# Integrated Dell Remote Access Controller 6 (iDRAC6), version 1.95

# Guide d'utilisation

# 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 de dommage matériel ou de perte de données en cas de non-respect des instructions.**

---



**2013 - 03**

# Table des matières

# 1

# Présentation d'iDRAC6

Integrated Dell Remote Access Controller6 (iDRAC6) est une solution matérielle et logicielle de gestion de systèmes fournissant des capacités de gestion à distance, la récupération de systèmes en panne et des fonctions de contrôle de l'alimentation pour les systèmes Dell PowerEdge.

iDRAC6 utilise un microprocesseur de type système sur une puce intégré pour le système de surveillance/contrôle distant. iDRAC6 coexiste sur la carte système avec le serveur PowerEdge géré. Le système d'exploitation du serveur exécute les applications ; iDRAC6 surveille et gère l'environnement et l'état du serveur en dehors du système d'exploitation.

Vous pouvez configurer iDRAC6 pour qu'il vous envoie des alertes par e-mail ou d'interruption SNMP (protocole de gestion de réseau simple) en cas d'avertissement ou d'erreur. Pour vous aider à diagnostiquer la cause probable d'un plantage du système, iDRAC6 peut journaliser des données d'événement et capturer une image de l'écran lorsqu'il détecte un plantage du système.

L'interface réseau iDRAC6 est activée par défaut avec l'adresse IP statique 192.168.0.120. Elle doit être configurée pour pouvoir accéder à iDRAC6. Une fois iDRAC6 configuré sur le réseau, il est accessible sur l'adresse IP qui lui a été attribuée avec l'interface Web iDRAC6, Telnet ou SSH (Secure Shell) et les protocoles de gestion de réseau pris en charge, tels que les protocoles IPMI (interface de gestion de plateforme intelligente).

## Nouveautés de cette version

- Prise en charge des configurations DIMM et cartes PCI (voir les notes de mise à jour pour en savoir plus).
- Prise en charge du navigateur Internet Explorer 10.
- La longueur de la clé de cryptage CSR (Certificate Signing Request) est modifiée à 2048 bits.

# Fonctionnalités de gestion d'iDRAC6 Express

iDRAC6 Express fournit les fonctionnalités de gestion suivantes :

- Permet l'enregistrement de système de noms de domaine dynamique (DDNS).
- Permet la gestion et la surveillance du système à distance à l'aide d'une interface Web et de la ligne de commande SM-CLP sur une connexion série, Telnet ou SSH.
- Permet la prise en charge de l'authentification Microsoft Active Directory : centralise les références utilisateur et les mots de passe iDRAC6 dans Active Directory à l'aide d'un schéma étendu ou d'un schéma standard.
- Mise à disposition d'une solution générique permettant de prendre en charge l'authentification LDAP (Lightweight Directory Access Protocol [protocole d'accès aux répertoires allégé]) : cette fonctionnalité ne requiert pas d'extension de schéma sur vos services de répertoire.
- Permet d'accéder aux informations sur le système et à la condition des composants à des fins de surveillance.
- Permet d'accéder au journal SEL, au journal iDRAC6 et au dernier écran de plantage ou de système ne répondant pas, indépendant de l'état du système d'exploitation.
- Offre l'option d'ajouter des notes de travail au journal du Lifecycle Controller via l'interface utilisateur ou la CLI.
- Permet de lancer l'interface Web iDRAC6 à partir de Dell OpenManage Server Administrator ou de Dell OpenManage IT Assistant.
- Vous avertit des problèmes potentiels du nœud géré au moyen d'un message électronique ou d'une interruption SNMP.
- Offre des fonctionnalités de gestion de la puissance à distance (comme la mise hors tension et la réinitialisation) depuis une console de gestion.
- Permet la prise en charge de l'interface de gestion de plateforme intelligente (IPMI).
- Permet une gestion à distance sécurisée du système via l'interface Web.
- La gestion de la sécurité du niveau de mot de passe empêche les accès non autorisés à un système distant.
- Offre des permissions affectables pour les différentes tâches de gestion des systèmes via une autorité basée sur les rôles.

- Ajoute la prise en charge IPv6, par exemple pour accéder à l'interface Web iDRAC6 à l'aide d'une adresse IPv6, spécifie l'adresse IPv6 pour le NIC d'iDRAC6 et spécifie un numéro de destination pour configurer une destination d'alerte SNMP IPv6.
- Fournit la gestion accessible par réseau au moyen du protocole WS-MAN (Web Services for Management).
- Ajoute la prise en charge du protocole SM-CLP (Server Management-Command Line Protocol) qui fournit des normes pour les implémentations de la CLI de gestion de systèmes.
- Permet d'effectuer l'amorçage (ou la restauration) depuis l'image du micrologiciel de votre choix via la restauration et récupération du micrologiciel.

Pour des informations supplémentaires sur iDRAC6 Express, voir le *Manuel du propriétaire du matériel* à l'adresse **dell.com/support/manuals**.

# iDRAC6 Enterprise et média vFlash

iDRAC6 Enterprise avec le média vFlash ajoute la prise en charge des fonctionnalités RACADM, de la Console virtuelle et du Média virtuel, un NIC dédié et un vFlash (avec la carte Dell vFlash Media en option). vFlash vous permet de stocker des images d'amorçage d'urgence et les outils de diagnostic sur le média vFlash. Pour plus d'informations sur iDRAC6 Enterprise et le média vFlash, voir le *Manuel du propriétaire du matériel* à l'adresse **dell.com/support/manuals**.

Le Tableau 1-1 répertorie les fonctionnalités disponibles pour BMC, iDRAC6 Express, iDRAC6 Enterprise et le média vFlash.

**Tableau 1-1. Liste de fonctionnalités iDRAC6**

| Fonction | BMC | iDRAC6 Express | iDRAC6 Enterprise | iDRAC6 Enterprise avec vFlash |
|---|---|---|---|---|
| Prise en charge de l'interface et des normes | | | | |
| IPMI 2.0 | ✓ | ✓ | ✓ | ✓ |
| IUG Web | ✗ | ✓ | ✓ | ✓ |

**Tableau 1-1. Liste de fonctionnalités iDRAC6 *(suite)***

| Fonction | BMC | iDRAC6 Express | iDRAC6 Enterprise | iDRAC6 Enterprise avec vFlash |
|---|---|---|---|---|
| SNMP | ✗ | ✓ | ✓ | ✓ |
| WSMAN | ✗ | ✓ | ✓ | ✓ |
| SMASH-CLP (SSH uniquement) | ✗ | ✓ | ✓ | ✓ |
| Ligne de commande RACADM (SSH et locale) | ✗ | ✓ | ✓ | ✓ |
| Ligne de commande RACADM (distante) | ✗ | ✗ | ✓ | ✓ |
| **Connectivité** | | | | |
| Modes réseau Partagé/Basculement | ✓ | ✓ | ✓ | ✓ |
| IPv4 | ✓ | ✓ | ✓ | ✓ |
| Marquage VLAN | ✓ | ✓ | ✓ | ✓ |
| IPv6 | ✗ | ✓ | ✓ | ✓ |
| DNS dynamique | ✗ | ✓ | ✓ | ✓ |
| NIC dédié | ✗ | ✗ | ✓ | ✓ |
| **Sécurité et authentification** | | | | |
| Autorité basée sur les rôles | ✓ | ✓ | ✓ | ✓ |
| Utilisateurs locaux | ✓ | ✓ | ✓ | ✓ |
| Cryptage SSL | ✓ | ✓ | ✓ | ✓ |
| Active Directory | ✗ | ✓ | ✓ | ✓ |
| Prise en charge LDAP générique | ✗ | ✓ | ✓ | ✓ |

**Tableau 1-1. Liste de fonctionnalités iDRAC6 *(suite)***

| Fonction | BMC | iDRAC6 Express | iDRAC6 Enterprise | iDRAC6 Enterprise avec vFlash |
|---|---|---|---|---|
| Authentification bifactorielle [1] | ✗ | ✓ | ✓ | ✓ |
| Connexion directe | ✗ | ✓ | ✓ | ✓ |
| Authentification PK (pour SSH) | ✗ | ✗ | ✓ | ✓ |
| **Gestion et conversion à distance** | | | | |
| Mise à jour de micrologiciel à distance | ✓[2] | ✓ | ✓ | ✓ |
| Contrôle de l'alimentation du serveur | ✓[2] | ✓ | ✓ | ✓ |
| Série sur LAN (avec proxy) | ✓ | ✓ | ✓ | ✓ |
| Série sur LAN (sans proxy) | ✓ | ✓ | ✓ | ✓ |
| Plafonnement de l'alimentation | ✓ | ✓ | ✓ | ✓ |
| Capture de l'écran du dernier plantage | ✗ | ✓ | ✓ | ✓ |
| Capture au démarrage | ✗ | ✓ | ✓ | ✓ |
| Média virtuel[3] | ✗ | ✗ | ✓ | ✓ |
| Console virtuelle[3] | ✗ | ✗ | ✓ | ✓ |
| Partage de console virtuelle[3] | ✗ | ✗ | ✓ | ✓ |
| Lancement de la console virtuelle distante | ✗ | ✗ | ✓ | ✓ |
| vFlash | ✗ | ✗ | ✗ | ✓ |

**Tableau 1-1. Liste de fonctionnalités iDRAC6 *(suite)***

| Fonction | BMC | iDRAC6 Express | iDRAC6 Enterprise | iDRAC6 Enterprise avec vFlash |
|---|---|---|---|---|
| **Surveillance** | | | | |
| Surveillance et alertes des capteurs | ✓[2] | ✓ | ✓ | ✓ |
| Contrôle de l'alimentation en temps réel | ✓ | ✓ | ✓ | ✓ |
| Graphique d'alimentation en temps réel | ✗ | ✓ | ✓ | ✓ |
| Compteurs d'alimentation historiques | ✗ | ✓ | ✓ | ✓ |
| **Journalisation** | | | | |
| Journal des événements système (SEL) | ✓ | ✓ | ✓ | ✓ |
| Journal du RAC | ✗ | ✓ | ✓ | ✓ |
| Syslog distant | ✗ | ✗ | ✓ | ✓ |
| **Lifecycle Controller** | | | | |
| Unified Server Configurator | ✓[4] | ✓ | ✓ | ✓ |
| Services distants (via WS-MAN) | ✗ | ✓ | ✓ | ✓ |
| Remplacement de pièce | ✗ | ✗ | ✗ | ✓ |

[1] L'authentification bifactorielle requiert Internet Explorer.

[2] La fonctionnalité est disponible uniquement via IPMI, et non via une IUG Web.

[3] La console virtuelle et le média virtuel sont disponibles avec les plug-ins Java et Active-X.

[4] Unified Server Configurator disponible via BMC est limité à l'installation et aux diagnostics du système d'exploitation uniquement.

✓ = pris en charge ; ✗ = non pris en charge

iDRAC6 dispose des fonctionnalités de sécurité suivantes :

- Connexion directe, authentification bifactorielle et authentification par clé publique.
- Authentification des utilisateurs via Active Directory (facultatif), via l'authentification LDAP (facultatif) ou via les références utilisateur et les mots de passe stockés sur le matériel.
- Autorisation basée sur les rôles, qui permet à un administrateur de configurer des privilèges spécifiques pour chaque utilisateur.
- Configuration des références utilisateur et des mots de passe via l'interface Web ou SM-CLP .
- SM-CLP et interfaces Web qui prennent en charge le cryptage 128 bits et 40 bits (dans les pays où le cryptage 128 bits n'est pas accepté) en utilisant la norme SSL 3.0.
- Configuration du délai d'expiration de la session (en secondes) via l'interface Web ou SM-CLP.
- Ports IP configurables (si applicable).

  **REMARQUE :** Telnet ne prend pas en charge le cryptage SSL.
- SSH qui utilise une couche de transport cryptée pour une sécurité plus élevée.
- 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.
- Possibilité de limiter la plage d'adresses IP pour les clients se connectant à iDRAC6.

## Plate-formes prises en charge

Pour les dernières plateformes prises en charge, voir le fichier « Lisez-moi » iDRAC6 et la *Matrice de prise en charge des logiciels des systèmes Dell* disponible à l'adresse **dell.com/support/manuals**.

## Systèmes d'exploitation pris en charge

Pour les informations les plus récentes, voir le fichier « Lisez-moi » iDRAC6 et la *Matrice de prise en charge des logiciels des systèmes Dell* disponible à l'adresse **dell.com/support/manuals**.

## Navigateurs Web pris en charge

Pour les informations les plus récentes, voir les *Notes de mise à jour iDRAC 1.95* et la *Matrice de prise en charge des logiciels des systèmes Dell* disponible à l'adresse **dell.com/support/manuals**.

**REMARQUE :** en raison de graves défauts de sécurité, la prise en charge de SSL 2.0 a été abandonnée. Votre navigateur doit être configuré pour activer SSL 3.0 afin de fonctionner correctement. Internet Explorer 6.0 n'est pas pris en charge.

## Connexions d'accès à distance prises en charge

Le Tableau 1-2 répertorie les fonctionnalités de connexion.

**Tableau 1-2. Connexions d'accès à distance prises en charge**

| Connexion | Fonctionnalités |
|---|---|
| NIC d'iDRAC6 | • Ethernet 10/100/1000 Mb/s<br>• Prise en charge de DHCP<br>• Interruptions SNMP et notifications d'événements par e-mail<br>• Prise en charge de l'environnement de commande SM-CLP (Telnet, SSH et RACADM) pour les opérations telles que la configuration iDRAC6, le démarrage système, la réinitialisation, la mise sous tension et les commandes d'arrêt<br>• Prise en charge des utilitaires IPMI, tels que IPMItool et ipmish |

## Ports iDRAC6

Le Tableau 1-3 répertorie les ports sur lesquels iDRAC6 écoute les connexions.Le Tableau 1-4 identifie les ports qu'iDRAC6 utilise comme client. Ces informations sont requises pour ouvrir des pare-feu pour pouvoir accéder à distance à un iDRAC6.

**Tableau 1-3. Ports d'écoute de serveur iDRAC6**

| Numéro de port | Fonction |
|---|---|
| 22* | SSH |
| 23* | Telnet |

**Tableau 1-3. Ports d'écoute de serveur iDRAC6 *(suite)***

| Numéro de port | Fonction |
|---|---|
| 80* | HTTP |
| 443* | HTTPS |
| 623 | RMCP/RMCP+ |
| 5900* | Clavier/souris de la console virtuelle, service Média virtuel, service Média virtuel sécurisé et vidéo Console virtuelle |

* Port configurable

**Tableau 1-4. Ports de client iDRAC6**

| Numéro de port | Fonction |
|---|---|
| 25 | SMTP |
| 53 | DNS |
| 68 | Adresse IP attribuée par DHCP |
| 69 | TFTP |
| 162 | interruption SNMP |
| 636 | LDAPS |
| 3 269 | LDAPS pour le catalogue global (CG) |

# Autres documents utiles

Outre le présent guide, les documents suivants disponibles sur le site Web du support de Dell à l'adresse **dell.com/support/manuals** fournissent des informations supplémentaires sur la configuration et le fonctionnement d'iDRAC6 au sein de votre système.

- L'aide en ligne iDRAC6 fournit des informations détaillées sur l'utilisation de l'interface Web.
- Le *Guide de référence de la ligne de commande RACADM pour iDRAC6 et CMC* fournit des informations sur les sous-commandes RACADM, les interfaces prises en charge, les groupes de base de données de propriété iDRAC6 et les définitions d'objets.

- Le *Guide d'utilisation de Dell Lifecycle Controller* fournit des informations sur Unified Server Configurator (USC), Unified Server Configurator – Lifecycle Controller Enabled (USC – LCE) et les services distants.
- Consultez le *Guide d'utilisation des utilitaires du contrôleur BMC Dell OpenManage* pour des informations sur iDRAC6 et l'interface IPMI.
- La *Matrice de prise en charge des logiciels des systèmes Dell* fournit des informations concernant les différents systèmes Dell, les systèmes d'exploitation pris en charge par ces systèmes et les composants Dell OpenManage pouvant être installés sur ces systèmes.
- Le *Guide d'installation de Dell OpenManage Server Administrator* contient des instructions visant à vous aider à installer Dell OpenManage Server Administrator.
- Le *Guide d'installation de Dell OpenManage Management Station Software* contient des instructions visant à vous aider à installer Dell OpenManage Management Station Software qui intègre l'utilitaire de gestion de la carte mère, les outils DRAC et le snap-in d'Active Directory.
- Le *Guide d'utilisation de Dell OpenManage Server Administrator* fournit des informations sur l'installation et l'utilisation de Server Administrator.
- Le *Guide d'utilisation des progiciels Dell Update Packages* fournit des informations sur l'obtention et l'utilisation des progiciels Dell Update Packages dans le contexte de la stratégie de mise à jour de votre système.
- Le *Glossaire* fournit des informations sur les termes utilisés dans ce document.

Les documents système suivants fournissent également des informations supplémentaires sur le système sur lequel iDRAC6 est installé :

- Pour installer un iDRAC6, consultez votre *Manuel du propriétaire du matériel*.
- 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 **dell.com/regulatory_compliance**. Les informations sur la garantie se trouvent dans ce document ou dans un document distinct.

- Les *Instructions d'installation du rack*, fournies avec le rack, indiquent comment installer votre système dans un rack.
- Le *Guide de mise en route* présente les fonctionnalités du système, les procédures de configuration et les spécifications techniques.
- Le *Manuel du propriétaire du matériel*, qui présente les fonctionnalités du système, contient des informations de dépannage ainsi que des instructions d'installation ou de remplacement des composants du système.
- La documentation relative aux logiciels de gestion de systèmes décrit les fonctionnalités, la configuration requise, l'installation et l'utilisation de base du logiciel.
- La documentation du système d'exploitation indique comment installer (au besoin), configurer et utiliser le système d'exploitation.
- La documentation fournie avec les composants achetés séparément indique comment configurer et installer ces options.
- Des mises à jour sont parfois fournies avec le système pour décrire les modifications apportées au système, au logiciel et/ou à la documentation.

  **REMARQUE :** lisez toujours les mises à jour en premier, car elles remplacent souvent les informations contenues dans d'autres documents.
- Les notes de mise à jour ou les fichiers « Lisez-moi » éventuellement fournis contiennent des mises à jour de dernière minute apportées au système ou à la documentation ou bien des informations techniques avancées destinées aux utilisateurs expérimentés ou aux techniciens.

# Accès aux documents depuis le site de support Dell

Pour accéder aux documents depuis le site de support Dell :

1. Rendez-vous sur **dell.com/support/manuals.**
2. Dans la section **Parlez-nous de votre système Dell**, sous **Non**, sélectionnez **Choisir à partir d'une liste de tous les produits Dell** et cliquez sur **Continuer**.
3. Dans la section **Sélectionner votre type de produit**, cliquez sur **Logiciel, Moniteurs, Électronique et Périphériques**.

4 Dans la section **Choisir vos Logiciel, Moniteurs, Électronique et Périphériques Dell**, cliquez sur **Software**.

5 Dans la section **Choisir votre logiciel Dell**, cliquez sur le lien depuis les options suivantes :

- Gestion de systèmes client
- Gestion de systèmes Enterprise
- Gestion de systèmes Enterprise à distance
- Outils de facilité de maintenance

6 Pour afficher le document, cliquez sur la version de produit requise.

Vous pouvez aussi accéder directement aux documents à l'aide des liens suivants :

- Pour les documents de Gestion de systèmes client : **dell.com/OMConnectionsClient**
- Pour les documents de Gestion de systèmes Enterprise : **dell.com/openmanagemanuals**
- Pour les documents de Gestion de systèmes Enterprise à distance : **dell.com/openmanagemanuals**
- Pour les documents d'Outils de facilité de maintenance : **dell.com/serviceabilitytools**

# 2

# Mise en route avec iDRAC6

iDRAC6 vous permet de surveiller, dépanner et réparer à distance un système Dell, même lorsque celui-ci est en panne. iDRAC6 intègre des fonctionnalités telles que Console virtuelle, Média virtuel, Authentification par carte à puce et Connexion directe (SSO).

