiser le contenu de la page **Utilisateurs**, cliquez sur **Actualiser**. Pour imprimer le contenu de la page **Utilisateurs**, cliquez sur **Imprimer**.

4. Sélectionnez les paramètres généraux de l'utilisateur.

Tableau 5-43. décrit les paramètres généraux de configuration d'un nom d'utilisateur et d'un mot de passe CMC (nouveau ou existant).

--	--

Propriété	Description
Réf. utilisateur	(Lecture seule) Identifie un utilisateur à l'aide de l'un des 16 nombres séquentiels prédéfinis utilisés à des fins d'écriture de scripts de l'interface de ligne de commande. La réf. utilisateur identifie un utilisateur donné lors de la configuration de cet utilisateur à l'aide de l'outil de l'interface de ligne de commande (RACADM). Vous ne pouvez pas modifier la référence utilisateur. Si vous modifiez des informations pour l'utilisateur root, ce champ est statique. Vous ne pouvez pas modifier le nom d'utilisateur root.
Activer l'utilisateur	Active ou désactive l'accès de l'utilisateur à CMC.
Nom d'utilisateur	Définit ou affiche le nom d'utilisateur CMC unique correspondant à l'utilisateur. Ce nom d'utilisateur peut contenir jusqu'à 16 caractères. Les noms d'utilisateur CMC ne peuvent pas contenir de barres obliques (/) ni de points (.). REMARQUE : Si vous modifiez le nom d'utilisateur, le nouveau nom apparaît dans l'interface utilisateur lors de la prochaine ouverture de session. Tout utilisateur qui ouvre une session après l'application du nouveau nom d'utilisateur pourra immédiatement observer la modification.
Modifier le mot de passe	Permet la modification du mot de passe d'un utilisateur existant. Définissez le nouveau mot de passe dans le champ Nouveau mot de passe . La case Modifier le mot de passe ne peut pas être sélectionnée si vous configurez un nouvel utilisateur. Vous ne pouvez la sélectionner que lorsque vous modifiez un paramètre utilisateur existant.
Le mot de passe	Définit un nouveau mot de passe pour un utilisateur existant. Pour modifier le mot de passe, vous devez également cocher la case Modifier le mot de passe . Le mot de passe peut contenir jusqu'à 20 caractères, qui s'affichent sous forme de points à mesure de leur saisie.
Confirmer le mot de passe	Vérifie le mot de passe que vous avez entré dans le champ Nouveau mot de passe . REMARQUE : les champs Nouveau mot de passe et Confirmer le nouveau mot de passe sont modifiables uniquement lorsque vous (1) configurez un nouvel utilisateur ou que vous (2) modifiez les paramètres d'un utilisateur existant, et que la case Modifier le mot de passe est cochée.

- Affectez l'utilisateur à un groupe d'utilisateurs du contrôleur CMC. Le [Tableau 5-40](#) décrit les privilèges utilisateur CMC.

Lorsque vous sélectionnez un privilège utilisateur dans le menu déroulant CMC Group (Groupe CMC), les privilèges activés (cochés) correspondent aux paramètres prédéfinis pour ce groupe.

Vous pouvez modifier les privilèges octroyés à un utilisateur en sélectionnant ou en désélectionnant des cases à cocher. Après avoir sélectionné un groupe CMC ou défini les privilèges d'un utilisateur, cliquez sur **Appliquer les modifications** pour que les changements effectués soient conservés.

- Cliquez sur **Appliquer les modifications**.

Pour actualiser le contenu de la page **Configuration utilisateur**, cliquez sur **Actualiser**.

Pour imprimer le contenu de la page **Configuration utilisateur**, cliquez sur **Imprimer**.

Configuration et gestion des certificats Microsoft Active Directory

 **REMARQUE** : vous devez disposer du privilège **Administrateur de configuration du châssis** pour configurer les paramètres Active Directory pour CMC.

 **REMARQUE** : pour plus d'informations sur la configuration d'Active Directory et sur la manière de configurer Active Directory avec le schéma standard ou un schéma étendu, voir [Utilisation du service d'annuaire CMC](#).

Vous pouvez utiliser le service Microsoft Active Directory pour configurer votre logiciel afin de fournir l'accès à CMC. Le service Active Directory vous permet d'ajouter et de contrôler les privilèges utilisateur CMC de vos utilisateurs existants.

Pour accéder à la page **Menu principal d'Active Directory** :

- Connectez-vous à l'interface Web.
- Cliquez sur l'onglet **Authentification utilisateur**, puis cliquez sur le sous-onglet **Services d'annuaire**. Sélectionnez le bouton radio pour Microsoft Active Directory schéma standard ou schéma étendu. Les tableaux Active Directory s'affichent.

Paramètres communs

Cette section vous permet de configurer et d'afficher les paramètres communs d'Active Directory pour CMC.

Tableau 5-44. Paramètres communs

--	--

Champ	Description
Activer Active Directory	Active la connexion Active Directory sur CMC. Vous devez installer des certificats SSL pour les serveurs Active Directory qui sont signés par la même autorité de certificat et les charger sur CMC.
Activer la connexion par carte à puce	Active l'inter-fonctionnement d'Active Directory basé sur l'authentification Kerberos prise en charge par un plug-in de navigateur auto-installé et fourni par Dell, et l'utilisation de carte à puce. Pour activer la carte à puce, cochez la case. Pour désactiver la carte à puce, décochez la case. Si vous activez la carte à puce, vous devez également configurer votre poste de travail client Microsoft Windows pour qu'il opère correctement avec la fonctionnalité de lecteur de cartes à puce. Cela implique d'installer les pilotes appropriés pour le lecteur de cartes à puce et ceux pour la carte à puce actuellement utilisée. Les pilotes de carte à puce varient selon les fournisseurs. La carte à puce doit être correctement programmée avec les autorisations nécessaires en utilisant les services d'inscription de carte à puce fournis par le serveur Active Directory adéquat. REMARQUE : la connexion par carte à puce et la connexion directe s'excluent mutuellement. Vous ne pouvez en configurer qu'une seule à la fois.
Activer la connexion directe	Permet à CMC d'utiliser Active Directory . Pour activer la connexion directe , cochez la case. Pour désactiver la connexion directe , décochez la case. Si vous activez la connexion directe , vous devez également définir les propriétés Active Directory et sélectionner le schéma que vous souhaitez utiliser. REMARQUE : La connexion par carte à puce et la connexion directe s'excluent mutuellement. Vous ne pouvez en configurer qu'une seule à la fois.
Activer la validation de certificat SSL	Permet la validation de certificat SSL pour la connexion SSL Active Directory de CMC. Pour désactiver la validation du certificat SSL, décochez la case. Attention : en désactivant cette fonctionnalité, vous exposez l'authentification à une attaque de l'homme du milieu (MITM). Pour que le navigateur fonctionne correctement, il faut que CMC soit accessible via une URL HTTP qui contient une adresse de domaine pleinement qualifiée pour CMC, à savoir http://cmc-6g2wxf1.dom.net . Une adresse IP simple pour CMC n'entraîne pas un bon fonctionnement de la connexion directe. Pour prendre en charge les adresses de domaine pleinement qualifiées, il est nécessaire d'enregistrer CMC auprès du service de nom de domaine du serveur Active Directory. Si l'authentification de navigateur à connexion directe est infructueuse, la méthode d'authentification locale et habituelle du navigateur par nom d'utilisateur / mot de passe est automatiquement présentée. De même, après une connexion directe réussie la méthode nom d'utilisateur / mot de passe est proposée lors d'une action de déconnexion. La connexion directe est destinée à être pratique, et non pas restrictive. REMARQUE : l'authentification du navigateur basée sur carte à puce ne fonctionne que pour les clients Microsoft Windows et Internet Explorer. Le plug-in de navigateur auto-installé et fourni par Dell (ActiveX control) est dépendant du système d'exploitation Microsoft Windows ayant le composant d'exécution suivant pré-installé : Microsoft Visual C++ 2005 Redistributable Package (x86). Le lien suivant peut aider à trouver le composant : http://www.microsoft.com/downloads/details.aspx?FamilyID=32BC1BEE-A3F9-4C13-9C99-220B62A191EE&displaylang=en . Le client Windows nécessite des « privilèges élevés » pour installer avec succès le contrôle ActiveX. De même, la configuration du navigateur doit pouvoir accepter l'installation des contrôles ActiveX non signés.
	L'activation de la carte à puce applique une politique d'authentification du navigateur par carte à puce uniquement. Les autres méthodes d'authentification du navigateur telles que l'authentification locale ou Active Directory par nom d'utilisateur / mot de passe sont limitées. Si la politique d'application de l'authentification par carte à puce uniquement est adoptée, il est important que l'opération de la carte à puce soit entièrement validée avant que les autres méthodes d'accès à CMC soient désactivées. Dans le cas contraire, l'accès à CMC peut être verrouillé par inadvertance.
Nom de domaine racine	Spécifie le nom de domaine utilisé par Active Directory. Le nom de domaine racine est le nom de domaine racine entièrement qualifié pour la forêt. REMARQUE : le nom de domaine racine doit être un nom de domaine valide qui respecte la convention d'attribution des noms x.y, où x est une chaîne de 1 à 256 caractères ASCII non séparés par des espaces, et où y est un type de domaine valide tel que com, edu, gov, int, mil, net ou org.
Délai d'attente AD	Définit le délai en secondes après lequel une session Active Directory inactive est automatiquement fermée. Valeurs valides : 15 300 secondes Par défaut : 90 secondes
Spécifier le serveur AD à rechercher (facultatif)	Active (si coché) l'appel dirigé vers le contrôleur de domaine et le catalogue global. Si vous activez cette option, vous devez également spécifier les emplacements du contrôleur de domaine et du catalogue global dans les paramètres suivants. REMARQUE : le nom apparaissant sur le certificat d'autorité de certification d'Active Directory n'est pas comparé au serveur Active Directory ou au serveur du catalogue global spécifié.
Contrôleur de domaine	Spécifie le serveur où votre service Active Directory est installé. Cette option n'est valide que si Spécifier le serveur AD à rechercher (facultatif) est activé.
Catalogue global	Spécifie l'emplacement du catalogue global sur le contrôleur de domaine d'Active Directory. Le catalogue global fournit une ressource pour rechercher une forêt Active Directory. Cette option n'est valide que si l'option Spécifier le serveur AD à rechercher (facultatif) est activée.

Paramètres du schéma standard

Affichée lorsque Microsoft Active Directory (schéma standard) est sélectionné, cette section présente les groupes de rôles avec les noms, domaines et

privilèges associés pour les groupes de rôles qui ont déjà été configurés.

Pour modifier les paramètres d'un groupe de rôles, cliquez sur son numéro dans la liste des groupes de rôles.

 **REMARQUE** : si vous cliquez sur le lien d'un groupe de rôles avant d'avoir appliqué les nouveaux paramètres que vous avez définis, ces derniers seront perdus. Afin d'éviter la perte de tout nouveau paramètre, cliquez sur **Appliquer** avant de cliquer sur le lien d'un groupe de rôles.

La page Configurer le groupe de rôles s'affiche.

- 1 Nom du groupe : nom qui identifie le groupe de rôles dans l'Active Directory associé à la carte CMC.
- 1 Domaine du groupe : domaine où se situe le groupe.
- 1 Privilèges de groupe : niveau de privilège du groupe.

Cliquez sur **Appliquer** pour enregistrer les paramètres.

Cliquez sur **Retourner à la page Configuration** pour retourner à la page **Services d'annuaire**.

Pour actualiser le contenu de la page **Services d'annuaire**, cliquez sur **Actualiser**.

Pour imprimer le contenu de la page **Services d'annuaire**, cliquez sur **Imprimer**.

Paramètres du schéma étendu

Affichée lorsque Microsoft Active Directory (schéma étendu) est sélectionné, cette section présente les propriétés suivantes :

- 1 Nom du dispositif CMC : affiche le nom de l'objet de dispositif RAC que vous avez créé pour CMC. Le nom du dispositif CMC identifie de manière unique la carte CMC dans Active Directory. Le nom du dispositif CMC doit être identique au nom courant du nouvel objet de dispositif RAC que vous avez créé dans votre contrôleur de domaine. Le nom de CMC doit être une chaîne de 1 à 256 caractères ASCII, sans espace entre les caractères. Pour plus d'informations sur les objets de dispositif RAC, consultez le Guide de l'utilisateur de CMC.
- 1 Nom de domaine CMC : affiche le nom DNS (chaîne) du domaine où l'objet de dispositif RAC d'Active Directory réside. Le nom de domaine de CMC doit être un nom de domaine valide composé de *x.y*, où *x* est une chaîne de 1 à 256 caractères ASCII sans espace entre les caractères et *y* est un type de domaine valide comme com, edu, gov, int, mil ou org.

Gestion des certificats Active Directory

Cette section affiche les propriétés du certificat Active Directory récemment transféré à CMC. Si vous avez téléchargé un certificat, utilisez ces informations pour vérifier que le certificat est valide et n'a pas expiré.

 **REMARQUE** : par défaut, CMC ne dispose pas d'un certificat de serveur délivré par une autorité de certification pour Active Directory. Vous devez téléverser un certificat de serveur valide, signé par une autorité de certification.

Les propriétés suivantes sont affichées pour le certificat :

- 1 Numéro de série : numéro de série du certificat.
- 1 Informations sur le sujet : sujet du certificat (nom de la personne ou de l'entreprise certifiée).
- 1 Renseignements sur l'émetteur : émetteur du certificat (nom de l'autorité de certification).
- 1 Valide à partir de : la date de début du certificat.
- 1 Valide jusqu'à : la date d'expiration du certificat.