La *station de gestion* est le système à partir duquel un administrateur gère à distance un système Dell doté d'un iDRAC6. Les systèmes ainsi surveillés sont appelés *systèmes gérés*.

Vous pouvez installer en option le logiciel Dell OpenManage sur la station de gestion ainsi que sur le système géré. Sans le logiciel Managed System, vous ne pouvez pas utiliser la RACADM localement et iDRAC6 ne peut pas saisir l'écran de la dernière panne.

Pour configurer iDRAC6, effectuez les étapes générales suivantes :

**REMARQUE :** cette procédure peut différer selon les systèmes. Consultez le *Manuel du propriétaire du matériel* de votre système sur le site Web du support de Dell à l'adresse **dell.com/support/manuals** pour obtenir des instructions précises sur la réalisation de cette procédure.

1. Configurez les propriétés, les paramètres réseau et les utilisateurs iDRAC6 : vous pouvez configurer iDRAC6 à l'aide de l'utilitaire de configuration iDRAC6, de l'interface Web ou de la RACADM.
2. (**Facultatif**) Si vous utilisez un système Windows, configurez Microsoft Active Directory pour accéder à iDRAC6 afin de pouvoir ajouter et contrôler les privilèges utilisateur iDRAC6 de vos utilisateurs existants dans le logiciel Active Directory.
3. (**Facultatif**) Configurez l'authentification par carte à puce : la carte à puce offre un niveau accru de sécurité à votre entreprise.
4. Configurez les points d'accès à distance, comme la console virtuelle et le média virtuel.
5. Configurez les paramètres de sécurité.
6. Configurez les alertes pour une capacité de gestion efficace des systèmes.
7. Configurez les paramètres de l'interface de gestion de plateforme intelligente (IPMI) iDRAC6 pour utiliser les outils IPMI normalisés pour gérer les systèmes sur votre réseau.

# 3

# Installation de base d'iDRAC6

Cette section fournit des informations pour installer et configurer le matériel et le logiciel de votre iDRAC6.

## Avant de commencer

Assurez-vous que vous disposez des éléments suivants, intégrés à votre système, avant de procéder à l'installation et à la configuration du logiciel iDRAC6 :

- Matériel iDRAC6 (déjà installé ou dans le kit en option)
- Procédures d'installation d'iDRAC6 (situées dans ce chapitre)
- DVD *Dell Systems Management Tools* and Documentation

## Installation du matériel iDRAC6 Express/Enterprise

**REMARQUE :** la connexion d'iDRAC6 émule une connexion de clavier USB. De ce fait, lorsque vous redémarrez le système, il ne vous prévient pas si votre clavier n'est pas connecté.

iDRAC6 Express/Enterprise peut être préinstallé sur votre système ou disponible séparément. Pour vous familiariser avec iDRAC6 installé sur votre système, consultez « Présentation générale de l'installation et de la configuration du logiciel », à la page 38.

Si aucun iDRAC6 Express/Enterprise n'est installé sur votre système, voir le *Manuel du propriétaire du matériel* de votre plateforme pour des instructions d'installation du matériel.

# Configuration de votre système pour utiliser un iDRAC6

Pour configurer votre système pour utiliser un iDRAC6, servez-vous de l'utilitaire de configuration d'iDRAC6.

Pour exécuter l'utilitaire de configuration d'iDRAC6 :

1. Allumez ou redémarrez le système.
2. Appuyez sur <Ctrl><E> lorsque vous y êtes invité pendant le POST.

   Si votre système d'exploitation commence à se charger alors que vous n'avez pas encore appuyé sur <Ctrl><E>, laissez-le terminer, puis redémarrez votre système et réessayez.
3. Configurez le LOM.
   a. À l'aide des touches fléchées, sélectionnez **Paramètres LAN,** puis appuyez sur <Entrée>. **La page Sélection de NIC** est affichée.
   b. À l'aide des touches fléchées, sélectionnez l'un des modes NIC suivants :
      - **Dédié :** sélectionnez cette option pour permettre au périphérique d'accès à distance d'utiliser l'interface réseau dédiée disponible sur iDRAC Enterprise. Cette interface n'est pas partagée avec le système d'exploitation hôte et achemine le trafic de gestion vers un réseau physique séparé en le séparant du trafic d'application Cette option est disponible uniquement si iDRAC6 Enterprise est installé dans le système. Après avoir installé la carte iDRAC6 Enterprise, assurez-vous de remplacer **Sélection de NIC** par **Dédié**. Cette opération peut être effectuée via l'utilitaire de configuration d'iDRAC6, l'interface Web iDRAC6 ou la RACADM.
      - **Partagé :** sélectionnez cette option pour partager l'interface réseau avec le système d'exploitation hôte. L'interface réseau du périphérique d'accès à distance est entièrement fonctionnelle quand le système d'exploitation hôte est configuré pour le regroupement de NIC. Le périphérique d'accès à distance reçoit des données via le NIC 1 et le NIC 2 mais transmet des données seulement via le NIC 1. Si le NIC 1 échoue, le périphérique d'accès à distance n'est pas accessible.

- **Partagé avec basculement LOM2 :** sélectionnez cette option pour partager l'interface réseau avec le système d'exploitation hôte. L'interface réseau du périphérique d'accès à distance est entièrement fonctionnelle quand le système d'exploitation hôte est configuré pour le regroupement de NIC. Le périphérique d'accès à distance reçoit des données via le NIC 1 et le NIC 2, mais transmet des données seulement via le NIC 1. Si le NIC 1 échoue, le périphérique d'accès à distance bascule sur le NIC 2 pour l'intégralité de la transmission des données. Le périphérique d'accès à distance continue d'utiliser le NIC 2 pour la transmission des données. Si le NIC 2 échoue, le périphérique d'accès à distance rebascule toutes les transmissions de données sur le NIC 1 si l'échec du NIC 1 a été corrigé.
- **Partagé avec basculement Tous les LOM :** sélectionnez cette option pour partager l'interface réseau avec le système d'exploitation hôte. L'interface réseau du périphérique d'accès à distance est entièrement fonctionnelle quand le système d'exploitation hôte est configuré pour le regroupement de NIC. Le périphérique d'accès à distance reçoit des données via les cartes réseau 1, 2, 3 et 4, mais transmet des données seulement via la carte réseau 1. Si le NIC 1 échoue, le périphérique d'accès à distance bascule l'intégralité de la transmission des données sur le NIC 2. Si le NIC 2 échoue, le périphérique d'accès à distance bascule l'intégralité de la transmission des données sur le NIC 3. Si le NIC 3 échoue, le périphérique d'accès à distance bascule l'intégralité de la transmission des données sur le NIC 4. Si le NIC 4 échoue, le périphérique d'accès à distance bascule l'intégralité de la transmission des données sur le NIC 1, mais uniquement si l'échec initial du NIC 1 a été corrigé.

4 Configurez les paramètres LAN du contrôleur réseau pour utiliser DHCP ou une source d'adresse IP statique.

a À l'aide de la touche fléchée vers le bas, sélectionnez **Paramètres LAN**, puis appuyez sur <Entrée>.

b À l'aide des touches fléchées vers la gauche et vers la droite, sélectionnez **Source d'adresse IP**.

c À l'aide des touches fléchées vers la gauche et vers la droite, sélectionnez **DHCP**, **Auto Config** ou **Statique**.

d Si vous avez sélectionné **Statique**, configurez les paramètres **Adresse IP**, **Masque de sous-réseau** et **Passerelle par défaut**.

e Appuyez sur <Échap>.

5 Appuyez sur <Échap>.

6 Sélectionnez **Enregistrer les changements et quitter**.

# Présentation générale de l'installation et de la configuration du logiciel

Cette section donne une vue d'ensemble de haut niveau des procédures d'installation et de configuration du logiciel iDRAC6. Pour plus d'informations sur les composants du logiciel iDRAC6, voir « Installation du logiciel sur le système géré », à la page 39.

## Installation du logiciel iDRAC6

Pour installer le logiciel iDRAC6 :

1 Installez le logiciel iDRAC6 sur le système géré. Voir « Installation du logiciel sur le système géré », à la page 39.

2 Installez le logiciel iDRAC6 sur la station de gestion. Voir « Installation du logiciel sur la station de gestion », à la page 40.

## Configuration d'iDRAC6

Pour configurer iDRAC6 :

1 Sélectionnez l'un des outils de configuration suivants :

- Interface Web (voir « Configuration d'iDRAC6 avec l'interface Web », à la page 47)
- CLI RACADM (voir le *Guide de référence de la ligne de commande RACADM pour iDRAC6 et CMC* disponible sur le site Web **dell.com/support/manuals**)
- Console Telnet (voir « Utilisation d'une console Telnet », à la page 93)

**REMARQUE :** l'utilisation simultanée de plusieurs outils de configuration iDRAC6 peut provoquer des résultats inattendus.

2 Configurez les paramètres réseau iDRAC6. Voir « Configuration des paramètres réseau d'iDRAC6 », à la page 114.

3 Ajoutez et configurez des utilisateurs iDRAC6. Voir « Ajout et configuration d'utilisateurs iDRAC6 », à la page 135.

4 Configurez le navigateur Web pour accéder à l'interface Web. Voir « Configuration d'un navigateur Web pris en charge », à la page 44.

5 Désactivez l'option de redémarrage automatique de Microsoft Windows. Voir « Désactivation de l'option Redémarrage automatique de Windows », à la page 344.

6 Mettez à jour le micrologiciel iDRAC6. Voir « Mise à jour du micrologiciel iDRAC6 », à la page 41.

## Installation du logiciel sur le système géré

L'installation du logiciel sur le système géré est facultative. Sans le logiciel Managed System, vous ne pouvez pas utiliser la RACADM localement et iDRAC6 ne peut pas saisir l'écran de la dernière panne.

Pour installer le logiciel Managed System, installez le logiciel sur le système géré à l'aide du DVD *Dell Systems Management Tools and Documentation*. Pour obtenir des instructions relatives à l'installation de ce logiciel, voir votre *Guide d'installation rapide du logiciel* disponible sur le site Web du support de Dell à l'adresse **support.dell.com\manuals**.

Le logiciel Managed System installe vos choix à partir de la version appropriée de Dell OpenManage Server Administrator sur le système géré.

**REMARQUE :** n'installez pas les logiciels iDRAC6 Management Station Software et iDRAC6 Managed System Software sur le même système.

Si Server Administrator n'est pas installé sur le système géré, vous ne pouvez pas afficher l'écran du dernier plantage du système ou utiliser la fonctionnalité **Récupération automatique**.

Pour plus d'informations sur l'écran du dernier plantage, voir « Affichage de l'écran du dernier plantage système », à la page 365.

# Installation du logiciel sur la station de gestion

Votre système est fourni avec le DVD *Dell Systems Management Tools and Documentation*. Ce DVD est composé des éléments suivants :

- Racine du DVD : contient Dell Systems Build and Update Utility qui fournit des informations de configuration du serveur et d'installation du système
- SYSMGMT : contient les produits Systems Management Software, dont Dell OpenManage Server Administrator

Pour plus d'informations sur Server Administrator, IT Assistant et Unified Server Configurator, voir le *Guide d'utilisation de Server Administrator*, le *Guide d'utilisation d'IT Assistant* et le *Guide d'utilisation de Lifecycle Controller* disponibles sur le site Web du support de Dell à l'adresse **dell.com/support/manuals**.

## Installation et retrait de la RACADM sur une station de gestion Linux

Pour utiliser les fonctionnalités de la RACADM distante, installez la RACADM sur une station de gestion fonctionnant sous Linux.

**REMARQUE :** lorsque vous exécutez **Configuration** sur le DVD *Dell Systems Management Tools and Documentation*, l'utilitaire RACADM pour tous les systèmes d'exploitation pris en charge est installé sur votre station de gestion.

## Installation de la RACADM

1. Ouvrez une session en tant que root sur le système sur lequel vous voulez installer les composants de la station de gestion.
2. Si nécessaire, montez le DVD *Dell Systems Management Tools and Documentation* à l'aide de la commande suivante ou d'une commande similaire :

   ```
   mount /media/cdrom
   ```

3. Naviguez vers le répertoire **/linux/rac** et exécutez la commande suivante :

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

Si vous avez besoin d'aide avec la commande RACADM, tapez **racadm help** après avoir émis les commandes précédentes.

### Désinstallation de la RACADM

Pour désinstaller la RACADM, ouvrez une invite de commande et tapez :

```
rpm -e <nom_du_progiciel_racadm>
```

où *<nom_du_progiciel_racadm>* est le progiciel rpm qui a été utilisé pour installer le logiciel du RAC.

Par exemple, si le nom du progiciel rpm est **srvadmin-racadm5**, tapez alors :

```
rpm -e srvadmin-racadm5
```

# Mise à jour du micrologiciel iDRAC6

Utilisez l'une des méthodes suivantes pour mettre votre micrologiciel iDRAC6 à jour.

- Interface Web (voir « Mise à jour du micrologiciel iDRAC6 avec l'interface Web », à la page 42)
- CLI RACADM (voir « Mise à jour du micrologiciel iDRAC6 avec la RACADM », à la page 42)
- Progiciels Dell Update Package (voir « Mise à jour du micrologiciel iDRAC6 à l'aide des progiciels Dell Update Package pour les systèmes d'exploitation Windows et Linux pris en charge », à la page 43)

### Avant de commencer

Avant de mettre à jour votre micrologiciel iDRAC6 à l'aide de la RACADM locale ou des progiciels Dell Update Package, procédez comme suit. Sinon, la mise à jour du micrologiciel échoue.

1. Installez et activez les pilotes IPMI et de nœud géré appropriés.
2. Si votre système fonctionne sous un système d'exploitation Windows, activez et démarrez le service **Windows Management Instrumentation** (WMI).
3. Si vous utilisez iDRAC6 Enterprise et que votre système exécute SUSE Linux Enterprise Server (version 10) pour Intel EM64T, démarrez le service **Raw**.
4. Débranchez et démontez le média virtuel.

**REMARQUE :** si la mise à jour du micrologiciel iDRAC6 est interrompue pour une raison quelconque, un délai atteignant 30 minutes peut être requis avant qu'une mise à jour du micrologiciel ne soit à nouveau autorisée.

5 Assurez-vous qu'USB est activé.

### Téléchargement du micrologiciel iDRAC6

Pour mettre à jour votre micrologiciel iDRAC6, téléchargez le dernier micrologiciel disponible sur le site Web du support de Dell à l'adresse **support.dell.com** et enregistrez le fichier sur votre système local.

Le progiciel de votre micrologiciel iDRAC6 se compose des éléments logiciels suivants :

- Code compilé et données du micrologiciel iDRAC6
- Fichiers de données de l'interface Web, JPEG et des autres interfaces utilisateur
- Fichiers de configuration par défaut

### Mise à jour du micrologiciel iDRAC6 avec l'interface Web

Pour des informations détaillées, voir « Mise à jour de l'image de récupération des services du micrologiciel iDRAC6/système », à la page 80.

### Mise à jour du micrologiciel iDRAC6 avec la RACADM

Vous pouvez mettre à jour le micrologiciel iDRAC6 à l'aide de l'outil RACADM CLI. Si vous avez installé Server Administrator sur le système géré, utilisez la RACADM locale pour mettre à jour le micrologiciel.

1 Téléchargez sur le système géré l'image de micrologiciel iDRAC6 depuis le site Web du support de Dell à l'adresse **support.dell.com**.

Par exemple :

```
C:\downloads\firmimg.d6
```

2 Exécutez la commande RACADM suivante :

```
racadm fwupdate -pud c:\downloads\
```

Vous pouvez également mettre à jour le micrologiciel à l'aide de la RACADM distante et d'un serveur TFTP.

Par exemple :

```
racadm -r <adresse IP iDRAC6> U <nom
d'utilisateur> -p <mot de passe> fwupdate -p -u -d
<chemin>
```

où *chemin* est l'emplacement, sur le serveur TFTP, où **firmimg.d6** est stocké, y compris l'adresse IP du serveur TFTP.

Chemin : <*IP du serveur TFTP*> -d < *Chemin de l'image de micrologiciel sur le serveur TFTP*>

- Cas1 : si l'image firmimg.d6 se trouve dans le dossier root (racine) tftp, le chemin est le suivant : <*IP du serveur TFTP*>
- Cas2 : si l'image firming.d6 se trouve dans le sous-dossier root (racine) tftp, le chemin est le suivant : <*IP du serveur TFTP*> -d /<*Chemin du sous-dossier*>

## Mise à jour du micrologiciel iDRAC6 à l'aide des progiciels Dell Update Package pour les systèmes d'exploitation Windows et Linux pris en charge

Téléchargez et exécutez les progiciels Dell Update Package pour les systèmes d'exploitation Windows et Linux pris en charge depuis le site Web du support de Dell à l'adresse **support.dell.com**. Pour plus d'informations, reportez-vous au *Guide d'utilisation des progiciels Dell Update Package* disponible sur le site Web du support de Dell à l'adresse **support.dell.com\manuals**.

**REMARQUE :** lors de la mise à jour du micrologiciel iDRAC6 à l'aide de l'utilitaire Dell Update Package dans Linux, les messages suivants peuvent s'afficher sur la console :

```
usb 5-2: device descriptor read/64, error -71

usb 5-2: device descriptor not accepting
address 2, error -71
```

Ces erreurs sont superficielles et doivent être ignorées. Ces messages sont dus à la réinitialisation des périphériques USB au cours de la mise à jour du micrologiciel et sont inoffensifs.

# Configuration d'un navigateur Web pris en charge

Les sections suivantes donnent des instructions pour configurer les navigateurs Web pris en charge.

## Configuration de votre navigateur Web pour la connexion à l'interface Web iDRAC6

Si vous vous connectez à l'interface Web iDRAC6 depuis une station de gestion qui se connecte à Internet via un serveur proxy, vous devez configurer le navigateur Web pour accéder à Internet depuis ce serveur.

Pour configurer votre navigateur Web Internet Explorer pour accéder à un serveur proxy :

1. Ouvrez une fenêtre de navigateur Web.
2. Cliquez sur **Outils**, puis sur **Options Internet**.
3. Dans la fenêtre **Options Internet**, cliquez sur l'onglet **Connexions**.
4. Sous **Paramètres du réseau local (LAN)**, cliquez sur **Paramètres du LAN**.
5. Si la case **Utiliser un serveur proxy** est sélectionnée, sélectionnez la case **Ne pas utiliser de serveur proxy pour les adresses locales**.
6. Cliquez sur **OK** deux fois.

## Liste des domaines de confiance

Lorsque vous accédez à l'interface Web iDRAC6 via le navigateur Web, vous serez peut-être invité à ajouter l'adresse IP iDRAC6 à la liste des domaines de confiance si l'adresse IP ne figure pas dans la liste. Lorsque vous avez terminé, cliquez sur **Actualiser** ou relancez le navigateur Web pour rétablir une connexion avec l'interface Web iDRAC6.

## Affichage de versions localisées de l'interface Web

### Windows

L'interface Web iDRAC6 est prise en charge dans les langues suivantes des systèmes d'exploitation Windows :

- Anglais
- Français

- Allemand
- Espagnol
- Japonais
- Chinois simplifié

Pour afficher une version localisée de l'interface Web iDRAC6 dans Internet Explorer :

1. Cliquez sur le menu **Outils** et sélectionnez **Options Internet**.
2. Dans la fenêtre **Options Internet**, cliquez sur **Langues**.
3. Dans la fenêtre **Langues**, cliquez sur **Ajouter**.
4. Dans la fenêtre **Ajouter une langue**, sélectionnez une langue prise en charge.