Utilisez les commandes ci-dessous pour télécharger et envoyer ce certificat :

- 1 Téléverser : lance le processus de téléversement du certificat. Ce certificat, qui vous est délivré par Active Directory, permet d'accéder à CMC.
- 1 Télécharger : lance le processus de téléchargement. Vous êtes invité à choisir un emplacement pour enregistrer le fichier. Lorsque vous sélectionnez cette option et cliquez sur **Suivant**, la boîte de dialogue **Téléchargement de fichier** apparaît. Utilisez cette boîte de dialogue pour spécifier l'emplacement réservé au certificat de serveur sur votre station de gestion ou réseau partagé.

 **REMARQUE** : par défaut, CMC ne dispose pas d'un certificat de serveur délivré par une autorité de certification pour Active Directory. Vous devez téléverser un certificat de serveur valide, signé par une autorité de certification.

Fichier Keytab Kerberos

Vous pouvez téléverser un fichier keytab Kerberos généré sur le serveur Active Directory associé. Vous pouvez générer le fichier keytab Kerberos depuis le serveur Active Directory en exécutant l'utilitaire **ktpass.exe**. Ce fichier keytab établit une relation de confiance entre le serveur Active Directory Server et CMC.

 **REMARQUE** : CMC ne dispose pas d'un fichier keytab Kerberos pour Active Directory. Vous devez téléverser un fichier keytab Kerberos généré. Voir la section [Configuration de la connexion directe](#) pour obtenir des informations détaillées.

Les actions suivantes sont autorisées :

- 1 Parcourir : ouvre une boîte de dialogue **Parcourir**, depuis laquelle vous sélectionnez le certificat de serveur que vous souhaitez téléverser.

- 1 Téléverser : lance le processus de téléchargement pour le certificat en utilisant le chemin du fichier que vous spécifiez.

Configuration et gestion des services LDAP génériques

Vous pouvez utiliser le service LDAP (Lightweight Directory Access Protocol) générique pour configurer votre logiciel afin qu'il fournisse l'accès à CMC. Le service LDAP vous permet d'ajouter et de contrôler les privilèges utilisateur CMC de vos utilisateurs existants.

 **REMARQUE** : vous devez disposer du privilège **Administrateur de configuration du châssis** pour configurer les paramètres Active Directory pour CMC.

Pour afficher et configurer LDAP :

1. Connectez-vous à l'interface Web.
2. Cliquez sur l'onglet **Authentification utilisateur**, puis cliquez sur le sous-onglet **Services d'annuaire**. La page **Services d'annuaire** s'affiche.
3. Cliquez sur le bouton radio associé au LDAP générique.
4. Configurez les options affichées et cliquez sur **Appliquer**.

Les options de configuration disponibles sont les suivantes :

Tableau 5-45. Paramètres communs

Paramètre	Description
LDAP générique activé	Active le service LDAP générique sur CMC.
Utilisez le nom unique (DN) pour rechercher l'appartenance au groupe.	Spécifie le nom unique (DN) de groupes LDAP dont les membres sont autorisés à accéder au dispositif.
Activer la validation de certificat SSL	Si activé, CMC utilise le certificat d'une autorité de certification pour valider le certificat du serveur LDAP pendant l'établissement de liaisons SSL.
Liaison de DN	Le nom unique d'un utilisateur utilisé pour établir la liaison au serveur lors de la recherche du nom unique de l'utilisateur d'ouverture de session. S'il n'est pas fourni, une liaison anonyme est utilisée.
Le mot de passe	Mot de passe de liaison à utiliser conjointement avec le nom unique de liaison. REMARQUE : le mot de passe de liaison contient des données confidentielles et doit être protégé de manière appropriée.
Nom unique de base à rechercher	Nom unique de la branche du répertoire à partir duquel toutes les recherches doivent débuter.
Attribut de l'identifiant de l'utilisateur	Spécifie l'attribut à rechercher. S'il n'est pas configuré, uid est utilisé par défaut. Il est recommandé qu'il soit unique dans le DN de base choisi, faute de quoi un filtre de recherche doit être configuré pour assurer l'unicité de l'utilisateur d'ouverture de session. Si le DN d'utilisateur ne peut pas être identifié par la recherche de la combinaison de l'attribut et du filtre de recherche, la connexion échoue avec une erreur.
Attribut de l'appartenance au groupe.	Spécifie l'attribut LDAP qui est utilisé pour vérifier l'appartenance au groupe. Il doit s'agir d'un attribut de la classe de groupe. S'il n'est pas spécifié, les attributs member et uniquemember sont utilisés.
Filtre de recherche	Indique un filtre de recherche LDAP valide. Ceci est utilisé si l'attribut d'utilisateur ne parvient pas à identifier de manière unique l'utilisateur d'ouverture de session dans le nom unique de base choisi. S'il n'est pas spécifié, la valeur est définie par défaut sur (objectClass=*), qui recherche tous les objets de l'arborescence. La longueur maximale de cette propriété est de 1 024 caractères.
Délai de réseau (secondes)	Définit le délai en secondes après lequel une session LDAP inactive est automatiquement fermée.
Délai de recherche (secondes)	Définit le délai en secondes après lequel une recherche est automatiquement fermée.

Sélection de vos serveurs LDAP

Vous pouvez configurer le serveur pour une utilisation avec le LDAP générique de deux façons. Les serveurs statiques permettent à l'administrateur de mettre un nom de domaine pleinement qualifié ou une adresse IP dans le champ. Par ailleurs, une liste de serveurs LDAP peut être récupérée en recherchant leur enregistrement SRV dans le DNS. Les éléments suivants sont les propriétés de la section Serveurs LDAP :

- 1 Utiliser les serveurs LDAP statiques : en sélectionnant cette option, le service LDAP utilise les serveurs spécifiés avec le numéro de port fourni (voir les détails ci-dessous).

 **REMARQUE** : vous devez sélectionner Statique ou DNS.

- 1 Adresse de serveur LDAP : préciser le nom de domaine pleinement qualifié ou l'adresse IP du serveur LDAP. Pour spécifier plusieurs serveurs LDAP redondants qui desservent le même domaine, fournissez la liste de tous les serveurs séparés par des virgules. CMC tente de se connecter à chaque serveur l'un après l'autre jusqu'à ce qu'une connexion soit établie.
- 1 Port de serveur LDAP : port de LDAP sur SSL, par défaut 636 s'il n'est pas configuré. Le port non SSL n'est pas pris en charge dans la version 3.0 de CMC puisque le mot de passe ne peut être transporté sans SSL.

- 1 Utiliser le DNS pour trouver des serveurs LDAP : en sélectionnant cette option, LDAP utilise le domaine de la recherche et le nom du service via DNS. Vous devez sélectionner Statique ou 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.

Gestion des paramètres de groupe LDAP

Le tableau dans la section Paramètres du groupe répertorie les groupes de rôles et affiche les noms, domaines et privilèges associés pour les groupes de rôles qui sont déjà configurés.

- 1 Pour configurer un nouveau groupe de rôles, cliquez sur un nom de groupe de rôles qui n'a pas de nom, de domaine et de privilège dans la liste.
- 1 Pour modifier les paramètres d'un groupe de rôles existant, cliquez sur le nom de groupe de rôles.

Lorsque vous cliquez sur un nom de groupe de rôles, la page **Configurer le groupe de rôles** s'affiche. L'aide relative à cette page est disponible via le lien Aide en haut à droite de la page.

Gestion des certificats de sécurité LDAP

Cette section affiche les propriétés du certificat LDAP récemment téléversé sur CMC. Si vous avez téléchargé un certificat, utilisez ces informations pour vérifier que le certificat est valide et n'a pas expiré.

 **REMARQUE** : par défaut, CMC ne dispose pas d'un certificat de serveur délivré par une autorité de certification pour Active Directory. Vous devez téléverser un certificat de serveur valide, signé par une autorité de certification.

Les propriétés suivantes sont affichées pour le certificat :

- 1 Numéro de série : numéro de série du certificat.
- 1 Informations sur le sujet : sujet du certificat (nom de la personne ou de l'entreprise certifiée).
- 1 Renseignements sur l'émetteur : émetteur du certificat (nom de l'autorité de certification).
- 1 Valide à partir de : la date de début du certificat.
- 1 Valide jusqu'à : la date d'expiration du certificat.

Utilisez les commandes ci-dessous pour télécharger et envoyer ce certificat :

- 1 **Téléverser** : lance le processus de téléversement du certificat. Ce certificat, qui vous est délivré par votre serveur LDAP, permet d'accéder à CMC.
 - 1 **Télécharger** : lance le processus de téléchargement. Vous êtes invité à choisir un emplacement pour enregistrer le fichier. Lorsque vous sélectionnez cette option et cliquez sur **Suivant**, la boîte de dialogue **Téléchargement de fichier** apparaît. Utilisez cette boîte de dialogue pour spécifier l'emplacement réservé au certificat de serveur sur votre station de gestion ou réseau partagé.
-

Sécurisation des communications CMC à l'aide de certificats SSL et numériques

Cette sous-section fournit des informations sur les fonctionnalités de sécurité des données suivantes qui sont intégrées dans CMC :

- 1 Secure Sockets Layer (SSL)
- 1 Requête de signature de certificat (RSC)
- 1 Accès au menu principal SSL
- 1 Génération d'une nouvelle RSC
- 1 Téléversement d'un certificat de serveur
- 1 Affichage d'un certificat de serveur

Secure Sockets Layer (SSL)

CMC utilise Web Server, un serveur configuré pour utiliser le protocole de sécurité SSL standard de l'industrie afin de transférer des données cryptées sur Internet. Basé sur la technologie de cryptage à clé publique et à clé privée, SSL est une technique très répandue permettant une communication authentifiée et cryptée entre les clients et les serveurs afin d'empêcher toute écoute indiscrète sur un réseau.

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

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

Ce processus de cryptage fournit un haut niveau de protection de données. CMC applique la norme de cryptage SSL à 128 bits, qui est la forme la plus fiable de cryptage généralement disponible pour les navigateurs Internet en Amérique du Nord.

CMC Web Server inclut un certificat numérique SSL Dell auto-signé (la référence serveur). Pour garantir un haut niveau de sécurité sur Internet, remplacez le certificat SSL de serveur Web en envoyant une requête à CMC pour générer une nouvelle requête de signature de certificat (RSC).

Requête de signature de certificat (RSC)

Une RSC est une requête numérique auprès d'une autorité de certification en vue de l'obtention d'un certificat de sécurité serveur. Les certificats de serveur sécurisé garantissent l'identité d'un système distant et assurent que les informations échangées avec le système distant ne peuvent être ni affichées, ni modifiées par d'autres. Pour garantir la sécurité de CMC, il est fortement recommandé de générer une RSC, de l'envoyer à une autorité de certification et de téléverser le certificat qu'elle vous renvoie.

Une autorité de certification est une entité commerciale reconnue dans l'industrie de l'informatique pour ses critères élevés en matière de dépistage et d'identification fiables et d'autres critères de sécurité importants. Thawte et VeriSign sont des exemples d'AC. Une fois que l'autorité de certification reçoit votre RSC, elle examine et vérifie les informations qu'elle contient. Si le demandeur répond aux normes de sécurité de l'autorité de certification, celle-ci émet un certificat qui identifie ce demandeur de manière unique pour les transactions effectuées sur des réseaux et sur Internet.

Une fois que l'autorité de certification approuve la RSC et qu'elle vous envoie un certificat, vous devez téléverser le certificat sur le micrologiciel CMC. Les informations de la RSC stockées sur le micrologiciel CMC doivent correspondre aux informations du certificat.

Accès au menu principal SSL

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

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

1. Connectez-vous à l'interface Web.
2. Cliquez sur l'onglet **Réseau**, puis sur le sous-onglet **SSL**. La page **Menu principal SSL** s'affiche.

Utilisez les options de la page **Menu principal SSL** pour générer une RSC à envoyer à une autorité de certification. Les informations de la RSC sont stockées dans le micrologiciel CMC.

Génération d'une nouvelle requête de signature de certificat

Pour des raisons de sécurité, Dell vous recommande fortement d'obtenir et de téléverser un certificat de serveur sécurisé sur 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 être ni affichées ni modifiées par d'autres personnes. Sans certificat de serveur sécurisé, CMC est vulnérable aux accès par les utilisateurs non autorisés.

Tableau 5-46. Options du menu principal SSL

Champ	Description
Générer une nouvelle requête de signature de certificat (RSC)	Sélectionnez cette option et cliquez sur Suivant pour ouvrir la page Générer la requête de signature de certificat (RSC) , sur laquelle vous pouvez générer une RSC à envoyer à une autorité de certification afin de demander un certificat Web sécurisé. REMARQUE : chaque nouvelle RSC supprime la RSC qui se trouve déjà sur le micrologiciel. Pour qu'une autorité de certification accepte votre RSC, la RSC de CMC doit correspondre au certificat renvoyé par l'autorité de certification.
Téléverser le certificat de serveur basé sur la RSC générée	Sélectionnez cette option et cliquez sur Suivant pour ouvrir la page Téléversement d'un certificat sur laquelle vous pouvez téléverser un certificat existant auquel votre société est autorisée à accéder et qu'elle utilise pour contrôler l'accès à CMC. REMARQUE : CMC accepte uniquement les certificats X509, encodés en base 64. Les certificats encodés DER ne sont pas acceptés. Si vous téléversez un nouveau certificat, il remplace le certificat par défaut que vous avez reçu avec CMC.
Téléverser une clé de serveur Web et un certificat	Sélectionnez cette option et cliquez sur Suivant pour ouvrir la page Téléversement d'une clé et d'un certificat de serveur Web sur laquelle vous pouvez téléverser une clé de serveur Web et un certificat de serveur existants auxquels votre société est autorisée à accéder et qu'elle utilise pour contrôler l'accès à CMC. REMARQUE : CMC accepte uniquement les certificats X.509 encodés en base 64. Les certificats binaires encodés DER ne sont pas acceptés. Si vous téléversez un nouveau certificat, il remplace le certificat par défaut que vous avez reçu avec CMC.