   Pour sélectionner plusieurs langues, appuyez sur <Ctrl>.
5. Sélectionnez la langue de votre choix et cliquez sur **Monter** pour déplacer la langue en haut de la liste.
6. Cliquez sur **OK**.
7. Dans la fenêtre **Langues**, cliquez sur **OK**.

#### Linux

Si vous exécutez la console virtuelle sur un client Red Hat Enterprise Linux (version 4) avec une GUI en chinois simplifié, le menu du visualiseur et un titre peuvent apparaître sous forme de caractères aléatoires. Ce problème est dû à l'encodage incorrect dans le système d'exploitation Red Hat Enterprise Linux (version 4) en chinois simplifié. Pour corriger ce problème, accédez et modifiez les paramètres d'encodage actuels en procédant comme suit :

1. Ouvrez un terminal de commande.
2. Tapez « paramètres régionaux » et appuyez sur <Entrée>. La sortie suivante s'affiche.

   ```
   LANG=zh_CN.UTF-8
   LC_CTYPE="zh_CN.UTF-8"
   LC_NUMERIC="zh_CN.UTF-8"
   LC_TIME="zh_CN.UTF-8"
   LC_COLLATE="zh_CN.UTF-8"
   LC_MONETARY="zh_CN.UTF-8"
   ```

```
LC_MESSAGES="zh_CN.UTF-8"
LC_PAPER="zh_CN.UTF-8"
LC_NAME="zh_CN.UTF-8"
LC_ADDRESS="zh_CN.UTF-8"
LC_TELEPHONE="zh_CN.UTF-8"
LC_MEASUREMENT="zh_CN.UTF-8"
LC_IDENTIFICATION="zh_CN.UTF-8"
LC_ALL=
```

3. Si les valeurs incluent « zh_CN.UTF-8 », aucune modification n'est nécessaire. Si les valeurs n'incluent pas « zh_CN.UTF-8 », passez à l'étape 4.
4. Naviguez vers le fichier **/etc/sysconfig/i18n**.
5. Dans le fichier, appliquez les modifications suivantes :

   Entrée actuelle :

   ```
   LANG="zh_CN.GB18030"
   SUPPORTED="zh_CN.GB18030:zh_CH.GB2312:zh_CN:zh"
   ```

   Entrée mise à jour :

   ```
   LANG="zh_CN.UTF-8"
   SUPPORTED="zh_CN.UTF-
   8:zh_CN.GB18030:zh_CH.GB2312:zh_CN:zh"
   ```

6. Fermez la session, puis ouvrez la session sur le système d'exploitation.
7. Relancez iDRAC6.

Lorsque vous passez de n'importe quelle autre langue au chinois simplifié, assurez-vous que ce problème n'existe plus. Sinon, répétez cette procédure.

Pour les configurations avancées d'iDRAC6, voir « Configuration avancée d'iDRAC6 », à la page 91.

# 4

# Configuration d'iDRAC6 avec l'interface Web

iDRAC6 fournit une interface Web qui vous permet de configurer les propriétés et les utilisateurs d'iDRAC6, d'effectuer des tâches de gestion à distance et de dépanner un système distant (géré) en cas de problème. Pour la gestion quotidienne des systèmes, utilisez l'interface Web iDRAC6. Ce chapitre décrit comment effectuer les tâches de gestion de systèmes courantes en utilisant l'interface Web iDRAC6 et vous donne des liens vers des informations connexes.

La plupart des tâches de configuration de l'interface Web peuvent être exécutées à l'aide des commandes RACADM ou celles du protocole SM-CLP (Server Management-Command Line Protocol).

Les commandes de la RACADM locale sont exécutées à partir du serveur géré.

Les commandes SM-CLP et RACADM SSH/Telnet sont exécutées dans un environnement accessible à distance avec une connexion Telnet ou SSH. Pour plus d'informations sur SM-CLP, voir « Utilisation de l'interface de ligne de commande SM-CLP iDRAC6 », à la page 249. Pour des informations supplémentaires sur les commandes RACADM, voir le *Guide de référence de la ligne de commande RACADM pour iDRAC6 et CMC* disponible sur le site Web du support de Dell à l'adresse **dell.com/support/manuals**.

**PRÉCAUTION : lorsque vous actualisez le navigateur en cliquant sur « Actualiser » ou en appuyant sur F5, il se peut que vous soyez déconnecté de la session d'IUG Web ou redirigé vers la page « Résumé du système ».**

# Accès à l'interface Web

Pour accéder à l'interface Web iDRAC6, effectuez les étapes suivantes :

1. Ouvrez une fenêtre d'un navigateur Web pris en charge.

   Pour accéder à l'interface Web à l'aide d'une adresse IPv4, passez à l'étape 2.

   Pour accéder à l'interface Web à l'aide d'une adresse IPv6, passez à l'étape 3.

2. Pour accéder à l'interface Web à l'aide d'une adresse IPv4, IPv4 doit être activé :

   Dans la barre **Adresse** du navigateur, tapez :

   `https://<iDRAC-IPv4-address>`

   Puis appuyez sur <Entrée>.

3. Pour accéder à l'interface Web à l'aide d'une adresse IPv6, IPv6 doit être activé.

   Dans la barre **Adresse** du navigateur, tapez :

   `https://[<iDRAC-IPv6-address>]`

   Puis appuyez sur <Entrée>.

4. Si le numéro de port HTTPS par défaut (port 443) a été modifié, tapez :

   `https://<adresse-IP-iDRAC>:<numéro-de-port>`

   où *adresse-IP-iDRAC* est l'adresse IP d'iDRAC6 et *numéro-de-port* le numéro de port HTTPS.

5. Dans le champ **Adresse**, tapez `https://<`*adresse-IP-iDRAC*`>` et appuyez sur <Entrée>.

   Si le numéro de port HTTPS par défaut (port 443) a été modifié, tapez :

   `https://<`*adresse-IP-iDRAC*`>:<`*numéro-de-port*`>`

   où *adresse-IP-iDRAC* est l'adresse IP d'iDRAC6 et *numéro-de-port* le numéro de port HTTPS.

   La fenêtre **Ouverture de session** iDRAC6 s'affiche.

### Ouverture de session

Vous pouvez ouvrir une session en tant qu'utilisateur iDRAC6 ou utilisateur Microsoft Active Directory. Le nom d'utilisateur et le mot de passe par défaut d'un utilisateur iDRAC6 sont **root** et **calvin**, respectivement.

Le privilège **Ouvrir une session sur iDRAC** doit vous avoir été octroyé par l'administrateur pour que vous puissiez ouvrir une session sur iDRAC6.

Pour ouvrir une session, effectuez les étapes suivantes :

1. Dans le champ **Nom d'utilisateur**, tapez l'un des éléments suivants :
   - Votre nom d'utilisateur iDRAC6.

     Le nom d'utilisateur des utilisateurs locaux est sensible à la casse. Les exemples sont `root`, `utilisateur_info` ou john_doe.
   - Votre nom d'utilisateur Active Directory.

     Les noms Active Directory peuvent être saisis sous la forme <*nom d'utilisateur*>, <*domaine*>\<*nom d'utilisateur*>, <*domaine*>/<*nom d'utilisateur*> ou <*utilisateur*>@<*domaine*>. Ils ne sont pas sensibles à la casse. Les exemples sont `dell.com\john_doe` ou `JOHN_DOE@DELL.COM`.
2. Dans le champ **Mot de passe**, tapez votre mot de passe utilisateur iDRAC6 ou Active Directory. Les mots de passe sont sensibles à la casse.
3. Depuis la boîte déroulante **Domaine**, sélectionnez *Cet iDRAC* pour ouvrir une session en tant qu'utilisateur iDRAC6 ou sélectionnez tout domaine disponible pour ouvrir une session en tant qu'utilisateur Active Directory.

   **REMARQUE :** pour les utilisateurs Active Directory, si vous avez spécifié le nom du domaine comme faisant partie du nom d'utilisateur, sélectionnez *Cet iDRAC* dans le menu déroulant.
4. Cliquez sur **OK** ou appuyez sur <Entrée>.

### Fermeture de session

1. Dans le coin supérieur droit de la fenêtre principale, cliquez sur **Fermer la session** pour fermer la session.
2. Fermez la fenêtre du navigateur.

**REMARQUE :** le bouton **Fermer la session** n'apparaît pas tant que vous n'avez pas ouvert une session.

**REMARQUE :** lorsque le navigateur est fermé sans avoir préalablement fermé la session normalement, la session peut rester ouverte jusqu'à ce qu'elle expire. Il est vivement recommandé de cliquer sur le bouton Fermer la session pour terminer la session ; sinon, la session peut rester active jusqu'à ce que son délai d'expiration soit atteint.

**REMARQUE :** la fermeture de l'interface Web iDRAC6 dans Microsoft Internet Explorer à l'aide du bouton Fermer (« x ») en haut à droite de la fenêtre peut générer une erreur d'application. Pour résoudre ce problème, téléchargez la dernière version de Cumulative Security Update for Internet Explorer à partir du site Web du support de Microsoft à l'adresse **support.microsoft.com**.

**PRÉCAUTION : si vous avez ouvert plusieurs sessions d'Interface utilisateur Web via <Ctrl+T> ou <Ctrl+N> pour accéder au même iDRAC6 à partir de la même station de gestion, puis fermez une de ces sessions, toutes les sessions d'IUG Web seront clôturées.**

### Utilisation des multiples onglets et fenêtres du navigateur

Des versions différentes de navigateurs Web font preuve de comportements différents à l'ouverture de nouveaux onglets et de nouvelles fenêtres. Microsoft Internet Explorer version 7 et 8 offrent la possibilité d'ouvrir des onglets ainsi que des fenêtres.

Un onglet hérite des caractéristiques d'un onglet récemment ouvert.

Appuyez sur `<Ctrl-T>` pour ouvrir un nouvel onglet dans la session active, puis ouvrez à nouveau une session.

Appuyez sur `<Ctrl-N>` pour ouvrir une nouvelle fenêtre de navigateur depuis la session active. Vous avez ouvert une session à l'aide de coordonnées déjà authentifiées.

La fermeture d'un onglet fait expirer tous les onglets de l'interface Web iDRAC6.

En outre, si vous ouvrez une session avec privilèges d'utilisateur privilégié dans un onglet, puis ouvrez une session en tant qu'administrateur dans un autre onglet, les privilèges de la première session ouverte sont acquis dans les deux onglets.

Le comportement de l'onglet est le même pour Mozilla Firefox 3 que pour Microsoft Internet Explorer version 7 et version 8.

**Tableau 4-1. Comportement des privilèges utilisateur dans les navigateurs pris en charge**

| Navigateur | Comportement des onglets | Comportement des fenêtres |
|---|---|---|
| Microsoft Internet Explorer 6 | Sans objet | Nouvelle session |
| Microsoft IE7 et IE8 | Depuis la dernière session ouverte | Nouvelle session |

# Configuration de la carte réseau iDRAC6

Cette section suppose qu'iDRAC6 a déjà été configuré et est accessible sur le réseau. Consultez « Configuration d'iDRAC6 », à la page 38 pour obtenir de l'aide sur la configuration réseau iDRAC6 initiale.

## Configuration des paramètres du réseau et du LAN IPMI

**REMARQUE :** vous devez disposer du droit **Configurer iDRAC** pour effectuer les étapes suivantes.

**REMARQUE :** la plupart des serveurs DHCP requièrent un serveur pour stocker un jeton d'identifiant de client dans son tableau de réservations. Le client (iDRAC, par exemple) doit fournir ce jeton pendant la négociation DHCP. iDRAC6 fournit l'option d'identifiant de client à l'aide d'un numéro (0) d'interface à un octet suivi par une adresse MAC à six octets.

**REMARQUE :** si vous travaillez avec le protocole STP (Spanning Tree Protocol) activé, assurez d'activer également PortFast ou une technologie similaire comme suit :
- Sur les ports pour le commutateur connecté à iDRAC6
- Sur les ports connectés à la station de gestion exécutant une session Console virtuelle d'iDRAC

**REMARQUE :** il se peut que vous voyiez le message suivant si le système s'arrête durant le POST: `Appuyez sur la touche F1 pour continuer, F2 pour exécuter le programme de configuration du système.`
Une des raisons possibles de l'erreur est une tempête du réseau qui cause la perte de la communication avec iDRAC6. Une fois que la tempête du réseau s'est calmée, redémarrez le système.

1 Cliquez sur **Paramètres iDRAC→ Réseau/Sécurité→ Réseau**.

2 Sur la page **Réseau,** vous pouvez saisir les paramètres réseau, les paramètres courants d'iDRAC6, les paramètres IPv4, les paramètres IPv6, les paramètres IPMI et les paramètres VLAN. Voir le Tableau 4-2, le Tableau 4-3, le Tableau 4-4, le Tableau 4-5, le Tableau 4-6 et le Tableau 4-7 pour les descriptions de ces paramètres.

3 Après la saisie des paramètres requis, cliquez sur **Appliquer**.

Les nouveaux paramètres de la page Réseau sont enregistrés.

**REMARQUE :** la modification des paramètres de l'adresse IP du NIC ferment toutes les sessions utilisateur et forcent les utilisateurs à se reconnecter à l'interface Web iDRAC6 avec les paramètres d'adresse IP mis à jour. Toutes les autres modifications nécessitent la réinitialisation du NIC, qui peut provoquer une brève perte de connectivité.

**Tableau 4-2. Paramètres réseau**

| Paramètre | Description |
|---|---|
| **NIC Selection (Sélection de carte réseau)** | Configure le mode courant sur les quatre modes possibles :<br>• Dédié<br>• Partagé (LOM1)<br>• Partagé avec basculement LOM2<br>• Partagé avec basculement tous les LOM<br>**REMARQUE :** l'option **Dédié** est uniquement disponible pour les cartes iDRAC Enterprise et l'option **Partagé avec basculement tous les LOM** peut être disponible uniquement pour quelques systèmes.<br>iDRAC6 ne communique pas localement via le même port physique si l'option Sélection de carte réseau est définie sur le mode **Partagé** ou **Partagé avec basculement**. Cela est dû au fait qu'un commutateur réseau n'envoie pas les paquets via le port par l'intermédiaire duquel il les a reçus.<br>Si la sélection du NIC est définie sur **Partagé avec basculement** (LOM 2 ou tous les LOM), il est recommandé de ne pas connecter les LOM à différents domaines de diffusion réseau.<br>Il est recommandé de ne pas regrouper les LOM avec des contrôleurs réseau d'extension lorsque le contrôleur iDRAC est configuré pour un mode partagé. Tout type de groupe entre les LOM est acceptable, indépendamment du mode de sélection de carte réseau (partagé/partagé avec basculement LOM2/partagé avec basculement tous les LOM). |
| **Adresse MAC** | Affiche l'adresse de contrôle de l'accès aux médias (MAC) qui identifie de manière unique chaque nœud d'un réseau. |
| **Activer le NIC** | Lorsqu'il est coché, ce paramètre indique que la carte réseau est activée et active les commandes restantes de ce groupe. Lorsqu'une carte réseau est désactivée, toutes les communications avec iDRAC6 via le réseau sont bloquées.<br>La valeur par défaut est **Activé**. |

**Tableau 4-2. Paramètres réseau *(suite)***

| Paramètre | Description |
|---|---|
| **Négociation automatique** | S'il est défini sur **Activé**, il affiche la vitesse du réseau et le mode en communiquant avec le routeur ou le commutateur le plus proche. S'il est défini sur **Désactivé**, il vous permet de définir la vitesse du réseau et le mode duplex manuellement.<br>Si l'option **Sélection de carte réseau** n'est *pas* définie sur **Dédié**, le paramètre Négociation automatique est toujours activée (**Activé**).<br>**REMARQUE :** lorsque le serveur est hors tension, les ports LOM intégrés prennent en charge une vitesse maximale de 100 Mbits/s. Par conséquent, la configuration des LOM et du commutateur de prise en charge de la négociation automatique garantit la connectivité vers iDRAC par le biais de transitions de puissance système. |
| **Vitesse du réseau** | Vous permet de définir la vitesse du réseau sur 100 Mbps ou 10 Mbps en fonction des besoins de votre environnement réseau. Cette option n'est pas disponible si Négociation automatique est défini sur **Activé**. |
| **Mode duplex** | Vous permet de définir le mode semi-duplex ou duplex intégral en fonction des besoins de votre environnement réseau. Cette option n'est pas disponible si **Négociation automatique** est défini sur **Activé**. |
| **MTU de NIC** | Vous permet de définir la taille de l'unité de transfert maximale (MTU/Maximum Transmission Unit) sur la carte réseau. |

**Tableau 4-3. Paramètres communs**

| Paramètre | Description |
|---|---|
| **Enregistrer iDRAC sur DNS** | Enregistre le nom iDRAC6 sur le serveur DNS.<br>La valeur par défaut est **Désactivé**. |
| **Nom iDRAC DNS** | Affiche le nom iDRAC6 uniquement lorsque **Enregistrer iDRAC sur DNS** est sélectionné. Le nom par défaut est idrac-*numéro_de_service*, où *numéro_de_service* est le numéro de service du serveur Dell, par exemple : idrac-00002. |

**Tableau 4-3. Paramètres communs *(suite)***

| Paramètre | Description |
|---|---|
| **Nom de domaine Auto Config** | Utilise le nom de domaine DNS par défaut. Lorsque la case à cocher n'est pas sélectionnée et que l'option **Enregistrer iDRAC sur DNS** est sélectionnée, modifiez le nom de domaine DNS dans le champ **Nom de domaine DNS**.<br>La valeur par défaut est **Désactivé**. |
| **Nom de domaine DNS** | Le champ **Nom de domaine DNS** par défaut est vide. Lorsque la case à cocher **Nom de domaine Auto Config** est sélectionnée, cette option est désactivée. |

**Tableau 4-4. Paramètres IPv4**

| Paramètre | Description |
|---|---|
| **Activer IPv4** | Si la carte réseau est activée, celle-ci sélectionne la prise en charge du protocole IPv4 et définit les autres champs de cette section à activer. |
| **Activation DHCP** | Invite iDRAC6 à obtenir une adresse IP pour la carte réseau sur le serveur de protocole de configuration dynamique à l'hôte (DHCP). La valeur par défaut est **Désactivé**. |
| **Adresse IP** | Spécifie l'adresse IP de la carte réseau iDRAC6. |
| **Masque de sous-réseau** | Vous permet de saisir ou de modifier une adresse IP statique pour la carte réseau iDRAC6. Pour modifier ce paramètre, désélectionnez la case à cocher Utiliser DHCP (pour l'adresse IP de la carte réseau). |
| **par défaut** | Adresse d'un routeur ou d'un commutateur. La valeur est au format « séparé par un point », par exemple 192.168.0.1. |
| **Utiliser DHCP pour obtenir des adresses de serveur DNS** | Activez DHCP pour obtenir des adresses de serveur DNS en sélectionnant la case à cocher **Utiliser DHCP pour obtenir des adresses de serveur DNS**. Lorsque vous n'utilisez pas DHCP pour obtenir les adresses de serveur DNS, indiquez les adresses IP dans les champs **Serveur DNS préféré** et **Autre serveur DNS**.<br>La valeur par défaut est **Désactivé**.<br>**REMARQUE :** lorsque la case à cocher **Utiliser DHCP pour obtenir des adresses de serveur DNS** est sélectionnée, les adresses IP ne peuvent pas être saisies dans les champs **Serveur DNS préféré** et **Autre serveur DNS.** |