Afficher le certificat de serveur	Sélectionnez l'option et cliquez sur le bouton Suivant pour ouvrir la page Afficher le certificat de serveur sur laquelle vous pouvez visualiser le certificat du serveur actuel.
-----------------------------------	---

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

Lorsqu'une RSC est générée depuis la page **Générer une requête de signature de certificat (RSC)**, vous êtes invité à en enregistrer une copie sur votre station de gestion ou votre réseau partagé, et les informations uniques utilisées pour générer la RSC sont stockées sur CMC. Ces informations sont utilisées par la suite pour authentifier le certificat de serveur que vous recevez de l'autorité de certification. Après avoir reçu le certificat de serveur de l'autorité de certification, vous devez ensuite le téléverser sur 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 les RSC existant déjà sur CMC. Si une RSC en attente est écrasée avant qu'une autorité de certification livre son certificat de serveur, CMC n'acceptera pas le certificat de serveur car les informations qu'il utilise pour authentifier le certificat auront été perdues. Soyez vigilant lorsque vous générez une RSC afin d'éviter de remplacer les RSC en attente.

Pour générer une RSC :

1. Sur la page Menu principal SSL, sélectionnez **Générer une nouvelle requête de signature de certificat (RSC)**, puis cliquez sur **Suivant**. La page **Générer une requête de signature de certificat (RSC)** s'affiche.
2. Entrez une valeur pour chaque attribut de la RSC.
3. Cliquez sur **Générer**. La boîte de dialogue **Téléchargement de fichier** apparaît.
4. Enregistrez le fichier `csr.txt` sur votre station de gestion ou votre réseau partagé. (Vous pouvez également ouvrir le fichier et l'enregistrer ultérieurement). Vous soumettez ensuite ce fichier à une autorité de certification.

Tableau 5-47. Options de la page **Générer une requête de signature de certificat (RSC)**

Champ	Description
Nom commun	Nom exact à certifier (généralement le nom de domaine du serveur Web, par exemple, <code>www.compagnixyz.com</code>). Sont valides : les caractères alphanumériques (A-Z, a-z, 0-9), les traits d'union, les traits de soulignement et les points. Ne sont pas valides : les caractères non-alphanumériques non repris ci-dessus (notamment @ # \$ % & *) et les caractères utilisés principalement dans d'autres langues que l'anglais tels que ß, à, é, ü.
Nom de l'organisation	Nom associé à votre compagnie (par exemple : <code>compagnie XYZ</code>). Sont valides : les caractères alphanumériques (A-Z, a-z, 0-9), les traits d'union, les traits de soulignement, les points et les espaces. Ne sont pas valides : les caractères non-alphanumériques non repris ci-dessus (notamment @ # \$ % & *).
Service de l'organisation	Nom associé à un groupe, comme un service (par exemple : groupe de l'entreprise). Sont valides : les caractères alphanumériques (A-Z, a-z, 0-9), les traits d'union, les traits de soulignement, les points et les espaces. Ne sont pas valides : les caractères non-alphanumériques non repris ci-dessus (notamment @ # \$ % & *).
Ville	Ville ou autre emplacement de votre compagnie (par exemple : <code>Atlanta, Hong Kong</code>). Sont valides : les caractères alphanumériques (A-Z, a-z, 0-9) et les espaces. Ne sont pas valides : les caractères non-alphanumériques non repris ci-dessus (notamment @ # \$ % & *).
État	État, province ou territoire où se trouve l'entité qui demande la certification (par exemple : <code>Texas, Québec, Bouches-du-Rhône</code>). REMARQUE : n'utilisez pas d'abréviations. Sont valides : les caractères alphanumériques (lettres en majuscules et en minuscules, 0-9) et les espaces. Ne sont pas valides : les caractères non-alphanumériques non repris ci-dessus (notamment @ # \$ % & *).
Pays	Pays où se trouve la compagnie qui demande la certification.
E-mail	Adresse de messagerie de votre compagnie. Entrez l'adresse de messagerie que vous souhaitez associer à la RSC. L'adresse de messagerie doit être valide et contenir le symbole @ (par exemple, <code>nom@compagnixyz.com</code>). REMARQUE : cette adresse de messagerie est facultative.

Téléversement d'un certificat de serveur

1. Sur la page **Menu principal SSL**, sélectionnez **Téléverser le certificat de serveur basé sur RSC généré**, puis cliquez sur **Suivant**. La page **Téléversement d'un certificat** s'affiche.
2. Entrez le chemin du fichier dans le champ de texte ou cliquez sur **Parcourir** pour sélectionner le fichier.
3. Cliquez sur **Appliquer**. Si le certificat n'est pas valide, un message d'erreur s'affiche.

 **REMARQUE** : la valeur **Chemin du fichier** affiche le chemin de fichier relatif du certificat que vous téléversez. Vous devez taper le chemin de fichier absolu, y compris le chemin et le nom de fichier complets et l'extension du fichier.

Pour actualiser le contenu de la page **Téléversement d'un certificat**, cliquez sur **Actualiser**.

Pour imprimer le contenu de la page **Téléversement d'un certificat**, cliquez sur **Imprimer**.

Téléverser une clé de serveur Web et un certificat

1. Sélectionnez **Téléverser une clé de serveur Web et un certificat**, puis cliquez sur **Suivant**.
2. Entrez le fichier de clé privée en utilisant le menu de navigation.
3. Sélectionnez un fichier de certificat en utilisant le menu de navigation.
4. Quand les deux fichiers sont téléchargés, cliquez sur **Appliquer**. Si la clé du serveur Web et le certificat ne correspondent pas, un message d'erreur s'affiche.

 **REMARQUE** : CMC accepte uniquement les certificats X509, encodés en base 64. Les certificats qui utilisent d'autres schémas de codage tels que DER ne sont pas acceptés. Si vous téléversez un nouveau certificat, il remplace le certificat par défaut que vous avez reçu avec CMC.

 **REMARQUE** : pour téléverser une clé de serveur Web et un certificat de serveur, vous devez avoir des privilèges d'**administrateur de configuration du châssis**.

 **REMARQUE** : après le chargement du micrologiciel, CMC est réinitialisé et devient temporairement indisponible. Pour éviter de déconnecter d'autres utilisateurs au cours d'une réinitialisation, avertissez les utilisateurs autorisés susceptibles de se connecter à CMC et recherchez les sessions actives affichées dans la page **Sessions** sous l'onglet **Réseau**.

Affichage d'un certificat de serveur

Sur la page **Menu principal SSL**, sélectionnez **Afficher le certificat de serveur**, puis cliquez sur **Suivant**. La page **Afficher le certificat de serveur** s'affiche.

Le [Tableau 5-48](#) décrit les champs et les descriptions associées énumérés dans la fenêtre **Certificat**.

Tableau 5-48. Informations relatives au certificat

Champ	Description
Série	Numéro de série du certificat.
Demandeur	Attributs du certificat saisis par le sujet.
Émetteur	Attributs du certificat renvoyés par l'émetteur.
Pas avant	Date d'émission du certificat
Pas après	Date d'expiration du certificat

Pour actualiser le contenu de la page **Afficher le certificat de serveur**, cliquez sur **Actualiser**.

Pour imprimer le contenu de la page **Afficher le certificat de serveur**, cliquez sur **Imprimer**.

Gestion des sessions

La page **Sessions** affiche toutes les instances en cours des connexions au châssis et vous permet de mettre fin à une session active.

 **REMARQUE** : pour terminer une session, vous devez disposer du privilège **Administrateur de configuration du châssis**.

Pour gérer ou fermer une session :

1. Ouvrez une session sur CMC via le Web.
2. Cliquez sur l'onglet **Réseau**, puis sur le sous-onglet **Sessions**.
3. Sur la page **Sessions**, localisez la session que vous souhaitez terminer, puis cliquez sur le bouton approprié.

Tableau 5-49. Propriétés des sessions

Propriété	Description
N° de session	Affiche le numéro d'identification généré séquentiellement pour chaque instance d'ouverture de session.
Le nom d'utilisateur	Affiche le nom d'ouverture de session de l'utilisateur (utilisateur local ou utilisateur Active Directory). Des exemples de noms d'utilisateur Active Directory sont <i>nom@domaine.com</i> , <i>domaine.com/nom</i> , <i>domaine.com\nom</i> .
Adresse IP	Affiche l'adresse IP de l'utilisateur.
Type de session	Décrit le type de session : Telnet, série, SSH, RACADM distant, SMASH CLP, WSMAN ou d'interface utilisateur graphique.
Terminer	Vous permet de fermer les sessions répertoriées, à l'exception de la vôtre. Pour mettre fin à la session associée, cliquez sur le bouton. Cette colonne est affichée uniquement si vous disposez du privilège Administrateur de configuration du châssis .

Configuration des services

CMC utilise Web Server, un serveur configuré pour utiliser le protocole de sécurité SSL standard de l'industrie afin d'accepter et de transférer les données cryptées depuis et vers des clients sur Internet. Web Server comprend un certificat numérique SSL auto-signé Dell (référence serveur) et est chargé d'accepter et de répondre aux requêtes HTTP sécurisées émanant des clients. Ce service est requis par l'interface Web et l'outil CLI distant pour communiquer avec CMC.

 **REMARQUE** : l'outil CLI distant (RACADM) et l'interface Web utilisent Web Server. Dans l'éventualité où Web Server n'est pas actif, RACADM distant et l'interface Web ne sont pas utilisables.

 **REMARQUE** : en cas de réinitialisation de Web Server, patientez au moins une minute pour que les services soient de nouveau disponibles. La réinitialisation du serveur Web se produit généralement suite à l'un des événements suivants : la configuration réseau ou les propriétés de sécurité réseau ont été modifiées via l'interface utilisateur Web CMC ou RACADM ; la configuration du port de serveur Web a été modifiée via l'interface utilisateur Web ou RACADM ; CMC a été réinitialisé ou un nouveau certificat de serveur SSL a été téléversé.

 **REMARQUE** : pour modifier les paramètres des services, vous devez disposer du privilège **Administrateur de configuration du châssis**.

Pour configurer les services CMC :

1. Ouvrez une session sur l'interface Web de CMC.
2. Cliquez sur l'onglet **Réseau**.
3. Cliquez sur le sous-onglet **Services**. La page **Services** s'affiche.
4. Configurez les services suivants, si nécessaire :
 - 1 Console série CMC ([Tableau 5-50](#))
 - 1 Serveur Web ([Tableau 5-51](#))
 - 1 SSH ([Tableau 5-52](#))
 - 1 Telnet ([Tableau 5-53](#))
 - 1 RACADM distant ([Tableau 5-54](#))
 - 1 SNMP ([Tableau 5-55](#))
 - 1 Syslog distant ([Tableau 5-56](#))
5. Cliquez sur **Appliquer** pour mettre à jour l'ensemble des délais par défaut, ainsi que les délais maximaux.

Tableau 5-50. Paramètres de la console série CMC

Paramètre	Description
Activé	Active l'interface de la console Telnet sur CMC. Par défaut : décoché (désactivé)
Redirection activée	Active la redirection de la console série/texte vers le serveur via votre client série/Telnet/SSH à partir de CMC. CMC se

	<p>connecte à iDRAC qui, de façon interne, se connecte au port COM2 du serveur.</p> <p>Options de configuration : coché (activé), décoché (désactivé)</p> <p>Par défaut : coché (activé).</p>
Délai d'attente en cas d'inactivité	<p>Indique le nombre de secondes s'écoulant avant la déconnexion automatique d'une session série inactive. La modification du paramètre Délai d'attente prend effet à la prochaine ouverture de session. Elle n'affecte pas la session en cours.</p> <p>Plage du délai d'attente : de 0 ou 60 à 10 800 secondes. Pour désactiver la fonctionnalité du délai d'attente, entrez 0.</p> <p>Par défaut : 1 800 secondes.</p>
Débit en bauds	<p>Indique la vitesse des données sur le port série externe de CMC.</p> <p>Options de configuration : 9 600, 19 200, 28 800, 38 400, 57 600 et 115 200 b/s.</p> <p>Par défaut : 115 200 b/s</p>
Authentification désactivée	<p>Permet l'authentification de l'ouverture de session de la console série de CMC.</p> <p>Par défaut : décoché (désactivé)</p>
Touche Échap	<p>Vous permet de spécifier la séquence d'échappement qui met fin à la redirection de la console série/texte lorsque vous utilisez la commande connect ou racadm connect.</p> <p>Par défaut : ^\ (maintenir la touche <Ctrl> enfoncée et taper une barre oblique inverse (\\))</p> <p> REMARQUE : l'accent circonflexe représente la touche <Ctrl>.</p> <p>Options de configuration :</p> <ul style="list-style-type: none"> 1 valeur décimale (par exemple : 95) 1 valeur hexadécimale (par exemple : 0x12) 1 valeur octale (par exemple : 007) 1 valeur ASCII (par exemple : ^a) <p>Les valeurs ASCII peuvent être représentées à l'aide des codes suivants de touches d'échappement :</p> <ul style="list-style-type: none"> 1 Échap suivi par un caractère alphabétique (a-z, A-Z) 1 Échap suivi par les caractères spéciaux suivants : [] \ ^ _ 1 Longueur maximale autorisée : 4
Taille de la mémoire tampon de l'historique	<p>Indique la taille maximale de l'historique du tampon, qui contient les derniers caractères inscrits dans la console série.</p> <p>Par défaut : 8 192 caractères</p>
Commande d'ouverture de session	<p>Spécifie la commande série qui est exécutée automatiquement lorsqu'un utilisateur ouvre une session sur l'interface de la console série de CMC.</p> <p>Exemple : connect server-1</p> <p>Par défaut : [Null]</p>

Tableau 5-51. Paramètres du serveur Web

Paramètre	Description
Activé	<p>Active les services de Web Server (accès via distante RACADM distant et l'interface Web) pour CMC.</p> <p>Par défaut : coché (activé)</p>
Nombre maximal de sessions	<p>Indique le nombre maximal de sessions d'interface utilisateur Web simultanées autorisées pour le châssis. La modification de la propriété Nombre maximal de sessions prend effet à l'ouverture de session suivante. Elle n'affecte pas les sessions actives ouvertes (y compris la vôtre). RACADM distant n'est pas affecté par la propriété Nombre maximal de sessions de Web Server.</p> <p>Plage autorisée : 1 à 4</p> <p>Par défaut : 4</p> <p>REMARQUE : si vous définissez la propriété Nombre maximal de sessions sur une valeur inférieure au nombre actuel de sessions actives et que vous fermez ensuite la session, vous ne pourrez pas ouvrir de session avant la fermeture ou l'expiration des autres sessions.</p>
Délai d'attente en cas d'inactivité	<p>Indique le nombre de secondes avant qu'une session d'interface utilisateur Web inactive soit automatiquement déconnectée. La modification du paramètre Délai d'attente prend effet à la prochaine ouverture de session. Elle n'affecte pas la session en cours.</p> <p>Plage du délai d'attente : 60 à 10 800 secondes.</p> <p>Par défaut : 1 800 secondes.</p>

Numéro de port HTTP	<p>Indique le port par défaut utilisé par CMC pour écouter une connexion de serveur.</p> <p>REMARQUE : lorsque vous indiquez l'adresse HTTP dans le navigateur, Web Server la redirige automatiquement et utilise HTTPS.</p> <p>Si le numéro de port HTTP par défaut (80) a été modifié, vous devez inclure le numéro de port dans l'adresse du champ d'adresse du navigateur, comme indiqué ci-dessous :</p> <p style="text-align: center;"><code>http://<adresse IP>:<numéro de port></code></p> <p>où <i>adresse IP</i> correspond à l'adresse IP du châssis et <i>numéro de port</i> représente le numéro de port HTTP autre que le numéro par défaut (80).</p> <p>Plage de configuration : 10 à 65 535</p> <p>Par défaut : 80</p>
Numéro de port HTTPS	<p>Affiche le port par défaut utilisé par CMC pour écouter une connexion de serveur sécurisée.</p> <p>Si le numéro de port HTTPS par défaut (443) a été changé, vous devez inclure le numéro de port dans l'adresse du champ d'adresse du navigateur, comme indiqué ci-dessous :</p> <p style="text-align: center;"><code>https://<adresse IP>:<numéro de port></code></p> <p>où <i>adresse IP</i> correspond à l'adresse IP du châssis et <i>numéro de port</i> représente le numéro de port HTTP autre que le numéro par défaut (80).</p> <p>Plage de configuration : 10 à 65 535</p> <p>Par défaut : 443</p>

Tableau 5-52. Paramètres SSH

Paramètre	Description
Activé	<p>Permet d'utiliser SSH sur CMC.</p> <p>Par défaut : coché (activé)</p>
Nombre maximal de sessions	<p>Le nombre maximal de sessions SSH simultanées autorisées pour le châssis. La modification de cette propriété prend effet à la prochaine ouverture de session. Elle n'affecte pas les sessions actives ouvertes (y compris la vôtre).</p> <p>Plage de configuration : 1 à 4</p> <p>Par défaut : 4</p> <p>REMARQUE : si vous définissez la propriété Nombre maximal de sessions sur une valeur inférieure au nombre actuel de sessions actives et que vous fermez ensuite la session, vous ne pourrez pas ouvrir de session avant la fermeture ou l'expiration des autres sessions.</p>
Délai d'attente en cas d'inactivité	<p>Indique le nombre de secondes s'écoulant avant la déconnexion automatique d'une session SSH inactive. La modification du paramètre Délai d'attente prend effet à la prochaine ouverture de session. Elle n'affecte pas la session en cours.</p> <p>Plage du délai d'attente : 0 ou 60 à 10 800 secondes. Pour désactiver la fonctionnalité du délai d'attente, entrez 0.</p> <p>Par défaut : 1 800 secondes.</p>
Numéro de port	<p>Port utilisé par CMC pour écouter une connexion de serveur.</p> <p>Plage de configuration : 10 à 65 535</p> <p>Par défaut : 22</p>

Tableau 5-53. Paramètres Telnet

Paramètre	Description
Activé	<p>Active l'interface de la console Telnet sur CMC.</p> <p>Par défaut : décoché (désactivé)</p>
Nombre maximal de sessions	<p>Le nombre maximal de sessions Telnet simultanées autorisées pour le châssis. La modification de cette propriété prend effet à la prochaine ouverture de session. Elle n'affecte pas les sessions actives ouvertes (y compris la vôtre).</p> <p>Plage autorisée : 1 à 4</p>

	<p>Par défaut : 4</p> <p>REMARQUE : si vous définissez la propriété Nombre maximal de sessions sur une valeur inférieure au nombre actuel de sessions actives et que vous fermez ensuite la session, vous ne pourrez pas ouvrir de session avant la fermeture ou l'expiration des autres sessions.</p>
Délai d'attente en cas d'inactivité	<p>Indique le nombre de secondes s'écoulant avant la déconnexion automatique d'une session Telnet inactive. La modification du paramètre Délai d'attente prend effet à la prochaine ouverture de session. Elle n'affecte pas la session en cours.</p> <p>Plage du délai d'attente : 0 ou 60 à 10 800 secondes. Pour désactiver la fonctionnalité du délai d'attente, entrez 0.</p> <p>Par défaut : 1 800 secondes.</p>
Numéro de port	<p>Indique le port par défaut utilisé par CMC pour écouter une connexion de serveur.</p> <p>Par défaut : 23</p>

Tableau 5-54. Paramètres de RACADM distant

Paramètre	Description
Activé	<p>Permet à l'utilitaire RACADM distant d'accéder à CMC.</p> <p>Par défaut : coché (activé)</p>
Nombre maximal de sessions	<p>Le nombre maximal de sessions RACADM simultanées autorisées pour le châssis. La modification de cette propriété prend effet à la prochaine ouverture de session. Elle n'affecte pas les sessions actives ouvertes (y compris la vôtre).</p> <p>Plage autorisée : 1 à 4</p> <p>Par défaut : 4</p> <p>REMARQUE : si vous définissez la propriété Nombre maximal de sessions sur une valeur inférieure au nombre actuel de sessions actives et que vous fermez ensuite la session, vous ne pourrez pas ouvrir de session avant la fermeture ou l'expiration des autres sessions.</p>
Délai d'attente en cas d'inactivité	<p>Indique le nombre de secondes s'écoulant avant la déconnexion automatique d'une session racadm inactive. Toute modification du paramètre Délai d'attente en cas d'inactivité sera effective à la prochaine ouverture de session ; elle n'aura aucune incidence sur la session actuelle. Pour désactiver la fonctionnalité Délai d'attente en cas d'inactivité, entrez 0.</p> <p>Plage du délai d'attente : 0 ou 10 à 1 920 secondes. Pour désactiver la fonctionnalité du délai d'attente, entrez 0.</p> <p>Par défaut : 30 secondes</p>

Tableau 5-55. Configuration SNMP

Paramètre	Description
Activé	<p>Active SNMP sur CMC.</p> <p>Valeurs valides : coché (activé), décoché (désactivé)</p> <p>Par défaut : décoché (désactivé)</p>
Nom de communauté	Indique la chaîne de communauté utilisée pour obtenir des données du démon SNMP de CMC.

Tableau 5-56. Configuration de Syslog distant

Paramètre	Description
Activé	<p>Permet la transmission et la capture à distance des entrées du journal de CMC et du journal du matériel au(x) serveur(s) spécifié(s).</p> <p>Valeurs valides : coché (activé), décoché (désactivé)</p> <p>Par défaut : décoché (désactivé)</p>
Serveur Syslog 1	Le premier des trois serveurs possibles qui hébergera une copie des entrées du journal de CMC et du journal du matériel. Spécifié sous la forme d'un nom d'hôte, d'une adresse IPv6 ou d'une adresse IPv4.

Serveur Syslog 2	Le deuxième des trois serveurs possibles qui hébergera une copie des entrées du journal de CMC et du journal du matériel. Spécifié sous la forme d'un nom d'hôte, d'une adresse IPv6 ou d'une adresse IPv4.
Serveur Syslog 3	Le troisième des trois serveurs possibles qui hébergera une copie des entrées du journal de CMC et du journal du matériel. Spécifié sous la forme d'un nom d'hôte, d'une adresse IPv6 ou d'une adresse IPv4.
Numéro de port Syslog	Spécifie le numéro de port sur le serveur distant pour recevoir une copie des entrées du journal de CMC et du journal du matériel. Le même numéro de port est utilisé pour les trois serveurs. Un numéro de port syslog valide est compris entre 10 et 65 535. Par défaut : 514

Configuration des bilans de puissance

CMC vous permet d'établir un bilan de puissance et de gérer l'alimentation du châssis. Le service de gestion de l'alimentation optimise la puissance consommée et réaffecte l'alimentation aux différents modules en fonction de la demande.

Pour des instructions sur la configuration de l'alimentation via CMC, voir [Configuration et gestion de l'alimentation](#).

Pour plus d'informations sur le service de gestion de l'alimentation de CMC, voir [Gestion de l'alimentation](#).

Gestion des mises à jour du micrologiciel

Cette section décrit comment utiliser l'interface Web pour mettre à jour le micrologiciel. Les composants suivants peuvent être mis à jour à l'aide de l'interface utilisateur ou de commandes RACADM :

- 1 CMC : principal et secondaire
- 1 Module iKVM
- 1 iDRAC
- 1 Périphériques d'infrastructure du module d'E/S

Lors de la mise à jour du micrologiciel, il convient de suivre la procédure recommandée, qui permet de prévenir une perte du service en cas d'échec de la mise à jour. Voir [Installation ou mise à jour du micrologiciel du module CMC](#) pour obtenir des conseils avant d'utiliser les instructions de cette section.

Affichage des versions actuelles du micrologiciel

La page Mise à jour affiche la version actuelle de tous les châssis de composants actualisables. Peuvent être inclus : le micrologiciel iKVM, le micrologiciel du contrôleur CMC principal et, le cas échéant, le micrologiciel du contrôleur CMC de secours, le micrologiciel iDRAC et le micrologiciel de périphérique d'infrastructure du module d'E/S. Pour plus d'informations, voir [Mise à jour du micrologiciel du périphérique d'infrastructure du module d'E/S](#).

Pour ouvrir une page de mise à jour pour certains dispositifs :

1. Cliquez sur le nom du dispositif ou cochez la case **Sélectionner / Désélectionner tout**.
2. Cliquez sur **Appliquer la mise à jour**.

Une page de mise à jour pour les dispositifs sélectionnés s'affiche.

Si le châssis renferme un serveur de génération antérieure avec iDRAC en mode de récupération ou si CMC détecte que le micrologiciel de l'iDRAC est endommagé, alors le module iDRAC de génération antérieure est également répertorié dans la page Mise à jour du micrologiciel. Voir [Récupération du micrologiciel iDRAC à l'aide de CMC](#) pour les étapes à suivre afin de récupérer le micrologiciel iDRAC à l'aide de CMC.

Pour afficher les composants du châssis pouvant être mis à jour :

1. Connectez-vous à l'interface Web. Pour plus d'informations, voir [Accès à l'interface Web CMC](#).
2. Cliquez sur **Présentation du châssis** dans l'arborescence.
3. Cliquez sur l'onglet **Update** (Mise à jour). La page **Mise à jour du micrologiciel** s'affiche.

Pour afficher les composants de serveur actualisables :

1. Connectez-vous à l'interface Web. Pour plus d'informations, voir [Accès à l'interface Web CMC](#).
2. Cliquez sur **Présentation des serveurs** dans l'arborescence.
3. Cliquez sur l'onglet **Update** (Mise à jour). La **Mise à jour du composant du serveur** s'affiche.

Mise à jour du micrologiciel

-  **REMARQUE** : pour mettre à jour le micrologiciel sur CMC, vous devez disposer du privilège **Administrateur de configuration du châssis**.
-  **REMARQUE** : la mise à jour de micrologiciel conserve les paramètres CMC et iKVM actuels.
-  **REMARQUE** : si une session de l'interface utilisateur Web est utilisée pour mettre à jour le micrologiciel d'un composant système, le paramètre **Délai d'attente** en cas d'inactivité doit être supérieur au délai de transfert du fichier. Dans certains cas, le transfert du fichier du micrologiciel peut prendre jusqu'à 30 minutes. Pour définir la valeur **Délai d'attente en cas d'inactivité**, voir [Configuration des services](#).