**Tableau 4-4. Paramètres IPv4 *(suite)***

| Paramètre | Description *(suite)* |
|---|---|
| Serveur DNS préféré | Adresse IP du serveur DNS. |
| Autre serveur DNS | Adresse IP alternative du serveur DNS. |

**Tableau 4-5. Paramètres IPv6**

| Paramètre | Description |
|---|---|
| Activer IPv6 | Si la case à cocher est sélectionnée, IPv6 est activé. Si la case à cocher n'est pas sélectionnée, IPv6 est désactivé. La valeur par défaut est Désactivé. |
| Activation de la configuration automatique | Cochez cette case pour permettre à iDRAC6 d'obtenir l'adresse IPv6 de la carte réseau iDRAC6 auprès du serveur de protocole de configuration dynamique à l'hôte (DHCPv6). En outre, l'activation de la configuration automatique désactive et supprime les valeurs statiques de l'adresse IP 1, de la longueur du préfixe et de la passerelle IP. |
| Adresse IP 1 | Configure l'adresse IPv6 de la carte réseau iDRAC. Pour modifier ce paramètre, vous devez tout d'abord désactiver **AutoConfig** en désélectionnant la case à cocher associée. |
| Longueur du préfixe | Configure la longueur du préfixe de l'adresse IPv6. Il peut s'agir de toute valeur comprise entre 1 et 128 compris. Pour modifier ce paramètre, vous devez tout d'abord désactiver **AutoConfig** en désélectionnant la case à cocher associée. |
| par défaut | Configure la passerelle statique pour la carte réseau iDRAC. Pour modifier ce paramètre, vous devez tout d'abord désactiver **AutoConfig** en désélectionnant la case à cocher associée. |
| Adresse locale de liaison | Spécifie l'adresse locale de liaison IPv6 du NIC de l'iDRAC6. |
| Adresse IP 2...15 | Spécifie l'adresse IPv6 de la carte réseau iDRAC6 supplémentaire en cas de disponibilité. |

**Tableau 4-5. Paramètres IPv6 *(suite)***

| Paramètre | Description |
|---|---|
| **Utiliser DHCP pour obtenir des adresses de serveur DNS** | Activez DHCP pour obtenir des adresses de serveur DNS en sélectionnant la case à cocher **Utiliser DHCP pour obtenir des adresses de serveur DNS**. Lorsque vous n'utilisez pas DHCP pour obtenir les adresses de serveur DNS, indiquez les adresses IP dans les champs **Serveur DNS préféré** et **Autre serveur DNS**.<br>La valeur par défaut est Désactivé.<br>**REMARQUE :** lorsque la case à cocher **Utiliser DHCP pour obtenir des adresses de serveur DNS** est sélectionnée, les adresses IP ne peuvent pas être saisies dans les champs **Serveur DNS préféré** et **Autre serveur DNS**. |
| **Serveur DNS préféré** | Configure l'adresse IPv6 statique du serveur DNS préféré. Pour modifier ce paramètre, vous devez tout d'abord décocher **Utiliser DHCP pour obtenir des adresses de serveur DNS**. |
| **Autre serveur DNS** | Configure l'adresse IPv6 statique de l'autre serveur DNS. Pour modifier ce paramètre, vous devez tout d'abord décocher **Utiliser DHCP pour obtenir des adresses de serveur DNS**. |

**Tableau 4-6. Paramètres IPMI**

| Paramètre | Description |
|---|---|
| **Activer IPMI sur LAN** | Lorsque ce paramètre est coché, il indique que le canal LAN IPMI est activé. La valeur par défaut est **Désactivé**. |
| **Limite du niveau de privilège du canal** | Configure le niveau de privilège minimal, pour l'utilisateur, qui peut être accepté sur le canal LAN. Sélectionnez l'une des options suivantes : **Administrateur**, **Opérateur** ou **Utilisateur**. L'option par défaut est **Administrateur**. |
| **Clé de cryptage** | Configure la clé de cryptage : 0 à 20 caractères hexadécimaux (aucun blanc autorisé). La valeur par défaut est tous les zéros. |

**Tableau 4-7. Paramètres VLAN**

| Paramètre | Description |
|---|---|
| **Activer le numéro VLAN** | Si cette option est activée, seul le trafic du numéro du LAN virtuel (VLAN) est accepté. |

**Tableau 4-7. Paramètres VLAN**

| Paramètre | Description |
|---|---|
| **Identifiant du VLAN** | Champ N° VLAN des champs 802.1g. Saisissez une valeur valide pour le numéro du VLAN (doit être un numéro entre 1 et 4 094). |
| **Priorité** | Champ Priorité des champs 802.1g. Saisissez un numéro entre 0 et 7 pour définir la priorité du numéro du VLAN. |

## Configuration du filtrage IP et du blocage IP

**REMARQUE :** vous devez disposer du droit **Configurer iDRAC** pour effectuer les étapes suivantes.

1. Cliquez sur **Paramètres iDRAC→ Réseau/Sécurité**, puis cliquez sur l'onglet **Réseau** pour ouvrir la page **Réseau**.
2. Cliquez sur **Paramètres avancés** pour configurer les paramètres de sécurité réseau.

   Le Tableau 4-8 décrit les **paramètres de la page Sécurité réseau**.
3. Après la reconfiguration des paramètres, cliquez sur **Appliquer**.

   Enregistre les nouveaux paramètres que vous avez créés dans la page Sécurité réseau.

**Tableau 4-8. Paramètres de la page Sécurité réseau**

| Paramètres | Description |
|---|---|
| **Plage IP activée** | Active la fonctionnalité Vérification de la plage IP, qui définit une plage d'adresses IP pouvant accéder à iDRAC. La valeur par défaut est **Désactivé**. |
| **Adresse de la plage IP** | Détermine le format binaire d'adresse IP accepté, en fonction des 1 dans le masque de sous-réseau. Cette valeur correspond à l'opérateur de bits AND avec le masque de sous-réseau de la plage IP pour déterminer la partie supérieure de l'adresse IP autorisée. Toute adresse IP comportant ce format binaire dans ses bits supérieurs est autorisée à établir une session iDRAC6. Les ouvertures de session à partir des adresses IP qui sont situées à l'extérieur de cette plage échouent. Les valeurs par défaut dans chaque propriété permettent à une plage d'adresses de 192.168.1.0 à 192.168.1.255 d'établir une session iDRAC6. |

**Tableau 4-8. Paramètres de la page Sécurité réseau *(suite)***

| Paramètres | Description |
|---|---|
| **Masque de sous-réseau de la plage IP** | Définit les positions binaires significatives dans l'adresse IP. Le masque de sous-réseau doit avoir la forme d'un masque de réseau, où les bits de plus fort poids sont tous des 1 avec une transition simple vers tous les zéros dans les bits de niveau inférieur. L'adresse par défaut est **255.255.255.0**. |
| **Blocage IP activé** | Active la fonctionnalité Blocage d'adresse IP, qui limite le nombre d'échecs de tentatives d'ouverture de session à partir d'une adresse IP spécifique pendant une durée présélectionnée. La valeur par défaut est **Désactivé**. |
| **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. Le nombre par défaut est **10**. |
| **Plage d'échecs avant blocage IP** | Détermine la période en secondes pendant laquelle des échecs du nombre d'échecs avant blocage IP doivent se produire pour déclencher la période de pénalité avant blocage IP. La période par défaut est **3 600**. |
| **Période de pénalité avant blocage IP** | Durée en secondes pendant laquelle les tentatives d'ouverture de session à partir d'une adresse IP avec un nombre d'échecs excessif sont rejetées. La période par défaut est **3 600**. |

# Configuration des événements sur plateforme

La configuration des événements sur plateforme offre un outil de configuration d'iDRAC6 pour effectuer les actions sélectionnées sur certains messages d'événement. Ces actions incluent Pas d'action, Redémarrer le système, Exécuter un cycle d'alimentation sur le système, Arrêter le système et Générer une alerte (interruption d'événements sur plateforme [PET] et/ou par e-mail).

Les événements sur plateforme filtrables sont répertoriés dans Tableau 4-9.

**Tableau 4-9. Filtres d'événements sur plateforme**

| Index | Événement sur plateforme |
|---|---|
| 1 | Assertion de ventilateur critique |
| 2 | Assertion d'avertissement concernant la batterie |
| 3 | Assertion critique de la batterie |
| 4 | Assertion critique de la tension |
| 5 | Assertion d'avertissement concernant la température |
| 6 | Assertion critique de la température |
| 7 | Assertion critique d'intrusion |
| 8 | Redondance dégradée |
| 9 | Perte de la redondance |
| 10 | Assertion d'avertissement concernant le processeur |
| 11 | Assertion critique du processeur |
| 12 | Assertion critique du processeur absent |
| 13 | Assertion d'avertissement concernant le bloc d'alimentation |
| 14 | Assertion critique du bloc d'alimentation |
| 15 | Assertion critique du bloc d'alimentation absent |
| 16 | Assertion critique du journal des événements |
| 17 | Assertion critique de la surveillance |
| 18 | Assertion d'avertissement concernant l'alimentation système |
| 19 | Assertion critique de l'alimentation système |
| 20 | Assertion informative du média Flash amovible absent |
| 21 | Assertion critique du média Flash amovible |
| 22 | Assertion d'avertissement du média Flash amovible |

Lorsqu'un événement sur plateforme se produit (par exemple, une assertion d'avertissement concernant la batterie), un événement système est généré et enregistré dans le journal des événements système (SEL). Si cet événement correspond à un filtre d'événements sur plateforme (PEF) activé et si vous avez configuré le filtre pour générer une alerte (PET ou par e-mail), une alerte PET ou par e-mail est alors envoyée à une ou plusieurs destinations configurées.

Si le même filtre d'événements sur plateforme est également configuré pour effectuer une action (tel qu'un redémarrage du système), l'action est effectuée.

### Configuration des filtres d'événements sur plateforme (PEF)

**REMARQUE :** configurez des filtres d'événements sur plateforme avant de configurer les interruptions d'événement sur plateforme ou les paramètres d'alerte par e-mail.

1. Ouvrez une session sur le système distant à l'aide d'un navigateur Web pris en charge. Voir « Accès à l'interface Web », à la page 48.
2. Cliquez sur **Système→ Alertes→ Événements sur plateforme**.
3. Sous **Configuration des filtres d'événements sur plateforme**, sélectionnez l'option **Activé** pour **activer les alertes de filtre d'événements sur plateforme**.

   **REMARQUE :** **activer les alertes de filtres d'événements sur plateforme** doit être activé pour qu'une alerte soit envoyée à une destination configurée valide (PET ou e-mail).
4. Dans le tableau **Liste des filtres d'événements sur plateforme**, effectuez les opérations suivantes pour le(s) filtre(s) que vous souhaitez configurer :
   - Sélectionnez l'une des actions suivantes :
     - Redémarrer le système
     - Exécuter un cycle d'alimentation sur le système
     - Arrêter le système
     - Pas d'action
   - Dans la colonne **Génération d'une alerte**, cochez la case pour activer la génération des alertes ou décochez la case pour désactiver la génération des alertes pour l'action sélectionnée.

**REMARQUE :** **générer une alerte** doit être activé pour qu'une alerte soit envoyée à une destination configurée valide (PET).

5 Cliquez sur **Appliquer**. Les paramètres sont enregistrés.

## Configuration des interruptions d'événement sur plateforme (PET)

**REMARQUE :** vous devez disposer du droit **Configurer iDRAC** pour ajouter ou activer/désactiver une alerte SNMP. Les options suivantes ne sont pas disponibles si vous ne disposez pas du droit **Configurer iDRAC**.

1 Ouvrez une session sur le système distant à l'aide d'un navigateur Web pris en charge.

2 Assurez-vous d'avoir effectué les procédures dans « Configuration des filtres d'événements sur plateforme (PEF) », à la page 61.

3 Cliquez sur **Système→ Alertes→ Paramètres d'interruptions**.

4 Dans la **liste des destinations iPv4** ou dans la **liste des destinations iPv6**, effectuez les opérations suivantes de sorte que le **numéro de destination** configure la destination de l'alerte SNMP IPv4 ou IPv6 :

   a Cochez ou décochez la case **État**. Une case cochée indique que l'adresse IP est activée pour recevoir les alertes. Une case décochée indique que l'adresse IP est désactivée pour recevoir les alertes.

   b Dans **Adresse IPv4 de destination** ou **Adresse IPv6 de destination**, entrez une adresse IP de destination d'interruption d'événement sur plateforme valide.

   c Dans **Interruption test**, cliquez sur **Envoyer** pour tester l'alerte configurée.

   **REMARQUE :** votre compte d'utilisateur doit avoir le droit **Alertes test** afin d'envoyer une interruption test. Pour en savoir plus, voir Tableau 6-6.

   Les modifications que vous avez spécifiées s'affichent dans la **liste des destinations** IPv4 ou iPv6.

5 Dans le champ **Chaîne de la communauté**, saisissez le nom de la communauté SNMP iDRAC.

   **REMARQUE :** la chaîne de la communauté de destination doit être la même que la chaîne de la communauté iDRAC6.

6 Cliquez sur **Appliquer**. Les paramètres sont enregistrés.

**REMARQUE :** si vous désactivez un filtre d'événements sur plateforme, l'interruption associée à ce capteur « défaillant » est également désactivée. Si l'option **Activer les alertes du filtre des évènements de la plateforme** est activée, les interruptions associées aux transitions « mauvais à bon » sont toujours générées. Par exemple, si vous désactivez l'option **Génération d'une alerte** pour le **Filtre d'assertion informative du média Flash amovible** et retirez la carte SD, l'interruption associée n'est pas affichée. L'interruption est générée si vous insérez à nouveau la carte SD. En revanche, si vous activez l'option **Activer les alertes du filtre des évènements de la plateforme**, une interruption est générée lorsque vous retirez ou insérez la carte SD.

## Configuration des alertes par e-mail

**REMARQUE :** si vous utilisez le serveur de messagerie Microsoft Exchange Server 2007, veillez à ce que le nom de domaine d'iDRAC soit configuré de sorte que le serveur de messagerie puisse recevoir les alertes par e-mail émanant d'iDRAC.

**REMARQUE :** les alertes par e-mail prennent en charge les adresses IPv4 et IPv6.

1. Ouvrez une session sur le système distant à l'aide d'un navigateur Web pris en charge.
2. Assurez-vous d'avoir effectué les procédures dans « Configuration des filtres d'événements sur plateforme (PEF) », à la page 61.
3. Cliquez sur **Système→ Alertes→ Paramètres d'alertes par e-mail**.
4. Dans le tableau **Adresses e-mail de destination**, effectuez les opérations suivantes pour configurer une adresse de destination pour le **numéro d'alerte par e-mail** :
   a. Cochez ou décochez la case **État**. Une case cochée indique que l'adresse e-mail est activée pour recevoir les alertes. Une case décochée indique que l'adresse e-mail est désactivée pour recevoir les alertes.
   b. Dans le champ **Adresse e-mail de destination**, tapez une adresse e-mail valide.
   c. Dans le champ **Description de l'e-mail**, tapez une brève description.
5. Dans **E-mail test**, cliquez sur **Envoyer** pour tester les paramètres des alertes par e-mail configurés.
6. Dans le champ **Adresse IP du serveur SMTP (e-mail),** saisissez une adresse IP valide ou le FQDN (fully qualified domain name - nom de domaine complet) du serveur SMTP à utiliser au cours de la configuration.

**REMARQUE :** pour envoyer un e-mail test avec succès, l'**adresse IP du serveur SMTP (e-mail)** doit être configurée sur la page **Paramètres d'alertes par e-mail**. Le serveur SMTP utilise l'adresse IP définie pour communiquer avec iDRAC6 afin d'envoyer des alertes par e-mail lorsqu'un événement sur plateforme se produit.

7 Cliquez sur **Appliquer**. Les paramètres sont enregistrés.

### Configuration IPMI via l'interface Web

1 Ouvrez une session sur le système distant à l'aide d'un navigateur Web pris en charge.

2 Configurez IPMI sur LAN.

a Dans l'arborescence du **Système**, cliquez sur **Paramètres iDRAC**.

b Cliquez sur l'onglet **Réseau/Sécurité**, puis sur **Réseau**.

c Sur la page **Réseau** sous **Paramètres IPMI**, sélectionnez **Activer IPMI sur LAN** et cliquez sur **Appliquer**.

d Mettez à jour les privilèges de canal LAN IPMI, si nécessaire.

**REMARQUE :** ce paramètre détermine les commandes IPMI qui peuvent être exécutées à partir de l'interface IPMI sur LAN. Pour plus d'informations, consultez les spécifications d'IPMI 2.0.

Sous **Paramètres IPMI**, cliquez sur le menu déroulant **Limite du niveau de privilège du canal**, sélectionnez **Administrateur**, **Opérateur** ou **Utilisateur** et cliquez sur **Appliquer**.

e Définissez la clé de cryptage du canal LAN IPMI, si nécessaire.

**REMARQUE :** l'interface IPMI iDRAC6 prend en charge le protocole RMCP+.

Sous **Paramètres LAN IPMI** dans le champ **Clé de cryptage**, tapez la clé de cryptage et cliquez sur **Appliquer**.

**REMARQUE :** la clé de cryptage doit se composer d'un nombre pair de caractères hexadécimaux d'un maximum de 40 caractères.

3 Configurez Communications série IPMI sur le LAN (SOL).

a Dans l'arborescence du **Système**, cliquez sur **Paramètres iDRAC**.

b Cliquez sur l'onglet **Sécurité réseau**, puis sur **Communications série sur LAN**.

c Sur la page **Communications série sur LAN**, sélectionnez **Activer les communications série sur LAN**.

d Mettez à jour le débit en bauds d'IPMI SOL.

**REMARQUE :** pour rediriger la console série sur LAN, assurez-vous que le débit en bauds de SOL est identique au débit en bauds de votre système géré.

e Cliquez sur le menu déroulant **Débit en bauds**, sélectionnez le débit en bauds approprié et cliquez sur **Appliquer**.

f Mettez à jour le privilège requis minimal. Cette propriété définit le privilège utilisateur minimal qui est requis pour utiliser la fonctionnalité **Communications série sur LAN**.

Cliquez sur le menu déroulant **Limite du niveau de privilège du canal**, puis sélectionnez **Utilisateur**, **Opérateur** ou **Administrateur**.

g Cliquez sur **Appliquer**.

4 Configurez les communications IPMI série.

a Dans l'onglet **Réseau/Sécurité**, cliquez sur **Série**.

b Dans le menu **Série**, remplacez le mode de connexion des communications série IPMI par le paramètre approprié.

Sous **Communications série IPMI**, cliquez sur le menu déroulant **Paramètres du mode de connexion** et sélectionnez le mode approprié.

c Configurez le débit en bauds des communications IPMI série.

Cliquez sur le menu déroulant **Débit en bauds**, sélectionnez le débit en bauds approprié et cliquez sur **Appliquer**.

d Définissez la **limite du niveau de privilège du canal** et le **contrôle du débit**.

e Cliquez sur **Appliquer**.

f Assurez-vous que MUX série est correctement défini dans le programme de configuration du BIOS du système géré.

- Redémarrez le système.
- Pendant le POST, appuyez sur <F2> pour accéder au programme de configuration du BIOS.
- Naviguez vers **Communications série**.

- Dans le menu **Connexion série**, assurez-vous que **Connecteur série externe** est défini sur **Périphérique d'accès à distance**.
- Enregistrez et quittez le programme de configuration du BIOS.
- Redémarrez le système.

Si les communications série IPMI sont en mode terminal, vous pouvez configurer les paramètres supplémentaires suivants :

- Contrôle de la suppression
- Contrôle d'écho
- Modification de ligne
- Nouvelles séquences linéaires
- Saisie de nouvelles séquences linéaires

Pour plus d'informations sur ces propriétés, voir la spécification d'IPMI 2.0. Pour en savoir plus sur les commandes en mode terminal, voir le *Guide d'utilisation des utilitaires du contrôleur de gestion de la carte mère Dell OpenManage* à l'adresse **dell.com/support/manuals**.