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 à la dernière révision. Pour mettre à jour les micrologiciels des périphériques, procédez comme suit :

- 1 Sélectionnez les périphériques à mettre à jour.
- 1 Cliquez sur le bouton **Appliquer** sous le groupement.
- 1 Cliquez sur **Naviguer** pour sélectionner l'image du micrologiciel.
- 1 Cliquez sur **Commencer la mise à jour de micrologiciel** pour démarrer le processus de mise à jour. Le message **Transfert en cours de l'image de fichier** s'affiche, suivi par une page d'état de l'avancement.

-  **REMARQUE** : vérifiez que vous disposez de la dernière version du micrologiciel. Vous pouvez télécharger la dernière version du fichier image du micrologiciel sur le site Web du support de Dell à l'adresse support.dell.com.

Mise à jour du micrologiciel du contrôleur CMC

-  **REMARQUE** : lorsqu'une mise à jour du micrologiciel d'un contrôleur CMC ou d'un module iDRAC est en cours sur un serveur, une partie ou l'ensemble des unités de ventilation du châssis fonctionne à 100 %. Ce comportement est normal.
-  **REMARQUE** : une fois le micrologiciel correctement téléversé, CMC principal se réinitialise et devient temporairement indisponible. Si un contrôleur CMC secondaire est présent, les rôles de CMC principal et secondaire permutent. Le contrôleur CMC secondaire devient le contrôleur CMC principal. Si une mise à jour est appliquée uniquement au contrôleur CMC actif (principal), ce dernier n'exécute pas l'image mise à jour après sa réinitialisation ; seul le contrôleur CMC de secours (secondaire) dispose de cette image. En général, il est vivement recommandé de maintenir des versions identiques du micrologiciel pour le contrôleur CMC secondaire et le contrôleur CMC principal.
-  **REMARQUE** : pour éviter de déconnecter d'autres utilisateurs au cours d'une réinitialisation, avertissez les utilisateurs autorisés susceptibles de se connecter à CMC et recherchez les sessions actives affichées dans la page **Sessions**. Pour ouvrir la page **Sessions**, sélectionnez **Châssis** dans l'arborescence, cliquez sur l'onglet **Réseau**, puis sur le sous-onglet **Sessions**. L'aide relative à cette page est disponible via le lien **Aide** en haut à droite de la page.
-  **REMARQUE** : lors du transfert de fichiers vers et à partir de CMC, l'icône de transfert de fichiers tourne. Si votre icône est inactive, vérifiez que votre navigateur est configuré pour autoriser les animations. Voir [Autorisation des animations dans Internet Explorer](#) pour des instructions.
-  **REMARQUE** : si vous rencontrez des problèmes lors du téléchargement de fichiers à partir de CMC dans Internet Explorer, activez l'option **Ne pas enregistrer les pages cryptées sur le disque**. Voir [Téléchargement de fichiers à partir de CMC dans Internet Explorer](#) pour des instructions.

Mise à jour du micrologiciel CMC

1. Dans la page **Mise à jour du micrologiciel**, sélectionnez le ou les modules CMC à mettre à jour en cochant la case **Mettre à jour les cibles**. Il est possible de mettre à jour simultanément les deux modules CMC.
2. Cliquez sur le bouton **Appliquer la mise à jour CMC** sous la liste des composants CMC.
 -  **REMARQUE** : le nom par défaut de l'image du micrologiciel de CMC est **firmimg.cmc**. Le micrologiciel de CMC doit être mis à jour en premier, avant le périphérique d'infrastructure du module d'E/S.
3. Dans le champ **Image de micrologiciel**, entrez le chemin du fichier image du micrologiciel sur votre station de gestion ou votre réseau partagé ou cliquez sur **Parcourir** pour accéder à l'emplacement du fichier.
4. Cliquez sur **Commencer la mise à jour de micrologiciel**. La section **Avancement de la mise à jour du micrologiciel** fournit des informations sur l'état de la mise à jour du micrologiciel. Un indicateur d'état s'affiche sur la page pendant le chargement du fichier image. La durée du transfert de fichiers peut fortement varier en fonction de la vitesse de la connexion. Lorsque le processus de mise à jour interne démarre, la page s'actualise automatiquement et l'horloge de mise à jour du micrologiciel s'affiche. Instructions supplémentaires à suivre :
 - 1 N'utilisez pas le bouton **Actualiser** et ne naviguez pas sur une autre page pendant le transfert.
 - 1 Pour annuler le processus, cliquez sur **Annuler le transfert du fichier et la mise à jour**. Cette option n'est disponible que pendant le transfert du fichier.
 - 1 L'état de la mise à jour s'affiche dans le champ **État de mise à jour**. Ce champ est mis à jour automatiquement pendant le transfert du fichier.

-  **REMARQUE** : la mise à jour de CMC peut prendre plusieurs minutes.

5. Pour un CMC de secours (secondaire), le champ **État de la mise à jour** affiche « Terminé » lorsque la mise à jour est terminée. Pour un CMC actif (principal), la session du navigateur et la connexion à CMC sont perdues temporairement pendant la mise hors tension de CMC au cours des dernières étapes de la mise à jour du micrologiciel. Vous devez rouvrir une session quelques minutes plus tard, lorsque le contrôleur CMC actif a redémarré.

Après la réinitialisation de CMC, le nouveau micrologiciel est affiché sur la page **Mise à jour du micrologiciel**.

-  **REMARQUE** : après la mise à niveau du micrologiciel, videz la mémoire cache du navigateur Web. Consultez l'aide en ligne de votre navigateur pour des instructions sur le vidage de la mémoire cache.

Mise à jour du micrologiciel du module iKVM

 **REMARQUE** : après le chargement du micrologiciel, le module iKVM est réinitialisé et devient temporairement indisponible.

1. Ouvrez à nouveau une session dans l'interface Web CMC.
2. Cliquez sur **Présentation du châssis** dans l'arborescence.
3. Cliquez sur l'onglet **Update** (Mise à jour). La page **Mise à jour du micrologiciel** s'affiche.
4. Sélectionnez le composant iKVM à mettre à jour en cochant la case **Mettre à jour les cibles** pour ce composant iKVM.
5. Cliquez sur le bouton **Appliquer la mise à jour iKVM** sous la liste des composants iKVM.
6. Dans le champ **Image de micrologiciel**, entrez le chemin du fichier image du micrologiciel sur votre station de gestion ou votre réseau partagé ou cliquez sur **Parcourir** pour accéder à l'emplacement du fichier.

 **REMARQUE** : le nom de l'image par défaut du micrologiciel iKVM est `ikvm.bin`. Cependant, vous pouvez modifier ce nom pour éviter toute confusion avec les images précédentes.

7. Cliquez sur **Commencer la mise à jour de micrologiciel**.
8. Cliquez sur **Yes (Oui)** pour continuer. La section **Avancement de la mise à jour du micrologiciel** fournit des informations sur l'état de la mise à jour du micrologiciel. Un indicateur d'état s'affiche sur la page pendant le chargement du fichier image. La durée du transfert de fichiers peut fortement varier en fonction de la vitesse de la connexion. Lorsque le processus de mise à jour interne démarre, la page s'actualise automatiquement et l'horloge de mise à jour du micrologiciel s'affiche. Instructions supplémentaires à suivre :
 1. N'utilisez pas le bouton **Actualiser** et ne naviguez pas sur une autre page pendant le transfert.
 1. Pour annuler le processus, cliquez sur **Annuler le transfert du fichier et la mise à jour**. Cette option n'est disponible que pendant le transfert du fichier.
 1. L'état de la mise à jour s'affiche dans le champ **État de mise à jour**. Ce champ est mis à jour automatiquement pendant le transfert du fichier.

 **REMARQUE** : la mise à jour d'iKVM peut prendre jusqu'à deux minutes.

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

Mise à jour du micrologiciel du périphérique d'infrastructure du module d'E/S

En effectuant cette mise à jour, le micrologiciel pour un composant de périphérique du module d'E/S est mis à jour, mais pas le micrologiciel du périphérique du module d'E/S lui-même ; le composant est l'ensemble de circuits d'interface entre le périphérique du module d'E/S et CMC. L'image de mise à jour pour le composant réside dans le système de fichiers CMC ; quant au composant, il est affiché comme périphérique actualisable sur l'interface utilisateur Web de CMC uniquement si la révision actuelle du composant et l'image du composant sur CMC ne correspondent pas.

1. Ouvrez à nouveau une session dans l'interface Web CMC.
2. Cliquez sur **Présentation du châssis** dans l'arborescence.
3. Cliquez sur l'onglet **Update** (Mise à jour). La page **Mise à jour du micrologiciel** s'affiche.
4. Sélectionnez le périphérique du module d'E/S à mettre à jour en cochant la case **Mettre à jour les cibles** pour ce périphérique du module d'E/S.
5. Cliquez sur le bouton **Appliquer la mise à jour IOM** sous la liste des composants IOM.

 **REMARQUE** : le champ **Image de micrologiciel** n'apparaît pas pour une cible de périphérique d'infrastructure du module d'E/S (IOMINF) car l'image requise se trouve sur CMC. Le micrologiciel CMC doit être mis à jour en premier, avant le micrologiciel IOMINF.

Les mises à jour d'IOMINF sont autorisées par CMC s'il détecte que le micrologiciel IOMINF est obsolète avec l'image contenue dans le système de fichiers CMC. Si le micrologiciel IOMINF est récent, CMC empêche les mises à jour d'IOMINF. Les périphériques IOMINF récents doivent être répertoriés en tant que périphériques pouvant être mis à jour.

6. Cliquez sur **Commencer la mise à jour de micrologiciel**. La section **Avancement de la mise à jour du micrologiciel** fournit des informations sur l'état de la mise à jour du micrologiciel. Un indicateur d'état s'affiche sur la page pendant le chargement du fichier image. La durée du transfert de fichiers peut fortement varier en fonction de la vitesse de la connexion. Lorsque le processus de mise à jour interne démarre, la page s'actualise automatiquement et l'horloge de mise à jour du micrologiciel s'affiche. Instructions supplémentaires à suivre :
 1. N'utilisez pas le bouton **Actualiser** et ne naviguez pas vers une autre page pendant le transfert de fichiers.
 1. L'état de la mise à jour s'affiche dans le champ **État de mise à jour**. Ce champ est mis à jour automatiquement pendant le transfert du fichier.

 **REMARQUE** : aucun décompte du temps de transfert ne s'affiche lors de la mise à jour du micrologiciel IOMINF. La mise à jour entraîne une courte perte de la connectivité au périphérique du module d'E/S, car ce dernier redémarre à la fin du processus. Lorsque la mise à jour est terminée, le nouveau micrologiciel est affiché et le système mis à jour n'est plus présent sur la page **Mise à jour du micrologiciel**.

Mise à jour du micrologiciel iDRAC du serveur

 **REMARQUE** : iDRAC (sur un serveur) se réinitialise et est temporairement indisponible après le chargement des mises à jour du micrologiciel.

 **REMARQUE** : la version du micrologiciel iDRAC doit être la version 1.4 ou une version ultérieure pour les serveurs disposant d'iDRAC, ou la version 2.0 ou une version ultérieure pour les serveurs sur lesquels iDRAC6 Enterprise est installé.

1. Ouvrez à nouveau une session dans l'interface Web CMC.
2. Cliquez sur **Présentation du châssis** dans l'arborescence.
3. Cliquez sur l'onglet **Update** (Mise à jour). La page **Mise à jour du micrologiciel** s'affiche.
4. Sélectionnez le ou les périphériques iDRAC à mettre à jour en cochant la case **Mettre à jour les cibles** pour ces périphériques.
5. Cliquez sur le bouton **Appliquer la mise à jour iDRAC** sous la liste des composants iDRAC.
6. Dans le champ **Image de micrologiciel**, entrez le chemin du fichier image du micrologiciel sur votre station de gestion ou votre réseau partagé ou cliquez sur **Parcourir** pour accéder à l'emplacement du fichier.
7. Cliquez sur **Commencer la mise à jour de micrologiciel**. La section **Avancement de la mise à jour du micrologiciel** fournit des informations sur l'état de la mise à jour du micrologiciel. Un indicateur d'état s'affiche sur la page pendant le chargement du fichier image. La durée du transfert de fichiers peut fortement varier en fonction de la vitesse de la connexion. Lorsque la procédure de mise à jour interne démarre, la page s'actualise automatiquement et l'horloge de mise à jour du micrologiciel s'affiche. Instructions supplémentaires à suivre :
 - 1 N'utilisez pas le bouton **Actualiser** et ne naviguez pas vers une autre page pendant le transfert de fichiers.
 - 1 Pour annuler le processus, cliquez sur **Annuler le transfert du fichier et la mise à jour**. Cette option n'est disponible que pendant le transfert du fichier.
 - 1 L'état de la mise à jour s'affiche dans le champ **État de mise à jour**. Ce champ est mis à jour automatiquement pendant le transfert du fichier.

 **REMARQUE** : la mise à jour peut prendre plusieurs minutes pour CMC ou le serveur.

Récupération du micrologiciel iDRAC à l'aide de CMC

Le micrologiciel iDRAC est généralement mis à jour à l'aide des fonctionnalités iDRAC telles que l'interface Web iDRAC, l'interface de ligne de commande SM-CLP ou les progiciels de mise à jour spécifiques aux systèmes d'exploitation téléchargés sur le site support.dell.com. Consultez le *Guide d'utilisation du micrologiciel iDRAC* pour des instructions de mise à jour du micrologiciel iDRAC.

Les générations initiales de serveurs peuvent avoir des micrologiciels corrompus récupérés par le nouveau processus de micrologiciel iDRAC de mise à jour. Lorsque CMC détecte un micrologiciel iDRAC corrompu, il répertorie le serveur dans la page **Mise à jour du micrologiciel**.

Suivez les étapes suivantes pour mettre à jour le micrologiciel iDRAC.

1. Téléchargez la dernière version du micrologiciel iDRAC sur votre ordinateur de gestion depuis l'adresse support.dell.com.
2. Ouvrez une session sur l'interface Web (voir [Accès à l'interface Web CMC](#)).
3. Cliquez sur **Présentation du châssis** dans l'arborescence.
4. Cliquez sur l'onglet **Update** (Mise à jour). La page **Mise à jour du micrologiciel** s'affiche.
5. Sélectionnez le ou les contrôleurs iDRAC à mettre à jour en cochant la case **Mettre à jour les cibles** pour ces périphériques.
6. Cliquez sur le bouton **Appliquer la mise à jour iDRAC** sous la liste des composants iDRAC.
7. Cliquez sur **Parcourir**, naviguez vers l'image du micrologiciel iDRAC que vous avez téléchargée et cliquez sur **Ouvrir**.

 **REMARQUE** : le nom par défaut de l'image du micrologiciel iDRAC est `firmimg.imc`. Le micrologiciel de CMC doit être mis à jour en premier, avant le périphérique d'infrastructure du module d'E/S.

8. Cliquez sur **Commencer la mise à jour de micrologiciel**. Instructions supplémentaires à suivre :
 - 1 N'utilisez pas le bouton **Actualiser** et ne naviguez pas vers une autre page pendant le transfert de fichiers.
 - 1 Pour annuler le processus, cliquez sur **Annuler le transfert du fichier et la mise à jour**. Cette option n'est disponible que pendant le transfert du fichier.
 - 1 L'état de la mise à jour s'affiche dans le champ **État de mise à jour**. Ce champ est mis à jour automatiquement pendant le transfert du fichier.

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

Gestion iDRAC

CMC fournit une page Déployer iDRAC pour permettre à l'utilisateur de définir les paramètres de configuration de réseau iDRAC pour les serveurs, qu'ils soient déjà installés ou nouvellement insérés. Un utilisateur peut configurer un ou plusieurs périphériques iDRAC installés à partir de cette page. L'utilisateur peut également définir les paramètres de configuration réseau iDRAC par défaut et le mot de passe racine pour les serveurs qui seront installés ultérieurement ; ces paramètres par défaut sont les paramètres **iDRAC QuickDeploy**.

Pour plus d'informations sur le comportement iDRAC, consultez les *Guides d'utilisation d'iDRAC* sur le site Web du support de Dell à l'adresse support.dell.com/manuals.

iDRAC QuickDeploy

La section **iDRAC QuickDeploy** de la page **Déployer iDRAC** contient les paramètres de configuration de réseau qui sont appliqués aux serveurs nouvellement insérés. Vous pouvez utiliser ces paramètres pour remplir automatiquement le tableau **Paramètres réseau iDRAC** qui se trouve sous la section QuickDeploy. Une fois que QuickDeploy est activé, les paramètres QuickDeploy sont appliqués aux serveurs après avoir été installés. Voir l'étape 8 dans [Configuration de la mise en réseau à l'aide de l'assistant de configuration de l'écran LCD](#) pour plus d'informations sur les paramètres iDRAC QuickDeploy.

Procédez comme suit pour activer et définir les paramètres **iDRAC QuickDeploy** :

1. Ouvrez une session sur l'interface Web de CMC.
2. Cliquez sur **Présentation des serveurs** dans l'arborescence.
3. Cliquez sur l'onglet **Configuration**. La page **Déployer iDRAC** apparaît.
4. Définissez les paramètres QuickDeploy en conséquence.

Tableau 5-57. Paramètres QuickDeploy

Paramètre	Description
QuickDeploy activé	Active/désactive la fonctionnalité QuickDeploy qui applique automatiquement les paramètres iDRAC configurés sur cette page aux serveurs nouvellement installés ; la configuration automatique <i>doit</i> être confirmée localement sur l'écran LCD. 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 : décoché (désactivé)
Définir le mot de passe racine d'iDRAC sur l'insertion de serveur	Spécifie si le mot de passe racine d'iDRAC du serveur doit être remplacé par la valeur fournie dans la boîte de dialogue Mot de passe racine iDRAC lorsque le serveur est inséré.
Mot de passe racine d'iDRAC	Lorsque les cases Définir le mot de passe racine d'iDRAC lors de l'insertion de serveur et QuickDeploy activé sont cochées, cette valeur de mot de passe est assignée au mot de passe de l'utilisateur racine iDRAC d'un serveur dès que ce dernier est inséré dans le châssis. Le mot de passe peut contenir entre 1 et 20 caractères imprimables (y compris les espaces).
Confirmer le mot de passe racine d'iDRAC.	Vérifie le mot de passe entré dans le champ Mot de passe racine d'iDRAC .
Activer le réseau local d'iDRAC	Active/désactive le canal de réseau local d'iDRAC. Par défaut : décoché (désactivé)
Activer IPv4 pour iDRAC	Active/Désactive IPv4 sur iDRAC. Le paramètre par défaut est activé.
Activer IPMI sur le réseau local d'iDRAC	Active/désactive le canal IPMI sur le réseau local pour chaque iDRAC présent dans le châssis. Par défaut : décoché (désactivé)
Activer DHCP pour iDRAC	Active/désactive DHCP pour chaque iDRAC présent dans le châssis. Si cette option est activée, les champs IP QuickDeploy , Masque de sous-réseau QuickDeploy et Passerelle QuickDeploy sont désactivés et ne peuvent pas être modifiés étant donné que DHCP assigne automatiquement ces paramètres pour chaque iDRAC. Par défaut : décoché (désactivé)
Démarrage de l'adresse IPv4 iDRAC (logement 1)	Spécifie l'adresse IP statique d'iDRAC du serveur dans le logement 1 de l'enceinte. L'adresse IP de chaque iDRAC suivant est incrémenté de un pour chaque logement à partir de l'adresse IP statique du logement 1. Si la somme de l'adresse IP et du numéro du logement est supérieure au masque de sous-réseau, un message d'erreur s'affiche. REMARQUE : le masque de sous-réseau et la passerelle ne sont pas incrémentés comme l'adresse IP. Par exemple, si l'adresse IP de début est 192.168.0.250 et que le masque de sous-réseau est 255.255.0.0, alors l'adresse IP QuickDeploy pour le logement 15 est 192.168.0.265. Si le masque de sous-réseau est 255.255.255.0, le message d'erreur La plage de l'adresse IP QuickDeploy n'est pas contenue dans le sous-réseau QuickDeploy s'affiche lorsque vous appuyez sur l'un des boutons Enregistrer les paramètres QuickDeploy ou Ajouter automatiquement avec les paramètres QuickDeploy .
Masque de sous-réseau IPv4 d'iDRAC	Spécifie le masque de sous-réseau QuickDeploy étant 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 iDRAC présent dans le châssis qui possède la capacité IPv6.
Activer la configuration automatique IPv6 d'iDRAC	Active iDRAC pour obtenir les paramètres IPv6 (adresse et longueur de préfixe) auprès d'un serveur DHCPv6 et autorise également la configuration automatique des adresses statiques. Le paramètre par défaut est activé.
Passerelle IPv6 d'iDRAC	Spécifie la passerelle IPv6 par défaut devant être assignée aux iDRAC. Le paramètre par défaut est « :: ».
Longueur de préfixe IPv6 iDRAC	Spécifie la longueur de préfixe devant être assignée pour les adresses IPv6 sur iDRAC. Le paramètre par défaut est 64.

- Pour enregistrer les sélections, cliquez sur le bouton **Enregistrer les paramètres QuickDeploy**. Si vous avez modifié les paramètres réseau iDRAC, cliquez sur le bouton **Appliquer les paramètres réseau d'iDRAC** pour déployer les paramètres sur iDRAC.
- Pour mettre à jour le tableau avec les derniers paramètres QuickDeploy activé enregistrés et restaurer les paramètres réseau iDRAC sur les valeurs actuelles pour chaque serveur installé, cliquez sur **Actualiser**.

 **REMARQUE** : si vous cliquez sur le bouton **Actualiser**, tous les paramètres de configuration réseau d'iDRAC QuickDeploy et d'iDRAC qui n'ont pas été enregistrés seront supprimés.

La fonctionnalité QuickDeploy est exécutée seulement si elle est activée et si un serveur est inséré dans le châssis. Si les cases **Définir le mot de passe racine iDRAC dans l'insertion de serveur** et **QuickDeploy activé** sont cochées, l'utilisateur est invité via l'interface LCD à autoriser ou non la modification du mot de passe. Si certains paramètres de configuration réseau diffèrent des paramètres iDRAC actuels, l'utilisateur peut accepter ou refuser les modifications.

 **REMARQUE** : s'il y a une différence par rapport au réseau local ou réseau local sur IPMI, l'utilisateur est invité à accepter le paramètre de l'adresse IP de déploiement rapide. Si la différence est le paramètre DHCP, l'utilisateur est invité à accepter le paramètre QuickDeploy DHCP.

Pour copier les paramètres QuickDeploy dans la section **Paramètres réseau d'iDRAC**, cliquez sur **Ajouter automatiquement avec les paramètres QuickDeploy**. Les paramètres de configuration réseau QuickDeploy sont copiés dans les champs correspondants du tableau **Paramètres de configuration réseau d'iDRAC**.

 **REMARQUE** : les modifications apportées aux champs de QuickDeploy sont immédiates. Cependant, les modifications qui sont apportées à un ou plusieurs paramètres de configuration réseau de serveur iDRAC risquent de prendre quelques minutes pour être propagées de CMC à iDRAC. Si vous appuyez trop tôt sur le bouton **Actualiser**, des données partiellement correctes pour un ou plusieurs serveurs iDRAC seront affichées.

Paramètres réseau d'iDRAC

La section **Paramètres réseau d'iDRAC** de la page **Déployer iDRAC** contient un tableau énumérant les paramètres de configuration réseau IPv4 et IPv6 d'iDRAC de tous les serveurs installés. En utilisant ce tableau, vous pouvez configurer les paramètres de configuration réseau d'iDRAC pour chaque serveur installé. Les valeurs initiales affichées dans chaque champ correspondent aux valeurs actuelles provenant d'iDRAC. Lorsque vous modifiez un champ et que vous cliquez sur **Appliquer les paramètres réseau d'iDRAC**, le champ modifié est enregistré sur iDRAC. Procédez comme suit pour activer et définir les **Paramètres réseau d'iDRAC** :

- Ouvrez une session sur l'interface Web de CMC.
- Cliquez sur **Présentation des serveurs** dans l'arborescence.
- Cliquez sur l'onglet **Configuration**.
La page **Déployer iDRAC** apparaît.
- Cochez la case **Déploiement rapide activé** pour activer les paramètres de déploiement rapide.
- Définissez les **Paramètres réseau d'iDRAC** en conséquence.

Tableau 5-58. Paramètres réseau d'iDRAC

Paramètre	Description
Ordre de priorité	Indique le logement occupé par le serveur du châssis. Les numéros de logement sont des numéros séquentiels, qui vont de 1 à 16 (16 logements sont disponibles dans le châssis), qui permettent d'identifier l'emplacement des serveurs dans le châssis. REMARQUE : lorsqu'il y a moins de 16 serveurs dans les logements, seuls les logements avec serveur sont affichés.
Nom	Affiche le nom du serveur présent dans chaque logement. Par défaut, les logements sont nommés SLOT-01 à SLOT-16 . REMARQUE : le nom d'un logement ne peut être vide ou NUL.
Activer le réseau local	Active (coché) ou désactive (décoché) le canal de réseau local. REMARQUE : lorsque le réseau local n'est pas sélectionné (désactivé), aucun autre paramètre de configuration réseau (IPMI sur réseau local, DHCP, Masque de sous-réseau de l'adresse IP et Passerelle) n'est utilisé. Ces champs ne sont pas

	accessibles.
Modifier le mot de passe racine	Permet (lorsque la case est cochée) de pouvoir modifier le mot de passe de l'utilisateur racine iDRAC. Les champs Mot de passe racine d'iDRAC et Confirmer le mot de passe racine d'iDRAC doivent être remplis pour réussir cette opération.
DHCP	S'il est sélectionné, le protocole DHCP est utilisé pour acquérir l'adresse IP, le masque de sous-réseau et la passerelle par défaut d'iDRAC ; sinon, les valeurs définies dans les champs de configuration réseau d'iDRAC sont utilisées. Le réseau local doit être activé pour définir ce champ.
IPMI sur le LAN	Active (case cochée) ou désactive (case décochée) le canal réseau local d'IPMI. Le réseau local doit être activé pour définir ce champ.
Adresse IP	Adresse IPv4 ou IPv6 statique assignée à iDRAC situé dans ce logement.
Masque de sous-réseau	Spécifie le masque de sous-réseau assigné au module iDRAC installé dans ce logement.
Passerelle	Spécifie la passerelle par défaut assignée au module iDRAC qui sera installé dans ce logement.
Activer IPv4	Active iDRAC dans le logement pour utiliser le protocole IPv4 sur le réseau. Vous devez sélectionner l'option Activer le réseau local pour que cette option soit active. Le paramètre par défaut est activé.
Activer IPv6	Active iDRAC dans le logement pour utiliser le protocole IPv6 sur le réseau. Vous devez sélectionner l'option Activer le réseau local et désélectionner l'option Configuration automatique pour que cette option soit active. Le paramètre par défaut est désactivé. REMARQUE : cette option est disponible uniquement si le serveur possède la capacité IPv6.
Configuration automatique	Active iDRAC pour obtenir les paramètres IPv6 (adresse et longueur de préfixe) auprès d'un serveur DHCPv6 et autorise également la configuration automatique des adresses statiques. REMARQUE : cette option est disponible uniquement si le serveur possède la capacité IPv6.
Longueur du préfixe	Spécifie la longueur, en bits, du sous-réseau IPv6 auquel appartient cet iDRAC.