## Configuration des utilisateurs d'iDRAC6

Voir la section « Ajout et configuration d'utilisateurs iDRAC6 », à la page 135 pour obtenir des informations détaillées.

## Sécurisation des communications iDRAC6 à l'aide de certificats SSL et numériques

Cette section fournit des informations sur les fonctionnalités de sécurité des données suivantes intégrées à votre iDRAC :

- Secure Sockets Layer (SSL)
- Requête de signature de certificat (RSC)
- Accès à SSL via l'interface Web
- Génération d'une RSC
- Téléversement d'un certificat de serveur
- Affichage d'un certificat de serveur

### Secure Sockets Layer (SSL)

iDRAC6 inclut un serveur Web qui est configuré pour utiliser le protocole de sécurité SSL standard de l'industrie afin de transférer des données cryptées sur un réseau. Basé sur la technologie de cryptage par clé publique et clé privée, SSL est une technologie répandue permettant la communication authentifiée et cryptée entre les clients et les serveurs afin d'empêcher toute écoute indiscrète au sein d'un réseau.

Un système activé SSL peut effectuer les tâches suivantes :

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

Le processus de cryptage fournit un haut niveau de protection de données. iDRAC6 applique la norme de cryptage SSL à 128 bits, la forme la plus sécurisée de cryptage généralement disponible pour les navigateurs Internet en Amérique du Nord.

Le serveur Web iDRAC6 dispose d'un certificat numérique SSL autosigné Dell (référence serveur) par défaut. Pour garantir un niveau de sécurité élevé sur Internet, remplacez le certificat SSL du serveur Web par un certificat signé par une autorité de certification connue. Pour lancer le processus d'obtention d'un certificat signé, vous pouvez utiliser l'interface Web iDRAC6 pour générer une requête de signature de certificat (RSC) avec les informations de votre société. Vous pouvez ensuite envoyer la RSC générée à une autorité de certification (AC) telle que VeriSign ou Thawte.

### Requête de signature de certificat (RSC)

Une RSC est une requête numérique envoyée à une AC en vue d'obtenir un certificat de serveur sécurisé. Les certificats de serveur sécurisés permettent aux clients du serveur de faire confiance à l'identité du serveur auquel ils se sont connectés et de négocier une session cryptée avec le serveur.

Une autorité de certification est une entité commerciale reconnue dans l'industrie de l'informatique pour ses critères élevés en matière d'analyse et d'identification fiables et d'autres critères de sécurité importants. Thawte et VeriSign sont des exemples d'AC. Une fois que l'AC reçoit une RSC, elle la contrôle et vérifie les informations qu'elle contient. Si le postulant remplit les normes de sécurité de l'AC, cette dernière émet un certificat signé numériquement qui identifie de manière exclusive le postulant pour les transactions effectuées sur des réseaux et sur Internet.

Une fois que l'AC approuve la RSC et envoie le certificat, téléversez ce dernier sur le micrologiciel iDRAC6. Les informations de la RSC stockés sur le micrologiciel iDRAC6 doivent correspondre aux informations contenues dans le certificat.

## Accès à SSL via l'interface Web

1. Cliquez sur **Paramètres iDRAC→ Réseau/Sécurité**.
2. Cliquez sur **SSL** pour ouvrir la page **SSL**.

Utilisez la page **SSL** pour effectuer l'une des options suivantes :

- Générer une requête de signature de certificat (RSC) à envoyer à une AC. Les informations de la RSC sont stockées dans le micrologiciel iDRAC6.
- Téléverser un certificat de serveur.
- Afficher un certificat de serveur.

Le Tableau 4-10 décrit les options de la page **SSL** ci-dessus.

**Tableau 4-10. Options de la page SSL**

| Champ | Description |
|---|---|
| **Générer une requête de signature de certificat (RSC)** | Cette option vous permet de générer une RSC à envoyer à une AC pour demander un certificat Web sécurisé.<br>**REMARQUE :** chaque nouvelle RSC supplante celle qui se trouve déjà sur le micrologiciel. La RSC présente dans le micrologiciel doit correspondre au certificat renvoyé par l'autorité de certification. |

**Tableau 4-10. Options de la page SSL**

| Champ | Description |
|---|---|
| **Téléverser un certificat de serveur** | Cette option vous permet de téléverser un certificat existant appartenant à votre société et qui est utilisé pour contrôler l'accès à iDRAC6.<br>**REMARQUE :** iDRAC6 accepte uniquement les certificats X509 encodés en base 64. Les certificats encodés DER ne sont pas acceptés. Téléversez un nouveau certificat pour remplacer le certificat par défaut que vous avez reçu avec votre iDRAC6. |
| **Afficher le certificat de serveur** | Cette option vous permet d'afficher un certificat de serveur existant. |

## Génération d'une requête de signature de certificat

1. À la page **SSL**, sélectionnez **Générer une requête de signature de certificat (RSC)**, puis cliquez sur **Suivant**.
2. Sur la page **Générer une requête de signature de certificat (RSC)**, saisissez une valeur pour chaque attribut de la RSC. Le Tableau 4-11 décrit les attributs de la RSC.
3. Cliquez sur **Générer** pour créer la RSC, le télécharger sur votre ordinateur local et l'enregistrer sur un répertoire spécifié.
4. Cliquez sur **Retourner au menu principal SSL** pour retourner à la page SSL.

**Tableau 4-11. Générer des attributs de requête de signature de certificat (RSC)**

| Champ | Description |
|---|---|
| **Nom commun** | Nom exact à certifier (normalement, le nom de domaine d'iDRAC, par exemple, **sociétéxyz.com**). Les caractères alphanumériques, les tirets et les points sont valides. |
| **Nom de l'organisation** | Nom associé à cette organisation (par exemple, Entreprise XYZ). Les caractères alphanumériques, les tirets et les points sont valides. |
| **Unité organisationnelle** | Nom associé à une division opérationnelle, comme un département (par exemple, Informatique). Les caractères alphanumériques, les tirets et les points sont valides. |

**Tableau 4-11. Générer des attributs de requête de signature de certificat (RSC) *(suite)***

| Champ | Description |
|---|---|
| Ville | Ville ou autre lieu où se trouve l'entité à certifier (par exemple, Round Rock). Les caractères alphanumériques, les tirets et les points sont valides. |
| Nom de l'état | État ou province où se trouve l'entité qui fait la demande de certification (par exemple, Texas). Les caractères alphanumériques, les tirets et les points sont valides. N'utilisez pas d'abréviations. |
| Code de pays | Nom du pays où se trouve l'entité qui fait la demande de certification. |
| E-mail | Adresse e-mail associée à la RSC. Tapez l'adresse e-mail de la société ou toute autre adresse e-mail associée à la RSC. Ce champ est optionnel. |

## Téléversement d'un certificat de serveur

1 À la page **SSL,** sélectionnez **Téléverser un certificat de serveur,** puis cliquez sur **Suivant**.

La page **Téléverser un certificat de serveur** s'affiche.

2 Dans le champ **Chemin du fichier**, tapez le chemin du certificat dans le champ **Valeur** ou cliquez sur **Parcourir** pour naviguer vers le fichier du certificat.

**REMARQUE :** La valeur **Chemin du fichier** affiche le chemin de fichier relatif du certificat que vous téléversez. Vous devez saisir le chemin de fichier absolu, qui comprend le chemin et le nom de fichier complets et l'extension du fichier.

3 Cliquez sur **Appliquer**.

4 Cliquez sur **Retourner au menu principal SSL** pour retourner à la page **principale du menu SSL**.

## Affichage d'un certificat de serveur

1 À la page **SSL**, sélectionnez **Afficher un certificat de serveur**, puis cliquez sur **Suivant**.

La page **Afficher un certificat de serveur** affiche le certificat de serveur que vous avez téléversé vers iDRAC.

Le Tableau 4-12 décrit les champs et les descriptions associées énumérés dans le tableau **Certificat**.

2 Cliquez sur **Retourner au menu principal SSL** pour retourner à la page **principale du menu SSL**.

**Tableau 4-12. Informations relatives au certificat**

| Champ | Description |
|---|---|
| **Numéro de série** | Numéro de série du certificat |
| **Informations sur le sujet** | Attributs du certificat saisis par le sujet |
| **Informations sur l'émetteur** | Attributs du certificat renvoyés par l'émetteur |
| **Valide du** | Date d'émission du certificat |
| **Valide jusqu'au** | Date d'expiration du certificat |

# Configuration et gestion d'Active Directory

La page vous permet de configurer et de gérer les paramètres d'Active Directory.

**REMARQUE :** vous devez avoir le droit **Configurer iDRAC** afin d'utiliser ou de configurer Active Directory.

**REMARQUE :** avant de configurer ou d'utiliser la fonctionnalité Active Directory, assurez-vous que votre serveur Active Directory est configuré pour communiquer avec iDRAC6.

**REMARQUE :** pour de plus amples informations sur la configuration d'Active Directory et la manière de configurer Active Directory avec le schéma ÉTendu ou le schéma standard, voir « Utilisation du service de répertoire iDRAC6 », à la page 151.

Pour accéder à la page **Configuration et gestion d'Active Directory** :

1 Cliquez sur **Paramètres iDRAC→ Réseau/Sécurité**.

2 Cliquez sur **Active Directory** pour ouvrir la page **Configuration et gestion d'Active Directory**.

Le Tableau 4-13 énumère les options de la page **Configuration et gestion d'Active Directory**.

3 Cliquez sur **Configurer Active Directory** pour configurer Active Directory. Voir « Utilisation du service de répertoire iDRAC6 », à la page 151 pour des informations détaillées sur la configuration.

4 Cliquez sur **Tester les paramètres** pour tester la configuration Active Directory à l'aide des paramètres spécifiés. Voir « Utilisation du service de répertoire iDRAC6 », à la page 151 pour des informations détaillées sur l'utilisation de l'option Tester les paramètres.

**Tableau 4-13. Options de la page Configuration et gestion d'Active Directory**

| Attribut | Description |
|---|---|
| **Paramètres communs** | |
| **Active Directory activé** | Spécifie si Active Directory est activé ou désactivé. |
| **Connexion directe activée** | Spécifie si la connexion directe est activée ou désactivée. Si elle est activée, vous pouvez ouvrir une session sur iDRAC6 sans saisir vos références d'utilisateur de domaine, par exemple le nom d'utilisateur et le mot de passe. Cochez la case pour activer la connexion directe. |
| **Sélection de schéma** | Spécifie si le schéma standard ou le schéma étendu est utilisé avec Active Directory.<br>**REMARQUE :** dans cette version, la fonctionnalité Authentification bifactorielle (TFA) articulée autour de la carte à puce n'est pas prise en charge si Active Directory est configuré pour le schéma étendu. La fonctionnalité Connexion directe (SSO) est prise en charge par le schéma standard et le schéma étendu. |
| **Nom de domaine de l'utilisateur** | Cette valeur contient jusqu'à 40 entrées de domaine d'utilisateur. Si elle est configurée, la liste des noms de domaine d'utilisateur apparaît dans la page d'ouverture de session comme un menu déroulant à partir duquel l'utilisateur d'ouverture de session doit effectuer un choix. Si elle n'est pas configurée, les utilisateurs d'Active Directory sont toujours en mesure d'ouvrir une session en saisissant le nom d'utilisateur au format nom_d'utilisateur@nom_de_domaine, nom_de_domaine/nom_d'utilisateur ou nom_de-_domaine\nom_d'utilisateur. |

**Tableau 4-13. Options de la page Configuration et gestion d'Active Directory *(suite)***

| Attribut | Description |
|---|---|
| **Délai d'attente** | Spécifie la durée, en secondes, accordée aux requêtes Active Directory pour qu'elles se terminent. La valeur par défaut est 120 secondes. |
| **Rechercher les contrôleurs de domaine avec DNS** | Sélectionnez l'option **Rechercher les contrôleurs de domaine avec DNS** pour obtenir les contrôleurs de domaine Active Directory émanant d'une recherche DNS. Lorsque cette option est sélectionnée, les adresses des serveurs des contrôleurs de domaine 1 à 3 sont ignorées. Sélectionnez **Domaine utilisateur de l'ouverture de session** pour effectuer la recherche DNS avec le nom de domaine de l'utilisateur d'ouverture de session. Sinon, sélectionnez **Définir un domaine** et saisissez le nom de domaine à utiliser pour la recherche DNS. iDRAC6 tente de se connecter à chacune des adresses (les 4 premières adresses renvoyées par la recherche DNS) l'une après l'autre jusqu'à ce qu'une connexion soit établie.<br><br>Si **Schéma étendu** est sélectionné, ces adresses sont celles des contrôleurs de domaine dans lesquels l'objet Périphérique iDRAC6 et les objets Association sont situés. Si **Schéma standard** est sélectionné, les contrôleurs de domaine sont ceux où se trouvent les comptes d'utilisateur et les groupes de rôles. |
| **Adresse du serveur du contrôleur de domaine 1-3 (FQDN ou IP)** | Spécifie le nom de domaine pleinement qualifié (FQDN) du contrôleur de domaine ou de l'adresse IP. Au moins une des 3 adresses doit être configurée. iDRAC6 tente de se connecter à chacune des adresses configurées une par une jusqu'à ce qu'une connexion soit établie. Si le schéma étendu est sélectionné, il s'agira des adresses des contrôleurs de domaine dans lesquels l'objet Périphérique 'iDRAC6 et les objets Association sont situés. Si le schéma standard est sélectionné, il s'agit des adresses des contrôleurs de domaine dans lesquels les comptes d'utilisateur et les groupes de rôles sont situés. |

**Tableau 4-13. Options de la page Configuration et gestion d'Active Directory *(suite)***

| Attribut | Description |
|---|---|
| **Validation de certificat activée** | iDRAC6 utilise le protocole SSL (Security Socket Layer) lors de la connexion à Active Directory. Par défaut, iDRAC6 utilise le certificat d'une autorité de certification chargé dans iDRAC6 pour valider le certificat de serveur SSL (Security Socket Layer) des contrôleurs de domaine durant l'établissement de liaisons SSL (Security Socket Layer) et fournit une sécurité accrue. La validation du certificat peut être désactivée à des fins de test ou bien l'administrateur système choisit de se fier aux contrôleurs de domaine dans la limite de sécurité sans valider leurs certificats SSL (Security Socket Layer). Cette option spécifie si la validation du certificat est activée ou désactivée. |
| **Certificat d'autorité de certification Active Directory** | |
| **Certificat** | Certificat de l'autorité de certificat qui signe les certificats de serveur SSL (Security Socket Layer) de tous les contrôleurs de domaine. |
| **Paramètres du schéma étendu** | **Nom iDRAC :** spécifie le nom qui identifie de manière unique iDRAC dans Active Directory. Cette valeur est NULL par défaut.<br>**Nom de domaine iDRAC :** nom du DNS (chaîne) du domaine où se trouve l'objet iDRAC d'Active Directory. Cette valeur est NULL par défaut.<br>Ces paramètres s'affichent uniquement si iDRAC a été configuré en vue d'une utilisation avec un schéma Active Directory étendu. |

**Tableau 4-13. Options de la page Configuration et gestion d'Active Directory *(suite)***

| Attribut | Description |
|---|---|
| **Paramètres du schéma standard** | **Adresse du serveur de catalogue global 1-3 (FQDN ou IP) :** spécifie le nom de domaine pleinement qualifié (FQDN) ou l'adresse IP du ou des serveurs de catalogue global. Au moins une des 3 adresses doit être configurée. iDRAC6 tente de se connecter à chacune des adresses configurées une par une jusqu'à ce qu'une connexion soit établie. Le serveur de catalogue global est exigé pour le schéma standard uniquement lorsque les comptes d'utilisateur et les groupes de rôles se trouvent dans des domaines différents.<br><br>**Groupes de rôles :** spécifie la liste des groupes de rôles associés à iDRAC6.<br><br>**Nom du groupe :** spécifie le nom qui identifie le groupe de rôles dans Active Directory associé à iDRAC6.<br><br>**Domaine du groupe :** spécifie le domaine du groupe.<br><br>**Privilège du groupe :** spécifie le niveau de privilège du groupe.<br><br>Ces paramètres s'affichent uniquement si iDRAC a été configuré en vue d'une utilisation avec un schéma Active Directory standard.<br><br>Sélectionnez l'option **Rechercher les serveurs de catalogue global** avec DNS et saisissez le **nom de domaine root (racine)** à utiliser dans le cadre d'une recherche DNS pour obtenir les serveurs de catalogue global Active Directory. Lorsque cette option est sélectionnée, les **adresses des serveurs de catalogue global 1 à 3** sont ignorées. iDRAC6 tente de se connecter à chacune des adresses (les 4 premières adresses renvoyées par la recherche DNS) l'une après l'autre jusqu'à ce qu'une connexion soit établie. Un serveur de catalogue global est exigé pour le schéma standard uniquement lorsque les comptes d'utilisateur et les groupes de rôles se trouvent dans des domaines différents. |

## Configuration et gestion de LDAP générique

iDRAC6 fournit une solution générique visant à prendre en charge l'authentification LDAP (Lightweight Directory Access Protocol). Cette fonctionnalité ne nécessite aucune extension de schéma au sein de vos services de répertoire. Pour des informations relatives à la configuration du service d'annuaire LDAP générique, voir « Service de répertoire LDAP générique », à la page 190.

## Configuration des services iDRAC6

**REMARQUE :** pour modifier ces paramètres, vous devez avoir le droit **Configurer iDRAC**.

1. Cliquez sur **Paramètres iDRAC→ Réseau/Sécurité**. Cliquez sur l'onglet **Services** pour afficher la page de configuration **Services**.
2. Configurez les services suivants, si nécessaire :
   - Configuration locale : voir Tableau 4-14
   - Web Server : voir Tableau 4-15 pour accéder aux paramètres Web Server.
   - SSH : voir Tableau 4-16 pour accéder aux paramètres SSH
   - Telnet : voir Tableau 4-17 pour les paramètres Telnet
   - RACADM distante : voir Tableau 4-18 pour les paramètres de la RACADM distante
   - Agent SNMP : voir Tableau 4-19 pour les paramètres SNMP
   - Agent de récupération de système automatique (ASR) : voir Tableau 4-20 pour les paramètres Agent ASR.
3. Cliquez sur **Appliquer** pour appliquer les paramètres de la page **Service**.