- Pour déployer le paramètre sur iDRAC, cliquez sur le bouton **Appliquer les paramètres réseau d'iDRAC**. Si vous avez modifié les paramètres de déploiement rapide, ceux-ci seront également enregistrés.
- Pour restaurer les paramètres réseau d'iDRAC sur les valeurs actuelles de chaque serveur installé et pour mettre à jour le tableau Déploiement rapide avec les derniers paramètres de déploiement rapide enregistrés, cliquez sur **Actualiser**.

 **REMARQUE** : si vous cliquez sur le bouton **Actualiser**, tous les paramètres de configuration de déploiement rapide d'iDRAC et réseau d'iDRAC qui n'ont pas été enregistrés sont supprimés.

Le tableau **Paramètres réseau d'iDRAC** reflète les paramètres de configuration réseau futurs ; les valeurs affichées pour les lames installées peuvent ou non être les mêmes que les paramètres de configuration réseau d'iDRAC installés actuellement. Après avoir apporté des modifications, appuyez sur le bouton **Actualiser** pour mettre à jour la page **Déployer iDRAC** avec les paramètres de configuration réseau de chaque iDRAC installé.

 **REMARQUE** : les modifications apportées aux champs de QuickDeploy sont immédiates. Cependant, les modifications qui sont apportées à un ou plusieurs paramètres de configuration réseau de serveur iDRAC risquent de prendre quelques minutes pour être propagées de CMC à iDRAC. Si vous appuyez trop tôt sur le bouton **Actualiser**, des données partiellement correctes pour un ou plusieurs serveurs iDRAC s'afficheront.

Lancement de la console à distance depuis l'interface utilisateur de CMC

Cette fonctionnalité vous permet de lancer une session clavier-écran-souris directement sur le serveur.

Pour lancer la console à distance depuis la page d'accueil de l'interface utilisateur de CMC :

- Cliquez sur le serveur spécifié dans le graphique du châssis.
- Dans **Liens rapides**, cliquez sur le lien **Lancer la console distante**.

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

- Dans l'arborescence du système, sélectionnez **Présentation des serveurs**.
- Cliquez sur **Lancer la console distante** dans le tableau pour le serveur spécifié.

Pour lancer une console distante de serveur pour une personne :

- Développez **Présentation des serveurs** dans l'arborescence. Tous les serveurs (1 à 16) s'affichent dans la liste développée des serveurs.
- Dans l'arborescence du système, cliquez sur le serveur que vous souhaitez afficher. La page **Condition du serveur** s'affiche.
- Cliquez sur **Lancer la console distante**.

La fonctionnalité de console distante est prise en charge uniquement lorsque toutes les conditions suivantes sont remplies :

- Le châssis est sous tension.

- 1 Le serveur est PowerEdge M610, M610X, M710, M710HD ou M910.
- 1 L'interface de réseau local sur le serveur est activée.
- 1 La version d'iDRAC est 2.20 ou ultérieure.
- 1 Le système hôte dispose du JRE (Java Runtime Environment) 6 Update 16 ou ultérieur.
- 1 Le navigateur sur le système hôte autorise les fenêtres contextuelles (le blocage de fenêtres contextuelles est désactivé).

 **REMARQUE** : la console distante peut également être lancée depuis l'interface graphique d'iDRAC. Voir l'interface graphique d'iDRAC pour plus de détails.

Lancement d'iDRAC en utilisant une signature unique

CMC fournit une gestion limitée des composants individuels du châssis, tels que les serveurs. Pour une gestion complète de ces composants individuels, CMC fournit un point de lancement de l'interface Web du contrôleur de gestion (iDRAC) du serveur.

Pour lancer la console de gestion iDRAC depuis la page **Serveurs** :

1. Ouvrez une session sur l'interface Web de CMC.
2. Cliquez sur **Présentation des serveurs** dans l'arborescence. La page **État des serveurs** s'affiche.
3. Cliquez sur l'icône **Lancer l'interface utilisateur iDRAC** pour le serveur que vous voulez gérer.

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

1. Ouvrez une session sur l'interface Web de CMC.
2. Développez **Présentation des serveurs** dans l'arborescence. Tous les serveurs (1 à 16) s'affichent dans la liste développée **Serveurs**.
3. Cliquez sur le serveur dont vous souhaitez afficher les informations. La page **Condition du serveur** s'affiche.
4. Cliquez sur l'icône **Lancer l'interface utilisateur iDRAC**.

Un utilisateur peut lancer l'interface utilisateur iDRAC sans avoir à ouvrir une session une deuxième fois, étant donné que cette fonctionnalité utilise l'authentification unique. Les stratégies de connexion directe sont décrites ci-dessous.

- 1 Un utilisateur CMC ayant un privilège administratif sur le serveur sera automatiquement connecté à iDRAC à l'aide de l'authentification unique. Une fois sur le site iDRAC, les privilèges administrateur sont automatiquement accordés à cet utilisateur. Cela est vrai même si le même utilisateur n'a pas de compte sur iDRAC ou si le compte n'a pas de privilèges administrateur.
- 1 Un utilisateur CMC qui n'a **PAS** de privilège administratif sur le serveur mais a le même compte sur iDRAC sera automatiquement connecté à iDRAC à l'aide de l'authentification unique. Une fois sur le site iDRAC, les privilèges qui ont été créés pour le compte iDRAC sont accordés à l'utilisateur.
- 1 Un utilisateur CMC qui n'a pas de privilège administratif sur le serveur ou le même compte sur iDRAC, ne sera **PAS** automatiquement connecté à iDRAC à l'aide de l'authentification unique. Cet utilisateur est dirigé vers la page d'ouverture de session iDRAC quand il appuie sur le bouton **Lancer l'interface utilisateur d'iDRAC**.

 **REMARQUE** : le terme « même compte » dans ce contexte signifie que l'utilisateur a le même nom d'ouverture de session avec un mot de passe correspondant pour CMC et pour iDRAC. Tout utilisateur qui a le même nom d'ouverture de session mais un mot de passe différent n'est pas 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.

 **REMARQUE** : 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**.

FlexAddress

Cette section décrit les écrans de l'interface Web de la fonctionnalité FlexAddress. FlexAddress est une mise à niveau facultative qui permet aux modules serveurs de remplacer l'ID WWN/MAC d'usine par un ID WWN/MAC fourni par le châssis.

 **REMARQUE** : vous devez acheter et installer la mise à niveau FlexAddress pour avoir accès à ces écrans de configuration. Si la mise à niveau n'a pas été achetée et installée, le texte suivant s'affiche sur l'interface Web :

Fonctionnalité en option non installée. Consultez le *Guide d'utilisation de Dell Chassis Management Controller* pour des informations sur la fonctionnalité d'administration des adresses WWN/MAC attribuées par le châssis.

Pour acheter cette fonctionnalité, contactez Dell à l'adresse www.dell.com.

Affichage l'état de FlexAddress

Vous pouvez utiliser l'interface Web pour consulter des informations sur l'état de FlexAddress. Vous pouvez consulter les informations relatives à l'ensemble

du châssis ou à un serveur particulier. Les informations affichées incluent :

- 1 Configuration des structures.
- 1 Fonctionnalité FlexAddress activée/désactivée.
- 1 Numéro et nom du logement.
- 1 Adresses attribuées par le châssis et le serveur.
- 1 Adresses en cours d'utilisation.

 **REMARQUE** : vous pouvez également consulter l'état de FlexAddress à l'aide de l'interface de ligne de commande. Pour plus d'informations sur les commandes, voir [Utilisation de FlexAddress](#).

Consultation de l'état de FlexAddress pour le châssis

Les informations sur l'état de FlexAddress peuvent concerner l'ensemble du châssis. Les informations de condition indiquent si la fonctionnalité est active et fournissent un aperçu de la condition de FlexAddress pour chaque serveur.

Pour savoir si FlexAddress est actif pour le châssis :

1. Ouvrez une session sur l'interface Web (voir [Accès à l'interface Web CMC](#)).
2. Cliquez sur **Présentation du châssis** dans l'arborescence.
3. Cliquez sur l'onglet **Configuration**. La page **Configuration générale** apparaît. L'entrée FlexAddress est marquée comme **Actif** ou **Non actif**. Actif indique que la fonctionnalité est installée sur le châssis. Non actif indique que la fonctionnalité n'est pas installée et n'est pas utilisée par le châssis.

Pour afficher une présentation des conditions FlexAddress pour chaque module du serveur :

1. Connectez-vous à l'interface Web ([Accès à l'interface Web CMC](#)).
2. Cliquez sur **Présentation des serveurs** → **Propriétés** → **WWN/MAC**.
3. La page **Résumé FlexAddress** s'affiche. Cette page vous permet de consulter la configuration WWN et les adresses MAC de tous les logements du châssis.

La page d'état fournit les informations suivantes :

Configuration de la structure	<p>Structure A, Structure B, et Structure C affichent le type des structures d'entrée/sortie installées.</p> <p>IDRAC affiche l'adresse MAC de gestion du serveur.</p> <p>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.</p>
Adresses WWN/MAC	<p>Affiche la configuration FlexAddress de chaque logement du châssis. Les informations affichées comprennent :</p> <ul style="list-style-type: none">1 Le contrôleur de gestion d'iDRAC n'est pas une structure, mais son adresse FlexAddress est traitée en tant que telle1 L'emplacement et le nom des logements1 L'état de FlexAddress (actif/ non actif)1 Le type de structure1 Les adresses WWN/MAC en cours d'utilisation attribuées par le châssis et attribuées par le serveur <p>Une coche verte indique le type de l'adresse active, soit attribuée par le serveur, soit attribuée par le châssis.</p>

4. Pour des informations supplémentaires, cliquez sur **Aide**.

Consulter l'état de FlexAddress pour le serveur

Il est également possible d'afficher des informations relatives à l'état de FlexAddress pour chaque serveur. Les informations au niveau d'un serveur comportent un résumé de l'état de FlexAddress pour ce serveur.

Pour afficher les informations FlexAddress des serveurs :

1. Ouvrez une session sur l'interface Web (voir [Accès à l'interface Web CMC](#)).

2. Développez **Présentation des serveurs** dans l'arborescence. Tous les serveurs (1 à 16) s'affichent dans la liste développée **Serveurs**.

3. Cliquez sur le serveur dont vous souhaitez afficher les informations.

La page **Condition du serveur** s'affiche.

4. Cliquez sur l'onglet **Configuration**, puis sur le sous-onglet **FlexAddress**. La page **Déployer FlexAddress** s'affiche. Cette page vous permet de consulter la configuration WWN et les adresses MAC du serveur sélectionné.

La page d'état fournit les informations suivantes :

Tableau 5-59. Informations sur la page des conditions

FlexAddress activé	Indique si la fonctionnalité FlexAddress est activée ou non pour ce logement particulier.	
État actuel	Affiche la configuration actuelle de FlexAddress : <ul style="list-style-type: none"> ▮ Attribuée par le châssis : l'adresse de logement sélectionnée est attribuée par le châssis à l'aide de FlexAddress. Les adresses WWN/MAC des logements restent identiques, même si un nouveau serveur est installé. ▮ Attribuée par le serveur : le serveur utilise l'adresse attribuée par le serveur ou l'adresse par défaut incorporée au matériel du contrôleur. 	
État de l'alimentation	Affiche l'état actuel de l'alimentation des serveurs. Valeurs possibles : Sous tension , Mise sous tension , Mise hors tension , Hors tension et - (si le serveur est absent).	
Intégrité	 OK	Indique que la fonctionnalité FlexAddress est présente et fournit son état à CMC. En cas de perte des communications entre CMC et FlexAddress, CMC ne pourra pas obtenir ni afficher la condition de l'intégrité de FlexAddress.
	 Informatif	Affiche des informations sur FlexAddress en l'absence de modification de la condition de l'intégrité (OK, Avertissement, Critique).
	 Avertissement	Indique que des alertes d'avertissement seules ont été émises et que des actions correctives doivent être effectuées . Si aucune action corrective n'est effectuée, des pannes critiques susceptibles d'affecter l'intégrité du serveur peuvent se produire.
	 Critique	Indique qu'au moins une alerte de panne a été générée. La condition Critique représente une panne système du serveur et des actions correctives doivent être effectuées immédiatement .
	Aucune valeur	Lorsque la fonctionnalité FlexAddress est absente, les informations d'intégrité ne sont pas fournies.
Micrologiciel iDRAC	Indique la version d'iDRAC actuellement installée sur le serveur.	
BIOS Version (Version du BIOS)	Affiche la version actuelle du BIOS du module de serveur.	
Ordre de priorité	Numéro de logement du serveur associé à l'emplacement de la structure.	
Emplacement	Affiche l'emplacement du module d'entrée/sortie (E/S) dans le châssis sous forme de numéro de groupe (A, B, ou C)/numéro de logement (1 ou 2). Noms de logement : A1, A2, B1, B2, C1 ou C2.	
Structure	Affiche le type de structure.	
Attribuée par le serveur	Affiche les adresses WWN/MAC attribuées par le serveur qui sont incorporées au matériel du contrôleur.	
Attribuée par le châssis	Affiche les adresses WWN/MAC utilisées pour ce logement particulier.	