**Tableau 4-14. Configuration locale**

| Paramètre | Description |
|---|---|
| **Désactiver la configuration locale d'iDRAC à l'aide de l'option ROM** | Désactive la configuration locale d'iDRAC à l'aide de l'option ROM. L'option ROM se trouve dans le BIOS et fournit un moteur d'interface utilisateur qui permet la configuration de BMC et d'iDRAC. L'option ROM vous invite à saisir le module de configuration en appuyant sur <Ctrl+E>. |
| **Désactiver la configuration locale d'iDRAC avec la RACADM** | Désactive la configuration locale d'iDRAC à l'aide de la RACADM locale. |

**Tableau 4-15. Paramètres du serveur Web**

| Paramètre | Description |
|---|---|
| **Enabled (Activé)** | Active ou désactive le serveur Web iDRAC6. Lorsqu'elle est cochée, cette case indique que le serveur Web est activé. **Activé** est sélectionné par défaut. |
| **Nombre maximal de sessions** | Nombre maximal de sessions simultanées du serveur Web autorisées pour ce système. Ce champ ne peut pas être modifié. Le nombre maximal de sessions simultanées est cinq. |
| **Sessions actives** | Nombre de sessions actuelles sur le système, inférieur ou égal à la value **Nombre maximal de sessions**. Ce champ ne peut pas être modifié. |
| **Délai d'attente** | Durée, en secondes, pendant laquelle une connexion peut rester inactive. La session est annulée quand le délai d'expiration est atteint. Les modifications apportées au paramètre Délai d'expiration prennent immédiatement effet et mettent fin à la session d'interface Web en cours. Le serveur Web est également réinitialisé. Veuillez attendre quelques minutes avant d'ouvrir une nouvelle session d'interface Web. La plage du délai d'expiration est de 60 à 10 800 secondes. La valeur par défaut est de 1 800 secondes. |

**Tableau 4-15. Paramètres du serveur Web *(suite)***

| Paramètre | Description |
|---|---|
| Numéro de port HTTP | Port sur lequel iDRAC6 écoute une connexion au navigateur. Le numéro de port par défaut est 80. |
| Numéro de port HTTPS | Port sur lequel iDRAC6 écoute une connexion au navigateur sécurisée. Le numéro de port par défaut est 443. |

**Tableau 4-16. Paramètres SSH**

| Paramètre | Description |
|---|---|
| Enabled (Activé) | Active ou désactive SSH. Lorsqu'il est coché, SSH est activé. |
| Nombre maximal de sessions | Nombre maximal de sessions SSH?simultanées autorisées pour ce système. Vous ne pouvez pas modifier ce champ.<br>**REMARQUE :** iDRAC6 prend en charge jusqu'à 2 sessions SSH simultanées. |
| Sessions actives | Nombre de sessions SSH actuelles sur le système, inférieur ou égal au paramètre **Nombre maximal de sessions**. Vous ne pouvez pas modifier ce champ. |
| Délai d'attente | Délai d'expiration en cas d'inactivité Secure Shell, en secondes. La plage du délai d'expiration est de 60 à 10 800 secondes. Saisissez 0 seconde pour désactiver la fonctionnalité Délai d'expiration. La valeur par défaut est 1 800. |
| Numéro de port | Port sur lequel iDRAC6 écoute une connexion SSH. Le numéro de port par défaut est 22. |

**Tableau 4-17. Paramètres Telnet**

| Paramètre | Description |
|---|---|
| Enabled (Activé) | Active ou désactive Telnet. Lorsqu'il est coché, Telnet est activé. |
| Nombre maximal de sessions | Nombre maximal de sessions Telnet?simultanées autorisées pour ce système. Vous ne pouvez pas modifier ce champ.<br>**REMARQUE :** iDRAC6 prend en charge jusqu'à 2 sessions Telnet simultanément. |

**Tableau 4-17. Paramètres Telnet**

| Paramètre | Description *(suite)* |
|---|---|
| Sessions actives | Nombre de sessions Telnet actuelles sur le système, inférieur ou égal au paramètre **Nombre maximal de sessions**. Vous ne pouvez pas modifier ce champ. |
| Délai d'attente | Délai d'expiration en cas d'inactivité Telnet, en secondes. La plage du délai d'expiration est comprise entre 60 et 10 800 secondes. Saisissez 0 seconde pour désactiver la fonctionnalité Délai d'expiration. La valeur par défaut est 1 800. |
| Numéro de port | Port sur lequel iDRAC6 écoute une connexion Telnet. Le numéro de port par défaut est **23**. |

**Tableau 4-18. Paramètres de la RACADM distante**

| Paramètre | Description |
|---|---|
| Enabled (Activé) | Active/Désactive la RACADM distante. Lorsqu'il est coché, la RACADM distante est activée. |
| Sessions actives | Nombre de sessions de la RACADM distante actuelles sur le système. Vous ne pouvez pas modifier ce champ. |

**Tableau 4-19. Paramètres SNMP**

| Paramètre | Description |
|---|---|
| Enabled (Activé) | Active/Désactive SNMP. Lorsqu'il est coché, SNMP est activé. |
| Nom de la communauté SNMP | Active/Désactive le nom de la communauté SNMP. Lorsqu'il est coché, le nom de la communauté SNMP est activé. Définissez la chaîne de la communauté SNMP à utiliser. Le nom de la communauté peut contenir jusqu'à 31 caractères (sans espaces). La valeur par défaut est **public**. |

**Tableau 4-20. Paramètre de l'agent de récupération de système automatique**

| Paramètre | Description |
|---|---|
| Enabled (Activé) | Active/Désactive l'agent de récupération de système automatique. Lorsqu'il est coché, l'agent de récupération de système automatique est activé. |

# Mise à jour de l'image de récupération des services du micrologiciel iDRAC6/système

**REMARQUE :** si le micrologiciel iDRAC6 devient corrompu, ce qui peut être le cas lorsque la progression de la mise à jour du micrologiciel iDRAC6 est interrompue avant qu'elle ne se termine, vous pouvez récupérer iDRAC6 à l'aide de l'interface Web iDRAC6.

**REMARQUE :** par défaut, la mise à jour du micrologiciel conserve les paramètres iDRAC6 actuels. Lors du processus de mise à jour, vous avez la possibilité de réinitialiser les paramètres d'usine de la configuration d'iDRAC6. Si vous définissez la configuration sur les paramètres d'usine, vous devez configurer le réseau à l'aide de l'utilitaire de configuration d'iDRAC6.

1. Ouvrez l'interface Web iDRAC6 et ouvrez une session sur le système distant.
2. Cliquez sur **Paramètres iDRAC**, puis cliquez sur l'onglet **Mettre à jour**.
3. Sur la page **Téléverser/Restaurer (Étape 1 sur 3)**, cliquez sur **Parcourir** pour sélectionner l'image de micrologiciel téléchargée à l'adresse **support.dell.com** ou l'image de récupération des services du système.

   **REMARQUE :** si vous exécutez Firefox, le curseur de texte n'apparaît pas dans le champ **Image de micrologiciel**.

   Par exemple :

   `C:\Updates\V1.0\<nom_de_l'image>`.

   OU

   `\\192.168.1.10\Mises à jour\V1.0\<nom_de_l'image>`

   Par défaut, le nom de l'image de micrologiciel est **firmimg.d6**.
4. Cliquez sur **Téléverser**.

   Le fichier va se téléverser vers iDRAC6. This process may take several minutes to complete.
   (Ce processus peut prendre plusieurs minutes.)

   Le message suivant s'affiche jusqu'à la fin du processus :

   `Téléversement du fichier en cours...`

5 À la page **Condition (page 2 sur 3)**, vous voyez les résultats de la validation effectuée sur le fichier image que vous avez téléversé.

- Si le fichier image de récupération du système s'est téléversé avec succès et a passé tous les points de vérification, le nom du fichier image s'affiche. Si l'image de micrologiciel a été téléversée, les versions actuelles et nouvelles du micrologiciel s'affichent.

  OU

- Si l'image ne s'est pas téléversée avec succès ou si elle n'a pas passé les points de vérification, un message d'erreur approprié s'affiche et la mise à jour retourne à la page **Téléverser/Restaurer (Étape 1 sur 3)**. Vous pouvez réessayer de mettre à jour iDRAC6 ou cliquer sur **Annuler** pour réinitialiser iDRAC6 sur le mode de fonctionnement normal.

6 Dans le cas d'une image de micrologiciel, la fonction **Conserver la configuration** vous donne la possibilité de conserver ou de supprimer la configuration existante d'iDRAC6. Cette option est sélectionnée par défaut.

**REMARQUE :** si vous décochez la case **Préserver la configuration**, les paramètres par défaut d'iDRAC6 sont rétablis. Dans les paramètres par défaut, le LAN est activé avec une adresse IPv4 statique. Vous ne pouvez pas ouvrir une session sur l'interface Web iDRAC6. Vous devez reconfigurer les paramètres du LAN à l'aide de l'utilitaire de configuration iDRAC6 pendant le POST du BIOS.

7 Cliquez sur **Mettre à jour** pour démarrer le processus de mise à jour.

8 La page **Mise à jour (Étape 3 sur 3)** affiche la condition de la mise à jour. La progression de la mise à jour, indiquée en pourcentage, apparaît dans la colonne **Progression**.

**REMARQUE :** lorsque vous êtes en mode mise à jour, le processus de mise à jour continue en fond d'écran même si vous naviguez en dehors de cette page.

Si la mise à jour du micrologiciel est terminée, iDRAC6 se réinitialise automatiquement. Vous devez fermer la fenêtre du navigateur ouverte et vous reconnecter à iDRAC6 avec une nouvelle fenêtre de navigateur. Un message d'erreur approprié s'affiche si une erreur se produit.

Si la mise à jour de la récupération des services du système réussit/échoue, un message de condition approprié s'affiche.

### Restauration du micrologiciel iDRAC6

iDRAC6 peut maintenir deux images de micrologiciel simultanées. Vous pouvez décider de démarrer à partir de (restaurer vers) l'image de micrologiciel de votre choix.

1. Ouvrez l'interface Web iDRAC6 et ouvrez une session sur le système distant.

   Cliquez sur **Système→Paramètres iDRAC**, puis cliquez sur l'onglet **Mettre à jour**.

2. À la page **Téléverser/Restaurer (Étape 1 sur 3)**, cliquez sur **Restaurer**. La version actuelle et la version restaurée du micrologiciel s'affichent à la page **Condition (Étape 2 sur 3)**.

   **Conserver la configuration** vous donne la possibilité de conserver ou de supprimer la configuration iDRAC6 existante. Cette option est sélectionnée par défaut.

   **REMARQUE :** si vous décochez la case **Préserver la configuration**, les paramètres par défaut d'iDRAC6 sont rétablis. Dans les paramètres par défaut, le LAN est activé. Vous ne pouvez pas ouvrir une session sur l'interface Web iDRAC6. Vous devez reconfigurer les paramètres LAN à l'aide de l'utilitaire de configuration iDRAC6 pendant le POST du BIOS ou à l'aide de la commande RACADM (disponible localement sur le serveur).

3. Cliquez sur **Mettre à jour** pour démarrer le processus de mise à jour du micrologiciel.

   À la page **Mise à jour (Étape 3 sur 3)**, vous voyez la condition de l'opération de restauration. La progression, indiquée en pourcentage, apparaît dans la colonne **Progression**.

   **REMARQUE :** lorsque vous êtes en mode mise à jour, le processus de mise à jour continue en fond d'écran même si vous naviguez en dehors de cette page.

   Si la mise à jour du micrologiciel est terminée, iDRAC6 se réinitialise automatiquement. Vous devez fermer la fenêtre du navigateur ouverte et vous reconnecter à iDRAC6 avec une nouvelle fenêtre de navigateur.

# Syslog distant

La fonctionnalité Syslog distant d'iDRAC6 vous permet d'écrire à distance le journal du RAC et le journal des événements système (SEL) sur un serveur syslog externe. L'intégralité des journaux du serveur peut être lue depuis un journal central.

Le protocole syslog distant ne nécessite aucune authentification de l'utilisateur. Quant aux journaux à saisir dans le serveur syslog distant, assurez-vous de la connectivité réseau entre iDRAC6 et le serveur syslog distant et que le serveur syslog distant s'exécute sur le même réseau qu'iDRAC6. Les entrées du syslog distant sont des paquets UDP (User Datagram Protocol) envoyés au port syslog du serveur syslog distant. En cas de panne réseau, iDRAC6 n'envoie pas le même journal une seconde fois. La journalisation à distance est effectuée en temps réel à mesure que les journaux sont enregistrés dans le journal du RAC et le journal SEL d'iDRAC6.

Le syslog distant peut être activé via l'interface Web distante :

1. Ouvrez une fenêtre d'un navigateur Web pris en charge.
2. Ouvrez une session sur l'interface Web iDRAC6.
3. Dans l'arborescence du système, sélectionnez **Système**→ onglet **Configuration**→ **Paramètres du syslog distant**. L'écran **Paramètres du syslog distant** s'affiche.

Le Tableau 4-21 répertorie les paramètres Syslog distant.

**Tableau 4-21. Paramètres Syslog distant**

| Attribut | Description |
|---|---|
| **Syslog distant activé** | Sélectionnez cette option pour activer la transmission et la saisie à distance du syslog sur le serveur spécifié. Lorsque le syslog est activé, de nouvelles entrées de journal sont envoyées à un ou à des serveurs syslog. |
| **Serveur syslog 1–3** | Saisissez l'adresse du serveur syslog distant afin de journaliser les messages iDRAC6 tels que le journal SEL et le journal du RAC. Les adresses du serveur syslog peuvent contenir des caractères alphanumériques, -, ., : et _. |
| **Numéro de port** | Saisissez le numéro de port du serveur syslog distant. Le numéro de port doit être compris entre 1 et 65 535. Le port par défaut est 514. |

**REMARQUE :** les niveaux de gravité définis par le protocole syslog distant diffèrent des niveaux de gravité standard du journal des événements système (SEL) IPMI. Toutes les entrées du syslog distant iDRAC6 sont ainsi rapportées dans le serveur syslog avec Avis comme niveau de gravité.

L'exemple suivant illustre l'utilisation des objets de configuration et de la commande RACADM afin de modifier les paramètres du syslog distant :

```
racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogEnable [1/0] ; la valeur par défaut
est 0

racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogServer1 <nom du serveur 1> ;
la valeur par défaut est vide

racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogServer2 <nom du serveur 2> ;
la valeur par défaut est vide

racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogServer3 <nom du serveur 3> ;
la valeur par défaut est vide

racadm config -g cfgRemoteHosts -o
cfgRhostsSyslogPort <numéro de port> ; la valeur
par défaut est 514
```

# Périphérique de démarrage initial

Cette fonctionnalité vous permet de sélectionner le périphérique de démarrage initial de votre système et d'activer **Démarrer une seule fois**. Le système démarre à partir du périphérique sélectionné lors des redémarrages suivants et consécutifs, et demeure le périphérique de démarrage initial dans l'ordre de démarrage du BIOS jusqu'à ce qu'il soit remodifié depuis l'IUG iDRAC6 ou depuis la séquence de démarrage du BIOS.

Le périphérique de démarrage initial peut être sélectionné via l'interface Web distante :

1. Ouvrez une fenêtre d'un navigateur Web pris en charge.
2. Ouvrez une session sur l'interface Web iDRAC6.

3 Dans l'arborescence du système, sélectionnez **Système→ Configuration→ Périphérique de démarrage initial**. L'écran **Périphérique de démarrage initial** s'affiche.

Le Tableau 4-22 répertorie les paramètres **Périphérique de démarrage initial**.

**Tableau 4-22. Périphérique de démarrage initial**

| Attribut | Description |
|---|---|
| **Périphérique de démarrage initial** | Sélectionnez le périphérique de démarrage initial dans la liste déroulante. Le système démarrera à partir du périphérique sélectionné lors des redémarrages suivants et consécutifs. |
| **Démarrer une seule fois** | Sélectionné = Activé ; désélectionné = Désactivé. Cochez cette option pour effectuer un démarrage à partir du périphérique sélectionné lors du prochain démarrage. Ensuite, le système démarrera à partir du périphérique de démarrage initial dans l'ordre de démarrage du BIOS. |

# Partage de fichiers à distance

La fonctionnalité Partage de fichiers distant (RFS) d'iDRAC6 permet de spécifier un fichier image ISO ou IMG situé sur un partage réseau et de le rendre disponible au système d'exploitation du serveur géré en tant que lecteur virtuel en le montant comme CD/DVD ou Disquette par le biais d'un système de fichiers réseau (NFS) ou d'un système de fichiers Internet commun (CIFS).

Le format du chemin de l'image partagé CIFS est le suivant :

`//<adresse ip ou nom de domaine>/<cheminversimage>`

Le format du chemin de l'image partagé NFS est le suivant :

`<adresseIP>:/<cheminversimage>`

**REMARQUE :** si vous utilisez NFS, assurez-vous de préciser le chemin <*cheminversimage*> exact, y compris l'extension du fichier image car il respecte la casse.

**REMARQUE :** <*adresseIP*> doit être une adresse IPv4. L'adresse IPv6 n'est actuellement pas prise en charge.

Si un nom d'utilisateur contient un nom de domaine, le nom d'utilisateur doit alors être saisi au format *<nom d'utilisateur>@<domaine>*. Par exemple, **user1@dell.com** est un nom d'utilisateur valide, à l'inverse de **dell\user1**.

Un nom de fichier qui se termine par l'extension IMG est redirigé en tant que disquette virtuelle et un nom de fichier qui se termine par l'extension ISO est redirigé en tant que CD-ROM virtuel. Le partage de fichiers à distance prend uniquement en charge les formats de fichier image .IMG et .ISO.

La fonctionnalité RFS utilise l'implémentation de média virtuel sous-jacente dans iDRAC6. Vous devez posséder des privilèges Média virtuel pour procéder au montage de RFS. Si un lecteur virtuel est déjà utilisé par le média virtuel, le lecteur ne pourra alors pas être monté en tant que RFS et vice-versa. Pour que RFS fonctionne, le média virtuel dans iDRAC6 doit alors être en mode *Connecter* ou *Connecter automatiquement*.

L'état de la connexion de RFS est disponible dans le journal iDRAC6. Une fois connecté, un lecteur virtuel monté en tant que RFS ne se déconnecte pas, même si vous fermez la session sur iDRAC6. La connexion RFS est fermée si iDRAC6 est réinitialisé ou si la connexion réseau est coupée. Les options de l'interface utilisateur et de la ligne de commande sont également disponibles dans iDRAC6 afin de fermer la connexion RFS.

**REMARQUE :** la fonctionnalité vFlash et RFS iDRAC6 n'ont aucun lien entre elles.

Pour activer le partage de fichiers à distance via l'interface Web iDRAC6, procédez comme suit :

1. Ouvrez une fenêtre d'un navigateur Web pris en charge.
2. Ouvrez une session sur l'interface Web iDRAC6.
3. Sélectionnez **Système→ onglet Partage de fichiers distant.**

   L'écran **Partage de fichiers à distance** apparaît.

Le Tableau 4-23 répertorie les paramètres du partage de fichiers à distance.

**Tableau 4-23. Paramètres du serveur de fichiers à distance**

| Attribut | Description |
|---|---|
| **Nom d'utilisateur** | Nom d'utilisateur pour se connecter au système de fichiers NFS/CIFS. |
| **Mot de passe** | Mot de passe pour se connecter au système de fichiers NFS/CIFS. |

**Tableau 4-23. Paramètres du serveur de fichiers à distance *(suite)***

| Attribut | Description |
|---|---|
| **Chemin d'accès du fichier image** | Chemin d'accès du fichier à partager via le partage de fichiers à distance. |
| **État** | **Connecté** : le fichier est partagé.<br>**Non connecté** : le fichier n'est pas partagé.<br>**Connexion en cours** : la connexion vers le partage est en cours. |

Cliquez sur **Connecter** pour vous connecter à RFS. Une fois la connexion établie avec succès, **Connecter** est désactivé.

**REMARQUE :** même si vous avez configuré le partage de fichiers à distance, l'interface utilisateur n'affiche pas cette information pour des raisons de sécurité.

Pour le partage de fichiers distant, la commande RACADM distante est la suivante :

`racadm remoteimage`.