5. Pour des informations supplémentaires, cliquez sur **Aide**.

Configurer FlexAddress

Si vous l'achetez en même temps que le châssis, il sera installé et activé à la mise sous tension du système. Si vous achetez FlexAddress séparément, vous devez installer la carte de fonctionnalité SD conformément aux instructions fournies dans le document *Spécifications techniques de la carte Secure Digital (SD) de Chassis Management Controller (CMC)*. Vous trouverez ce document sur le site web support.dell.com/manuals.

Vous devez mettre le serveur hors tension avant de commencer la configuration. Vous pouvez activer ou désactiver FlexAddress structure par structure. Vous pouvez également activer/désactiver cette fonctionnalité logement par logement. Une fois que vous avez activé cette fonctionnalité par structure, vous pouvez sélectionner les logements à activer. Par exemple, si la structure A est activée, la fonctionnalité FlexAddress est activée uniquement sur la structure A des logements activés. Toutes les autres structures utilisent les identifiants WWN/MAC d'usine sur le serveur.

La fonctionnalité FlexAddress est activée sur tous les logements sélectionnés pour les structures activées. Par exemple, il n'est pas possible d'activer les structures A et B et d'activer FlexAddress pour le logement 1 de la structure A, mais pas de la structure B.

 **REMARQUE** : vous pouvez également configurer FlexAddress à l'aide de l'interface de ligne de commande. Pour plus d'informations sur les commandes, voir [Utilisation de FlexAddress](#).

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

Vous pouvez activer ou désactiver la fonctionnalité FlexAddress pour des structures et des logements au niveau du châssis. Cette fonctionnalité est d'abord activée structure par structure ; c'est seulement ensuite qu'elle est activée pour des logements. Les structures et les logements doivent être activés pour configurer FlexAddress.

Effectuez les étapes suivantes pour activer ou désactiver des structures et des logements afin d'utiliser la fonctionnalité FlexAddress :

1. Ouvrez une session sur l'interface Web (voir [Accès à l'interface Web CMC](#)).
2. Cliquez sur **Présentation des serveurs** dans l'arborescence.
3. Cliquez sur l'onglet **Configuration** → sous-onglet FlexAddress. La page **Déployer FlexAddress** s'affiche.
4. La section **Sélectionner des structures pour WWN/MAC attribués par le châssis** comporte une case à cocher pour **Structure A**, **Structure B**, **Structure C** et **iDRAC**.
5. Cliquez sur la case à cocher de chaque structure pour laquelle vous voulez activer FlexAddress. Pour désactiver une structure, décochez la case située en regard de celle-ci.

 **REMARQUE** : si aucune structure n'est sélectionnée, FlexAddress n'est pas activée pour les logements sélectionnés.

Dans la page **Sélectionner des logements pour les WWN/MAC attribués par le châssis** la case de chacun des logements (1 à 16) est activée.

6. Cliquez sur la case **Activée** de chaque logement pour lequel vous souhaitez activer FlexAddress. Si vous souhaitez sélectionner tous les logements, cochez la case **Sélectionner/Désélectionner tout**. Pour désactiver un logement, décochez la case **Activée**.

 **REMARQUE** : si un serveur est présent dans le logement, mettez-le hors tension pour pouvoir activer la fonctionnalité FlexAddress sur ce logement.

 **REMARQUE** : si aucun logement n'est sélectionné, FlexAddress n'est pas activée pour les structures sélectionnées.

7. Cliquez sur **Appliquer** pour enregistrer les modifications.
Pour des informations supplémentaires, cliquez sur **Aide**.

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.

Pour activer ou désactiver un logement individuel afin d'utiliser la fonctionnalité FlexAddress :

1. Ouvrez une session sur l'interface Web (voir [Accès à l'interface Web CMC](#)).
2. Développez **Présentation des serveurs** dans l'arborescence. Tous les serveurs (1 à 16) s'affichent dans la liste développée **Serveurs**.
3. Cliquez sur le serveur dont vous souhaitez afficher les informations. La page **Condition du serveur** s'affiche.
4. Cliquez sur l'onglet **Configuration**, puis sur le sous-onglet **FlexAddress**. La page **État de FlexAddress** s'affiche.
5. Utilisez le menu déroulant **FlexAddress activé** pour effectuer votre sélection. Sélectionnez **Oui** pour activer FlexAddress et **Non** pour désactiver la fonctionnalité.
6. Cliquez sur **Appliquer** pour enregistrer les modifications. Pour des informations supplémentaires, cliquez sur **Aide**.

Partage de fichiers distants

L'option Partage de fichiers de média virtuel distants mappe un fichier depuis un lecteur de partage sur le réseau à un ou plusieurs serveurs via CMC pour déployer ou mettre à jour un système d'exploitation. Lorsque la connexion est établie, le fichier distant est accessible comme s'il se trouvait sur le système local. Deux types de média sont pris en charge : lecteurs de disquette et lecteurs de CD/DVD.

1. Ouvrez une session sur l'interface Web (voir [Accès à l'interface Web CMC](#)).
2. Cliquez sur **Présentation des serveurs** dans l'arborescence.
3. Cliquez sur l'onglet **Configuration**, puis sur le sous-onglet **Partage de fichiers distants**. La page **Déployer le partage de fichiers distants** apparaît.
4. Définissez les paramètres Partage de fichiers distants.

Tableau 5-60. Paramètres Partage de fichiers distants

Paramètre	Description
Chemin d'accès du fichier image	Le chemin des fichiers image est requis uniquement pour les opérations de connexion et de déploiement. Il ne s'applique pas aux opérations de déconnexion. Le nom du chemin du lecteur réseau est monté sur le serveur via un protocole SMB Windows ou NFS Linux/Unix. Par exemple, pour vous connecter au CIFS, tapez : //<adresse IP pour connexion à ce système de fichiers CIFS>/<chemin de fichier>/<nom de l'image> Pour vous connecter au NFS, tapez : //<adresse IP à connecter pour le système de fichiers NFS>:/<chemin de fichier>/<nom de l'image> Les noms de fichiers qui se terminent par .img sont connectés en tant que disquettes virtuelles. Les noms de fichiers qui se terminent par .iso sont connectés en tant que CD/DVD virtuels. Le nom peut comporter jusqu'à 511 caractères.
Nom d'utilisateur	Le nom d'utilisateur est requis uniquement pour les opérations de connexion et de déploiement. Il ne s'applique pas aux opérations de déconnexion. Le nombre maximum de caractères pouvant être spécifiés dans ce champ est 40.
Le mot de passe	Le mot de passe est requis uniquement pour les opérations de connexion et de déploiement. Il ne s'applique pas aux opérations de déconnexion. Le nombre maximum de caractères pouvant être spécifiés dans ce champ est 40.
Ordre de priorité	Identifie l'emplacement du logement. Les numéros de logement sont séquentiels, de 1 à 16 (pour les 16 logements disponibles dans le châssis).
Nom	Indique le nom du logement. Les logements sont nommés selon leur position dans le châssis.
Modèle	Affiche le nom du modèle du serveur.
État de l'alimentation	Affiche l'état d'alimentation du serveur : - : CMC n'a pas encore déterminé l'état d'alimentation du serveur. Désactivé : le serveur ou le châssis est hors tension. Activé : le châssis et le serveur sont sous tension. Mise sous tension : état temporaire entre Désactivé et Activé. En cas de réussite, l'état de l'alimentation est Activé. Mise hors tension : état temporaire entre Activé et Désactivé. En cas de réussite, l'état de l'alimentation est Désactivé.
Condition de la connexion	Affiche la condition de la connexion du partage de fichiers distants.
Sélectionner/Désélectionner tout	Sélectionnez cette option avant de lancer une opération de partage de fichiers distants. Les opérations de partage de fichiers distants sont les suivantes : Connecter, Déconnecter et Déployer.

5. Cliquez sur **Connecter** pour vous connecter à un partage de fichiers distants. Pour vous connecter à un partage de fichiers distants, vous devez fournir le chemin, le nom d'utilisateur et le mot de passe. La réussite de l'opération vous permet d'accéder au média.

Cliquez sur **Déconnecter** pour vous déconnecter d'un partage de fichiers distants précédemment connecté.

Cliquez sur **Déployer** pour déployer le périphérique du média.

 **REMARQUE** : enregistrez tous les fichiers de travail avant d'exécuter la commande `deploy` car cette action entraîne le redémarrage du serveur.

Cette commande implique les actions suivantes :

- o Le partage de fichiers distants est connecté.
- o Le fichier est sélectionné comme premier périphérique d'amorçage pour les serveurs.
- o Le serveur est redémarré.
- o Le serveur est mis sous tension s'il était hors tension.

Questions les plus fréquentes

Le [Tableau 5-61](#) répertorie les questions fréquemment posées, tout en gérant et récupérant un système distant.

Tableau 5-61. Gestion et récupération d'un système distant

Question	Réponse
Lorsque j'accède à l'interface Web CMC, un avertissement de sécurité s'affiche et	CMC est doté d'un certificat de serveur CMC par défaut qui assure la sécurisation du réseau pour l'interface Web et les fonctionnalités de RACADM distant. Lorsque ce certificat est utilisé, le navigateur Web affiche un

<p>indique que le nom d'hôte du certificat SSL ne correspond pas au nom d'hôte CMC.</p>	<p>avertissement de sécurité car le certificat par défaut est attribué au certificat par défaut CMC, lequel ne correspond pas au nom d'hôte CMC (l'adresse IP, par exemple).</p> <p>Pour corriger ce problème de sécurité, téléversez un certificat de serveur CMC attribué à l'adresse IP CMC. Lorsque vous générez la requête de signature de certificat (RSC) qui servira à émettre le certificat, assurez-vous que le nom commun (CN) de la RSC corresponde à l'adresse IP CMC (192.168.0.120, par exemple) ou au nom de CMC DNS enregistré.</p> <p>Afin de vous assurer que la RSC correspond au nom de DNS CMC enregistré :</p> <ol style="list-style-type: none"> 1. Cliquez sur Présentation du châssis dans l'arborescence du système. 2. Cliquez sur l'onglet Réseau, puis sur Réseau. La page Configuration du réseau apparaît. 3. Cochez la case Enregistrer CMC sur DNS. 4. Dans le champ Nom CMC DNS, saisissez le nom CMC. 5. Cliquez sur Appliquer les modifications. <p>Voir Sécurisation des communications CMC à l'aide de certificats SSL et numériques pour plus d'informations sur la génération de RSC et l'émission de certificats.</p>
<p>RACADM distante et les services Web ne sont plus disponibles lorsque les propriétés sont modifiées. Pourquoi ?</p>	<p>Après la réinitialisation du Web Server CMC, il peut s'écouler une minute avant que les services RACADM distant et l'interface Web ne redeviennent disponibles.</p> <p>Le Web Server CMC est réinitialisé dans les cas suivants :</p> <ul style="list-style-type: none"> 1 quand la configuration réseau ou les propriétés de sécurité réseau sont modifiées à l'aide de l'interface utilisateur Web CMC. 1 quand la propriété <code>cfgRacTuneHttpsPort</code> est modifiée (y compris lorsqu'une commande <code>config -f <fichier config></code> la modifie). 1 quand <code>racresetcfg</code> est utilisée ou que la sauvegarde de la configuration du châssis est restaurée. 1 quand CMC est réinitialisé. 1 quand un nouveau certificat de serveur SSL est téléversé.
<p>Mon serveur DNS n'enregistre pas mon CMC. Pourquoi ?</p>	<p>Certains serveurs DNS ne peuvent enregistrer que des noms de 31 caractères maximum.</p>
<p>Lorsque j'accède à l'interface Web CMC, un avertissement de sécurité s'affiche et indique que le certificat SSL a été émis par une autorité de certification qui n'est pas fiable.</p>	<p>CMC est doté d'un certificat de serveur CMC par défaut qui assure la sécurisation du réseau pour l'interface Web et les fonctionnalités de RACADM distant. Ce certificat <i>n'est pas</i> émis par une autorité de certification de confiance. Pour résoudre ce problème de sécurité, téléversez un certificat de serveur CMC émis par une autorité de certification de confiance (Thawte ou Verisign, par exemple). Pour plus d'informations sur l'émission de certificats, voir Sécurisation des communications CMC à l'aide de certificats SSL et numériques.</p>
<p>Le message suivant s'affiche pour des raisons inconnues :</p> <p>Accès distant : échec de l'authentification SNMP</p> <p>Pourquoi ?</p>	<p>Pendant la découverte, IT Assistant tente de vérifier les noms de communauté get et set du périphérique. Dans IT Assistant, le nom de communauté get = public et le nom de communauté set = private. Par défaut, le nom de communauté de l'agent CMC est public. Lorsque IT Assistant envoie une requête de définition, l'agent CMC génère une erreur d'authentification SNMP car il accepte uniquement les requêtes de la communauté = public.</p> <p>Vous pouvez changer le nom de communauté CMC à l'aide de RACADM.</p> <p>Pour afficher le nom de communauté CMC, utilisez la commande suivante :</p> <pre>racadm getconfig -g cfgOobSnmp</pre> <p>Pour définir le nom de communauté CMC, utilisez la commande suivante :</p> <pre>racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <nom de communauté></pre> <p>Pour ne pas générer d'interruption d'authentification SNMP, vous devez entrer des noms de communauté qui seront acceptés par l'agent. Comme CMC n'accepte qu'un seul nom de communauté, vous devez entrer le même nom pour les communautés get et set lorsque vous configurez les découvertes sous IT Assistant.</p>

Dépannage du CMC

L'interface Web CMC fournit des outils d'identification, de diagnostic et de résolution des problèmes rencontrés avec votre châssis. Pour plus d'informations sur la résolution des problèmes, voir « [Dépannage et récupération](#) ».

[Retour à la page Contenu](#)