`racadm remoteimage <options>`

Les options sont les suivantes :

- `-c` ; connecter image
- `-d` ; déconnecter image
- `-u` <*nom d'utilisateur*> ; nom d'utilisateur permettant d'accéder au partage réseau
- `-p` <*mot de passe*> ; mot de passe permettant d'accéder au partage réseau
- `-l` <*emplacement_de_l'image*> ; emplacement de l'image sur le partage réseau ; mettez des guillemets autour de l'emplacement
- `-s` ; affiche la condition actuelle

**REMARQUE :** le nombre maximal de caractères pris en charge pour **Nom d'utilisateur** et **Mot de passe** est 40, et 511 pour **Chemin de fichier image**. Tous les caractères, y compris les caractères alphanumériques et les caractères spéciaux, sont autorisés pour ces trois champs, à l'exception des caractères suivants :

- ' (apostrophe)
- " (guillemet anglais)

- , (virgule)
- < (inférieur à)
- > (supérieur à)

# Module SD interne double

Le module Dual SD interne (IDSDM) fournit de la redondance sur la carte SD de l'hyperviseur en utilisant une autre carte SD qui crée une image miroir du contenu de la première carte SD. La deuxième carte SD peut être définie sur le module IDSDM tout comme l'autre carte SD en définissant l'option **Redondance** sur **mode Miroir** sur l'écran **Périphériques intégrés** de la configuration du BIOS système. Pour plus d'informations sur les options du BIOS du module IDSDM, voir le *Manuel du propriétaire du matériel* disponible sur le site Web du support de Dell à l'adresse **dell.com/support/manuals**.

**REMARQUE :** dans la configuration du BIOS, sur l'écran **Périphériques intégrés**, l'option **Port USB interne** doit être définie sur **Activé**. Si elle définie sur **Désactivé**, le module IDSDM n'est pas visible au système en tant que périphérique de démarrage.

L'une des deux cartes SD peut être la carte maîtresse. Par exemple, si deux cartes SD sont installées dans le module IDSDM alors que le courant alternatif n'alimente plus le système, la carte SD1 est considérée comme étant la carte active ou maîtresse. La carte SD2 est la carte de sauvegarde, et toutes les écritures du module IDSDM sur le système de fichiers seront transférées sur les deux cartes ; en revanche, les lectures ne seront effectuées qu'à partir de la carte SD1. À tout moment, en cas d'échec ou de retrait de la carte SD1, la carte SD2 devient automatiquement la carte active (maîtresse). La carte SD vFlash est désactivée en mode Miroir.

**Tableau 4-24. Condition IDSDM**

| IDSDM - Mode Miroir | Carte SD1 | Carte SD2 | Carte SD vFlash |
|---|---|---|---|
| Enabled (Activé) | Actif | Actif | Inactif |
| Disabled (Désactivé) | Actif | Inactif | Actif |

Grâce à iDRAC, vous pouvez afficher la condition, l'intégrité et la disponibilité du module IDSDM.

L'état de la redondance de la carte SD et les événements d'échec sont consignés dans le journal SEL, affichés à l'écran LCD, et des alertes PET sont générées si les alertes sont activées.

### Affichage de l'état du module Dual SD interne via l'interface utilisateur

1. Connectez-vous à l'interface utilisateur Web iDRAC.
2. Cliquez sur **Média flash amovible**. La page **Média vFlash amovible** s'affiche. Cette page affiche les deux sections suivantes :

- **Module Dual SD interne** : s'affiche uniquement si le module IDSDM est en mode redondant. L'**état de la redondance** s'affiche comme **Total**. Si cette section n'est pas présente, la carte se trouve alors à l'état de mode non redondant. Les indications de l'**état de la redondance** valide sont les suivantes :
  - **Total** : les cartes SD 1 et 2 fonctionnent correctement.
  - **Perdu** : l'une des cartes SD, ou les deux, ne fonctionne(nt) pas correctement.
- **État du module SD interne** : affiche l'état de la carte SD pour les cartes SD1, SD2 et vFlash en incluant les informations suivantes :
  - Condition :
    -  : indique que la carte est ok.
    -  : indique que la carte est hors ligne ou protégée contre l'écriture.
    -  : Indique qu'une alerte est émise.
  - Emplacement : emplacement des cartes SD.
  - Condition En ligne : les cartes SD1, SD2 et vFlash peuvent être dans l'un des états répertoriés à la section Tableau 4-25.

**Tableau 4-25. États de la carte SD**

| Carte Secure Digital | State (État) | Description |
|---|---|---|
| SD1 et SD2 | Boot (Démarrage) | Le contrôleur est en cours de démarrage. |
| | Actif | La carte est prête à accepter les requêtes de lecture/écriture SD. |
| | Mode Veille | La carte est la carte secondaire. Elle reçoit une copie de toutes les écritures SD. |
| | En panne | Une erreur est signalée au cours d'une lecture ou écriture de la carte SD. |
| | Absent | La carte SD n'est pas détectée. |
| | Hors ligne | Au démarrage, la signature d'identification de la carte (CID) de la carte diffère de la valeur de stockage non volatile (NV) ou la carte est la destination d'une opération de copie en cours. |
| | Protégé contre l'écriture | La carte est protégée contre l'écriture par le verrou physique présent sur la carte SD. Le module IDSDM ne peut pas utiliser de carte protégée contre l'écriture. |
| vFlash | Actif | La carte est prête à accepter les requêtes de lecture/écriture SD. |
| | Absent | La carte SD n'est pas détectée. |

# 5

# Configuration avancée d'iDRAC6

Contenant des informations sur la configuration avancée d'iDRAC6, cette section est recommandée aux utilisateurs ayant des connaissances avancées en gestion des systèmes et désirant personnaliser l'environnement d'iDRAC6 en fonction de leurs besoins spécifiques.

## Avant de commencer

Vous devez avoir terminé l'installation et la configuration de base du matériel et du logiciel de votre iDRAC6. Pour en savoir plus, voir « Installation de base d'iDRAC6 », à la page 35.

## Configuration d'iDRAC6 pour l'affichage de la sortie série à distance sur SSH/Telnet

Vous pouvez configurer iDRAC6 pour la console série distante en procédant de la manière suivante :

Configurez d'abord le BIOS pour activer la console série :

1. Allumez ou redémarrez le système.
2. Appuyez sur <F2> dès que vous avez vu le message suivant :

   ```
   <F2> = System Setup (Configuration du système)
   ```

3. Faites défiler la fenêtre et sélectionnez **Communications série** en appuyant sur <Entrée>.
4. Définissez les options de l'écran **Communications série** comme suit :

   ```
   communications série....Activé avec la redirection
   série via com2
   ```

   **REMARQUE :** vous pouvez définir les communications série sur **Activé avec la redirection série via com1** tant que le champ Adresse du port série, périphérique série2, est également défini sur com1.

   ```
   adresse du port série....Périphérique série1 =
   com1, périphérique série2 = com2
   ```

```
connecteur série externe....Périphérique série 1
débit en bauds de secours....115 200
type de terminal distant....vt100/vt220
redirection après démarrage....Activé
```

Sélectionnez ensuite **Enregistrer les modifications**.

5 Appuyez sur <Échap> pour quitter le programme **Configuration système** et terminer la configuration du programme Configuration système.

### Configuration des paramètres d'iDRAC6 pour activer SSH/Telnet

Configurez ensuite les paramètres iDRAC6 pour activer ssh/Telnet via la RACADM ou l'interface Web iDRAC6.

Pour configurer les paramètres iDRAC6 afin d'activer ssh/Telnet avec la RACADM, exécutez les commandes suivantes :

```
racadm config -g cfgSerial -o cfgSerialTelnetEnable 1
racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

Vous pouvez également exécuter les commandes RACADM à distance ; voir « Utilisation de la RACADM à distance », à la page 117.

Pour configurer les paramètres iDRAC6 afin d'activer ssh/Telnet à l'aide de l'interface Web iDRAC6, procédez comme suit :

1 Étendez l'arborescence du **Système**, puis cliquez sur **Paramètres iDRAC**.

2 Cliquez sur l'onglet **Réseau/Sécurité**, puis sur **Services**.

3 Sélectionnez **Activé** dans la section **SSH** ou **Telnet**.

4 Cliquez sur **Appliquer les modifications**.

Connectez-vous ensuite à iDRAC6 via Telnet ou SSH.

### Démarrage d'une console texte via Telnet ou SSH

Lorsque vous avez ouvert une session sur iDRAC6 via le logiciel du terminal de votre station de gestion avec Telnet ou SSH, vous pouvez rediriger la console texte du système géré en utilisant **console com2** qui est une commande Telnet/SSH. Un seul client **console com2** est pris en charge à la fois.

Pour vous connecter à la console texte du système géré, ouvrez une invite de commande iDRAC6 (affichée via une session Telnet ou SSH) et tapez :

```
console com2
```

La commande `console -h com2` affiche le contenu du tampon de l'historique série avant qu'une entrée ne soit faite à partir du clavier ou que de nouveaux caractères ne proviennent du port série.

La taille par défaut (et maximale) du tampon de l'historique est 8 192 caractères. Vous pouvez définir ce nombre sur une valeur plus petite avec la commande :

```
racadm config -g cfgSerial -o cfgSerialHistorySize
<nombre>
```

Pour configurer Linux pour la direction de la console pendant le démarrage, voir « Configuration de Linux pour la console série pendant le démarrage », à la page 97.

## Utilisation d'une console Telnet

### Exécution de Telnet à l'aide de Windows XP ou Windows 2003

Si votre station de gestion exécute Windows XP ou Windows 2003, un problème peut surgir au niveau des caractères lors d'une session Telnet iDRAC6. 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 à partir du 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.

### Exécution de Telnet à l'aide de Windows 2000

Si votre station de gestion exécute Windows 2000, vous ne pouvez pas accéder à la configuration du BIOS en appuyant sur la touche <F2>. Pour résoudre ce problème, utilisez le client Telnet fourni avec le téléchargement gratuit recommandé de Windows Services for UNIX 3.5 de Microsoft. Accédez à **microsoft.com/downloads/** et recherchez *Windows Services for UNIX* 3.5.

#### Activation de Microsoft Telnet pour la console virtuelle Telnet

**REMARQUE :** certains clients Telnet fonctionnant sous les systèmes d'exploitation Microsoft risquent de ne pas pouvoir afficher correctement l'écran de configuration du BIOS lorsque la console virtuelle du BIOS est définie pour l'émulation VT100/VT220. Si ce problème se produit, mettez à jour l'affichage en choisissant le mode ANSI pour la console virtuelle du BIOS. Pour effectuer cette procédure dans le menu de configuration du BIOS, sélectionnez **Console virtuelle** → **Type de terminal distant** → **ANSI**.

**REMARQUE :** lorsque vous configurez la fenêtre d'émulation VT100 du client, définissez la fenêtre ou l'application qui affiche la console virtuelle redirigée sur 25 lignes x 80 colonnes pour que le texte s'affiche correctement ; sinon, certains écrans de texte risquent d'être illisibles.

1. Activez **Telnet** dans **Services du composant Windows.**
2. Connectez-vous à iDRAC6 sur la station de gestion.

   Ouvrez une invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

   `telnet <adresse IP>:<numéro de port>`

   où *adresse IP* est l'adresse IP d'iDRAC6 et *numéro de port* est le numéro de port Telnet (si vous utilisez un nouveau port).

#### *Configuration de la touche Retour arrière pour votre session Telnet*

Selon le client Telnet, l'utilisation de la touche <Retour> peut avoir des résultats inattendus. Par exemple, la session peut renvoyer en écho `^h`. Toutefois, la plupart des clients Telnet Microsoft et Linux peuvent être configurés pour utiliser la touche <Retour>.

Pour configurer les clients Microsoft Telnet pour qu'ils utilisent la touche <Retour> :

1. Ouvrez une fenêtre d'invite de commande (si nécessaire).
2. Si vous n'exécutez pas déjà de session Telnet, tapez :

   `telnet`

   Si vous exécutez une session Telnet, appuyez sur <Ctrl><]>.
3. À l'invite, tapez :

   `set bsasdel`

   Le message suivant s'affiche :

   `Retour arrière sera envoyé en tant que Supprimer.`

Pour configurer une session Linux Telnet pour qu'elle utilise la touche <Retour> :

1. Ouvrez une invite de commande et tapez :

   ```
   stty erase ^h
   ```

2. À l'invite, tapez :

   ```
   telnet
   ```

### Utilisation de Secure Shell (SSH)

Il est essentiel que les périphériques de votre système et la gestion des périphériques soient sécurisés. Les périphériques connectés intégrés sont au cœur de nombreux processus d'affaires. Si ces périphériques sont compromis, votre entreprise peut être menacée, ce qui exige de nouvelles demandes de sécurité pour le logiciel de gestion de périphériques de l'interface de ligne de commande (CLI).

Secure Shell (SSH) est une session de ligne de commande qui inclut les mêmes capacités qu'une session Telnet, mais avec une sécurité accrue. iDRAC6 prend en charge la version 2 de SSH avec authentification par mot de passe. SSH est activé sur iDRAC6 lorsque vous installez ou mettez à jour votre micrologiciel iDRAC6.

Vous pouvez utiliser `PuTTY` ou `OpenSSH` sur la station de gestion pour vous connecter à l'iDRAC6 du système géré. Lorsqu'une erreur se produit pendant la procédure d'ouverture de session, le client secure shell émet un message d'erreur. Le texte du message dépend du client et n'est pas contrôlé par iDRAC6.

**REMARQUE :** `OpenSSH` doit être exécuté à partir d'un émulateur de terminal VT100 ou ANSI sous Windows. L'exécution d'`OpenSSH` à l'invite de commande Windows n'offre pas une fonctionnalité complète (quelques touches ne répondent pas et aucun graphique n'est affiché).

Seules deux sessions SSH simultanées sont prises en charge. Le délai d'expiration de la session est contrôlé par la propriété `cfgSsnMgtSshIdleTimeout` tel que décrit dans le *Guide de référence de la ligne de commande RACADM pour iDRAC6 et CMC* disponible sur le site Web du support de Dell à l'adresse **dell.com/support/manuals**.

Pour activer SSH sur iDRAC6, tapez :

```
racadm config -g cfgSerial -o cfgSerialSshEnable 1
```

Pour changer le port SSH, tapez :

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

Pour des informations supplémentaires sur les propriétés `cfgSerialSshEnable` et `cfgRacTuneSshPort`, voir le *Guide de référence de la ligne de commande RACADM pour iDRAC6 et CMC* disponible sur le site Web du support de Dell à l'adresse **dell.com/support/manuals**.

L'implémentation SSH iDRAC6 prend en charge plusieurs schémas de cryptographie, comme illustré dans le Tableau 5-1.

**Tableau 5-1. Schémas de cryptographie**

| Type de schéma | Schéma |
|---|---|
| Cryptographie asymétrique | Spécification de bits (aléatoire) Diffie-Hellman DSA/DSS 512-1024 conformément au NIST |
| Cryptographie symétrique | • AES256-CBC<br>• RIJNDAEL256-CBC<br>• AES192-CBC<br>• RIJNDAEL192-CBC<br>• AES128-CBC<br>• RIJNDAEL128-CBC<br>• BLOWFISH-128-CBC<br>• 3DES-192-CBC<br>• ARCFOUR-128 |
| Intégrité du message | • HMAC-SHA1-160<br>• HMAC-SHA1-96<br>• HMAC-MD5-128<br>• HMAC-MD5-96 |
| Authentification | • Mot de passe |

**REMARQUE :** SSHv1 n'est pas pris en charge.

### Configuration de Linux pour la console série pendant le démarrage

Les étapes suivantes sont spécifiques au chargeur GRUB (GRand Unified Bootloader) de Linux. Des modifications similaires devront être apportées si vous utilisez un chargeur de démarrage différent.

**REMARQUE :** lorsque vous configurez la fenêtre d'émulation VT100 du client, définissez la fenêtre ou l'application qui affiche la console virtuelle 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 Paramètres généraux dans le fichier et ajoutez les deux nouvelles lignes suivantes :

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

2. Ajoutez deux options à la ligne du noyau :

   ```
   kernel console=ttyS1,115200n8r console=tty1
   ```

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

Le Tableau 5-2 fournit un exemple de fichier **/etc/grub.conf** qui illustre les modifications décrites dans cette procédure.

**Tableau 5-2. Exemple de fichier : /etc/grub.conf**

```
# 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
```

**Tableau 5-2. Exemple de fichier : /etc/grub.conf *(suite)***

```
#          root (hd0,0)
#          kernel /boot/vmlinuz-version ro root=
/dev/sda1
#          initrd /boot/initrd-version.img
#
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.gz
serial --unit=1 --speed=57600
terminal --timeout=10 serial

title Red Hat Linux Advanced Server (2.4.9-e.3smp)
   root (hd0,0)
   kernel /boot/vmlinuz-2.4.9-e.3smp ro root=
/dev/sda1 hda=ide-scsi console=ttyS0 console=
ttyS1,115200n8r
   initrd /boot/initrd-2.4.9-e.3smp.img
title Red Hat Linux Advanced Server-up (2.4.9-e.3)
   root (hd0,00)
   kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 s
   initrd /boot/initrd-2.4.9-e.3.im
```

Lorsque vous modifiez le fichier **/etc/grub.conf**, observez les instructions suivantes :

1. Désactivez l'interface graphique du GRUB et utilisez l'interface texte ; sinon, l'écran du GRUB ne s'affiche pas sur la console virtuelle du RAC. Pour désactiver l'interface utilisateur, commentez la ligne commençant par `splashimage`.
2. Pour activer plusieurs options GRUB afin de démarrer les sessions de console virtuelle via la connexion série du RAC, ajoutez la ligne suivante à toutes les options :

   ```
   console=ttyS1,115200n8r console=tty1
   ```

   Le Tableau 5-2 illustre l'ajout de `console=ttyS1,57600` uniquement à la première option.

#### Activation de l'ouverture de session sur la console virtuelle après le démarrage

Modifiez le fichier **/etc/inittab** comme suit :

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

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

Le Tableau 5-3 illustre un exemple de fichier avec la nouvelle ligne.

**Tableau 5-3. Exemple de fichier : /etc/innitab**

```
#
# inittab  Ce fichier explique 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 - halt (interrompre) (Ne définissez PAS
initdefault sur ce niveau)
#   1 - Single user mode (Mode d'utilisateur unique)
#   2 - Multiuser, without NFS (Multi-utilisateurs,
sans NFS) (Identique à 3, si vous ne disposez pas
d'une
#       mise en réseau)
#   3 - Full multiuser mode (Mode multi-utilisateurs
intégral)
#   4 - unused (inutilisé)
#   5 - X11
#   6 : reboot (Do NOT set initdefault to this)
(redémarrer (Ne définissez PAS initdefault sur ce
niveau)
#
id:3:initdefault:

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

**Tableau 5-3. Exemple de fichier : /etc/innitab *(suite)***

```
l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6
# Éléments à exécuter à chaque niveau d'exécution.
ud::once:/sbin/update

# 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 »
```

**Tableau 5-3. Exemple de fichier : /etc/innitab *(suite)***

```
# 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** comme suit :

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

```
ttyS1
```

Le Tableau 5-4 illustre un exemple de fichier avec la nouvelle ligne.

**Tableau 5-4. Exemple de fichier : /etc/securetty**

```
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
```

**REMARQUE :** utilisez la séquence de touches d'arrêt (~B) pour exécuter les commandes de touches **Magic SysRq** Linux sur une console de série à l'aide de l'outil IPMI.

# Configuration d'iDRAC6 pour la connexion série

Vous pouvez utiliser l'une des interfaces suivantes pour vous connecter à iDRAC6 via la connexion série :

- CLI iDRAC6
- Connexion directe en mode de base
- Connexion directe en mode terminal

Pour configurer votre système en vue de l'utilisation de ces interfaces, procédez de la manière suivante :

1. Configurez le **BIOS** pour activer la connexion série :
   a. Allumez ou redémarrez le système.
   b. Appuyez sur <F2> dès que vous avez vu le message suivant :
      `<F2> = System Setup (Configuration du système)`
   c. Faites défiler la fenêtre et sélectionnez **Communications série** en appuyant sur <Entrée>.
   d. Définissez l'écran **Communications série** comme suit :
      `connecteur série externe....périphérique d'accès à distance`
   e. Sélectionnez **Enregistrer les modifications**.
   f. Appuyez sur <Échap> pour quitter le programme **Configuration système** et terminer la configuration du programme Configuration système.
2. Connectez votre câble DB-9 ou Null Modem de la station de gestion au serveur de nœud géré. Voir « Connexion du câble DB-9 ou null modem pour la console série », à la page 108.
3. Assurez-vous que votre logiciel d'émulation du terminal de gestion est configuré pour la connexion série. Voir « Configuration du logiciel d'émulation de terminal de la station de gestion », à la page 108.
4. Configurez les paramètres d'iDRAC6 pour activer les connexions série via la RACADM ou l'interface Web iDRAC6.

Pour configurer les paramètres d'iDRAC6 afin d'activer les connexions séries à l'aide de la RACADM, exécutez la commande suivante :

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 1
```

Pour configurer les paramètres d'iDRAC6 afin d'activer les connexions séries à l'aide de l'interface Web iDRAC6, procédez de la manière suivante :

1. Étendez l'arborescence du **Système**, puis cliquez sur **Paramètres iDRAC**.
2. Cliquez sur l'onglet **Réseau/Sécurité**, puis sur **Série**.
3. Sélectionnez **Activé** dans la section **Série RAC**.
4. Cliquez sur **Appliquer les modifications**.

Lorsque vous êtes connecté en série à l'aide des paramètres précédents, une invite d'ouverture de session s'affiche. Saisissez le nom d'utilisateur et le mot de passe iDRAC6 (les valeurs par défaut sont respectivement `root` et `calvin`).

Dans cette interface, vous pouvez exécuter des fonctionnalités telles que la RACADM. Par exemple, pour imprimer le journal des événements système, saisissez la commande RACADM suivante :

```
racadm getsel
```

### Configuration d'iDRAC pour la connexion directe en mode de base et en mode terminal

À l'aide de la RACADM, exécutez la commande suivante pour désactiver l'interface de ligne de commande d'iDRAC6 :

```
racadm config -g cfgSerial -o cfgSerialConsoleEnable 0
```

Exécutez ensuite la commande RACADM suivante pour activer la connexion directe en mode de base :

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialConnectionMode 1
```

Vous pouvez également exécuter la commande RACADM suivante pour activer la connexion directe en mode terminal :

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialConnectionMode 0
```

Vous pouvez effectuer les mêmes actions en utilisant l'interface Web iDRAC6 :

1. Étendez l'arborescence du **Système**, puis cliquez sur **Paramètres iDRAC**.
2. Cliquez sur l'onglet **Réseau/Sécurité**, puis sur **Série**.
3. Désélectionnez **Activé** dans la section **Série RAC**.

Pour la connexion directe en mode de base :

Dans la section **Série IPMI**, faites passer le menu déroulant **Paramètres du mode de connexion** à **Connexion directe en mode de base**.

Pour la connexion directe en mode terminal :

Dans la section **Série IPMI**, faites passer le menu déroulant **Paramètres du mode de connexion** à **Connexion directe en mode terminal**.

4 Cliquez sur **Appliquer les modifications**. Pour plus d'informations sur la connexion directe en mode de base et en mode terminal, voir « Configuration des modes série et terminal », à la page 112.

La connexion directe en mode de base vous permet d'utiliser des outils tels qu'ipmish directement via la connexion série. Par exemple, pour imprimer le journal des événements système à l'aide d'ipmish via le mode de base IPMI, exécutez la commande suivante :

```
ipmish -com 1 -baud 57600 -flow cts -u root -p calvin
sel get
```

La connexion directe en mode terminal vous permet d'émettre des commandes ASCII sur iDRAC6. Par exemple, pour activer/désactiver le serveur via la connexion directe en mode terminal :

1 Connectez-vous à iDRAC6 via le logiciel d'émulation de terminal.

2 Tapez la commande suivante pour ouvrir une session :

```
[SYS PWD -U root calvin]
```

Les éléments suivants s'affichent alors :

```
[SYS]
```

```
[OK]
```

3 Tapez la commande suivante pour vous assurer que l'ouverture de session a réussi :

```
[SYS TMODE]
```

Les éléments suivants s'affichent alors :

```
[OK TMODE]
```

4 Pour désactiver le serveur (le serveur se désactive immédiatement), tapez la commande suivante :

```
[SYS POWER OFF]
```

5 Pour activer le serveur (l'activation est immédiate) :

```
[SYS POWER ON]
```

### Commutation entre le mode Communication d'interface série du RAC et Console série

iDRAC6 prend en charge les séquences de la touche Échap permettant de commuter entre la communication d'interface série du RAC et la console série.

Pour définir votre système de manière à ce qu'il autorise ce comportement, procédez comme suit :

1 Allumez ou redémarrez le système.

2 Appuyez sur <F2> dès que vous avez vu le message suivant :

```
<F2> = System Setup (Configuration du système)
```

3 Faites défiler la fenêtre et sélectionnez **Communications série** en appuyant sur <Entrée>.

4 Définissez l'écran **Communications série** comme suit :

communications série....Activé avec la redirection série via com2

**REMARQUE :** vous pouvez définir le champ **Communications série** sur **Activé avec la redirection série via com1** si le **périphérique série2** du **champ Adresse du port série** est également défini sur com1.

adresse du port série -- Périphérique série1 = com1, périphérique série2 = com2

connecteur série externe -- Périphérique série 2

débit en bauds de secours....115 200

type de terminal distant....vt100/vt220

redirection après démarrage....Activé

Sélectionnez ensuite **Enregistrer les modifications**.

5 Appuyez sur <Échap> pour quitter le programme **Configuration système** et terminer la configuration du programme Configuration système.

Connectez le câble null modem entre le connecteur série externe du système géré et le port série de la station de gestion.

Utilisez un programme d'émulation de terminal (HyperTerminal ou TeraTerm) sur la station de gestion et, en fonction de l'avancement du processus de démarrage du serveur géré, les écrans du POST ou les écrans du système d'exploitation apparaissent. Ceci repose sur la configuration : SAC pour Windows et les écrans en mode texte Linux pour Linux. Définissez les paramètres de terminal de la station de gestion : Débit en bauds :115 200 ; données : 8 bits ; parité : aucune ; arrêt : 1 bit et contrôle du débit : aucun.

Pour passer au mode Communication d'interface série du RAC lorsque vous vous trouvez en mode Console série, utilisez la séquence de touches suivante :

```
<Échap> + <Maj> <9>
```

La séquence de touches ci-dessus vous dirige vers l'invite « Ouverture de session sur iDRAC » (si le RAC est défini sur le mode « RAC série ») ou le mode «  Connexion série » où les commandes de terminal peuvent être émises (si le RAC est défini sur « Connexion directe IPMI série en mode terminal »).

Pour passer au mode Console série lorsque vous êtes en mode Communication d'interface série du RAC, utilisez la séquence de touches suivante :

```
<Échap> + <Maj> <q>
```

En mode terminal, pour permuter la connexion vers le port système COM2, utilisez :

```
<Échap> + <Maj> <q>
```

Lorsque vous êtes connecté au port système COM2 et que vous voulez revenir au mode terminal, utilisez :

```
<Échap> + <Maj> <9>
```

# Connexion du câble DB-9 ou null modem pour la console série

Pour accéder au système géré en utilisant une console texte série, connectez un DB-9 ou null modem au port COM du système géré. Pour que la connexion fonctionne avec le câble null modem, les paramètres de communications série correspondants doivent être définis dans la configuration CMOS. Certains des câbles DB-9 n'ont pas le brochage/les signaux requis pour cette connexion. Le câble DB-9 utilisé pour cette connexion doit avoir les spécifications décrites dans le Tableau 5-5.

**REMARQUE :** le câble DB-9 peut également être utilisé pour la console virtuelle texte du BIOS.

**Tableau 5-5. Brochage requis pour le câble DB-9 ou null modem**

| Nom du signal | Broche DB-9 (broche du serveur) | Broche DB-9 (broche de la station de travail) |
|---|---|---|
| FG (masse de l'armature) | – | – |
| TD (transmission de données) | 3 | 2 |
| RD (réception de données) | 2 | 3 |
| RTS (demande d'envoi) | 7 | 8 |
| CTS (prêt à envoyer) | 8 | 7 |
| SG (terre du signal) | 5 | 5 |
| DSR (ensemble de données prêt) | 6 | 4 |
| CD (détection de porteuse) | 1 | 4 |
| DTR (terminal de données prêt) | 4 | 1 et 6 |

# Configuration du logiciel d'émulation de terminal de la station de gestion

iDRAC6 prend en charge une console texte série ou Telnet d'une station de gestion exécutant l'un des types de logiciel d'émulation de terminal suivants :

- Linux Minicom dans un Xterm
- HyperTerminal Private Edition (version 6.3) de Hilgraeve
- Linux Telnet dans un Xterm
- Microsoft Telnet

Effectuez les étapes des sous-sections suivantes pour configurer votre type de logiciel de terminal. Si vous utilisez Microsoft Telnet, la configuration n'est pas nécessaire.

## Configuration de Linux Minicom pour l'émulation de console série

Minicom est l'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 l'émulation de console série », à la page 110 pour configurer les autres versions de Minicom.

### Configuration de Minicom version 2.0 pour l'émulation de console série

**REMARQUE :** pour que le texte s'affiche correctement, il est recommandé d'utiliser une fenêtre Xterm plutôt que la console par défaut fournie lors de l'installation de Linux pour afficher la console Telnet.

1. Pour lancer une nouvelle session Xterm, tapez `xterm &` à l'invite de commande.
2. Dans la fenêtre Xterm, déplacez le curseur de la souris dans le coin inférieur droit de la fenêtre et redimensionnez la fenêtre sur 80 x 25.
3. 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 17.
4. À l'invite de commande Xterm, tapez `minicom -s`.
5. Sélectionnez **Configuration du port série** et appuyez sur <Entrée>.
6. Appuyez sur <a> et sélectionnez le périphérique série approprié (**/dev/ttySo**, par exemple).
7. Appuyez sur <e> et définissez l'option **B/s/Par/Bits** sur **57600 8N1**.
8. Appuyez sur <f>, définissez **Contrôle du débit matériel** sur **Oui** et définissez **Contrôle du débit logiciel** sur **Non**.
9. Pour quitter le menu **Configuration du port série**, appuyez sur <Entrée>.
10. Sélectionnez **Modem et numérotation** et appuyez sur <Entrée>.

11 Dans le menu **Configuration de la numérotation du modem et des paramètres**, appuyez sur <Retour> pour effacer les paramètres **init**, **reset**, **connect** et **hangup** et les laisser vides.

12 Pour enregistrer chaque valeur vide, appuyez sur <Entrée>.

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

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

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

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

17 Pour agrandir la fenêtre de Minicom à 80 x 25, faites glisser le coin de la fenêtre.

18 Appuyez sur <Ctrl+a>, <z>, <x> pour quitter Minicom.

**REMARQUE :** si vous utilisez Minicom pour la console virtuelle texte série afin de configurer le BIOS du système géré, il est recommandé d'activer la couleur dans Minicom. Pour activer la couleur, tapez la commande suivante : `minicom -c on`

Assurez-vous que la fenêtre Minicom affiche une invite de commande. Lorsque l'invite de commande apparaît, votre connexion est réussie et vous pouvez vous connecter à la console du système géré avec la commande série **connect**.

#### Paramètres de Minicom requis pour l'émulation de console série

Utilisez le Tableau 5-6 pour configurer une version quelconque de Minicom.

**Tableau 5-6. Paramètres de Minicom pour l'émulation de console série**

| Description du paramètre | Paramètre requis |
|---|---|
| B/s/Par/Bits | 57600 8N1 |
| Contrôle du débit matériel | Oui |
| Contrôle du débit logiciel | Non |
| Émulation de terminal | ANSI |

**Tableau 5-6. Paramètres de Minicom pour l'émulation de console série *(suite)***

| Description du paramètre | Paramètre requis |
|---|---|
| Paramètres de la numérotation du modem et des paramètres | Effacez les paramètres **init**, **reset**, **connect** et **hangup** pour qu'ils soient vides |
| Taille de fenêtre | 80 x 25 (pour redimensionner, faites glisser le coin de la fenêtre) |

## Configuration d'HyperTerminal pour la console série

HyperTerminal est l'utilitaire d'accès au port série de Microsoft Windows. Pour définir correctement la taille de l'écran de votre console virtuelle, utilisez HyperTerminal Private Edition version 6.3 de Hilgraeve.

**PRÉCAUTION : toutes les versions de système d'exploitation Microsoft Windows comprennent le logiciel d'émulation de terminal HyperTerminal de Hilgraeve. Cependant, la version comprise ne fournit pas beaucoup de fonctions requises lors de l'utilisation de la console virtuelle. Ainsi, utilisez l'édition 6.3 à la place ou tout logiciel d'émulation terminal qui prend en charge VT100/VT220 ou mode d'émulation ANSI. Un exemple d'émulateur de terminal complet VT100/VT220 ou ANSI qui prend en charge la console virtuelle sur votre système est HyperTerminal Private de Hilgraeve.**

Pour configurer HyperTerminal pour la console série :

1. Lancez le programme HyperTerminal.
2. Tapez le nom de la nouvelle connexion et cliquez sur **OK**.
3. À côté de **Connecter en utilisant :**, sélectionnez le port COM de la station de gestion (COM2, par exemple) auquel vous avez connecté le câble DB-9 ou null modem et cliquez sur **OK**.
4. Configurez les paramètres du port COM comme indiqué dans Tableau 5-7.
5. Cliquez sur **OK**.
6. Cliquez sur **Fichier→ Propriétés**, puis sur l'onglet **Paramètres**.
7. Définissez la **Référence du terminal Telnet** sur **ANSI**.
8. Cliquez sur **Configuration du terminal** et choisissez **26** pour **Lignes de l'écran**.
9. Définissez **Colonnes** sur 80 et cliquez sur **OK**.

**Tableau 5-7. Paramètres du port COM de la station de gestion**

| Description du paramètre | Paramètre requis |
|---|---|
| Bits par seconde | 57 600 |
| Bits de données | 8 |
| Parity (Parité) | None (Aucune) |
| Bits d'arrêt | 1 |
| Contrôle du débit | Matériel |

# Configuration des modes série et terminal

## Configuration du mode série IPMI et iDRAC6

1. Étendez l'arborescence du **Système**, puis cliquez sur **Paramètres iDRAC**.
2. Cliquez sur l'onglet **Réseau/Sécurité**, puis sur **Série**.
3. Configurez les paramètres série IPMI.

   Voir le Tableau 5-8 pour une description des paramètres série IPMI.
4. Configurez les paramètres série d'iDRAC6.

   Voir le Tableau 5-9 pour une description des paramètres série d'iDRAC6.
5. Cliquez sur **Appliquer les changements** pour appliquer les modifications de série IPMI et iDRAC6.
6. Cliquez sur le bouton approprié de la page **Série** pour continuer. Voir l'*Aide en ligne iDRAC6* pour une description des paramètres de la page **Configuration de série**.

**Tableau 5-8. Paramètres série IPMI**

| Paramètre | Description |
|---|---|
| **Paramètres du mode de connexion** | • Connexion directe en mode de base : mode de base série IPMI<br>• Connexion directe en mode terminal : mode terminal série IPMI |
| **Baud Rate (Débit en bauds)** | • Définit la vitesse de transmission de données. Sélectionnez **9 600 b/s**, **19,2 kb/s**, **57,6 kb/s** ou **115,2 kb/s**. |

**Tableau 5-8. Paramètres série IPMI *(suite)***

| Paramètre | Description |
|---|---|
| Contrôle du débit | • Aucun : contrôle du débit matériel désactivé<br>• RTS/CTS : contrôle du débit matériel activé |
| Limite du niveau de privilège du canal | • Administrateur<br>• Opérateur<br>• User (Utilisateur) |

**Tableau 5-9. Paramètres série iDRAC6**

| Paramètre | Description |
|---|---|
| Enabled (Activé) | Active ou désactive la console série iDRAC6. Coché = Activé ; décoché = Désactivé |
| Délai d'attente | La durée maximale d'inactivité de la ligne, en secondes, qui doit s'écouler avant que la ligne ne soit déconnectée La plage est comprise entre 60 et 1 920 secondes. La valeur par défaut est 300 secondes. Utilisez 0 seconde pour désactiver la fonctionnalité Délai d'expiration. |
| Redirection activée | Active ou désactive la console virtuelle. Coché = Activé ; décoché = Désactivé |
| Baud Rate (Débit en bauds) | Vitesse de transmission de données sur le port série externe. Les valeurs sont les suivantes : 9 600 b/s, 19,2 kb/s, 57,6 kb/s et 115,2 kb/s. La valeur par défaut est 57,6 kb/s. |
| Touche Échap | Spécifie la touche <Échap>. Les caractères ^\ sont définis par défaut. |
| Taille du tampon de l'historique | Taille du tampon de l'historique série qui contient les derniers caractères écrits sur la console virtuelle. La valeur maximale et par défaut est de 8 192 caractères. |
| Commande d'ouverture de session | Ligne de commande iDRAC6 à exécuter lors d'une ouverture de session valide. |

## Configuration du mode terminal

1. Étendez l'arborescence du **Système**, puis cliquez sur **Paramètres iDRAC**.
2. Cliquez sur l'onglet **Réseau/Sécurité**, puis sur **Série**.

3 Sur la page **Série**, cliquez sur **Paramètres du mode terminal**.

4 Configurez les paramètres du mode terminal.

Voir le Tableau 5-10 pour une description des paramètres du mode terminal.

5 Cliquez sur **Appliquer les modifications**.

6 Cliquez sur le bouton approprié de la page **Paramètres du mode terminal** pour continuer. Voir l' *Aide en ligne iDRAC6* pour une description des boutons de la page **Paramètres du mode Terminal**.

**Tableau 5-10. Paramètres du mode terminal**

| Paramètre | Description |
|---|---|
| Modification de ligne | Active ou désactive la modification de ligne. |
| Contrôle de la suppression | Sélectionnez l'une des options suivantes :<br>• iDRAC émet un caractère <retarr.><sp><retarr.> lorsque <retarr.> ou <suppr.> est reçu.<br>• iDRAC émet un caractère <suppr.> lorsque <retarr.> ou <suppr.> est reçu. |
| Contrôle d'écho | Active ou désactive l'écho. |
| Contrôle de l'établissement de liaisons | Active ou désactive l'établissement de liaisons. |
| Nouvelle séquence linéaire | Sélectionnez Aucun, <CR-LF>, <NULL>, <CR>, <LF-CR> ou <LF>. |
| Saisie d'une nouvelle séquence linéaire | Sélectionnez <CR> ou <NULL>. |

# Configuration des paramètres réseau d'iDRAC6

**PRÉCAUTION : si vous modifiez les paramètres réseau de votre iDRAC6, la connexion réseau en cours risque d'être coupée.**

Configurez les paramètres réseau d'iDRAC6 avec l'un des outils suivants :

- Interface Web : voir « Configuration de la carte réseau iDRAC6 », à la page 51.

- CLI RACADM : voir cfgLanNetworking dans le *Guide de référence de la ligne de commande RACADM pour iDRAC6 et CMC* disponible sur le site Web du support de Dell à l'adresse **dell.com/support/manuals**.
- Utilitaire de configuration d'iDRAC6 : voir « Configuration de votre système pour utiliser un iDRAC6 », à la page 36.

**REMARQUE :** pour déployer iDRAC6 dans un environnement Linux, voir « Installation de la RACADM », à la page 40.

# Accès à iDRAC6 via un réseau

Une fois iDRAC6 configuré, vous pouvez accéder à distance au système géré en utilisant l'une des interfaces suivantes :

- Interface Web
- RACADM.
- Console Telnet
- SSH
- IPMI

Le Tableau 5-11 décrit chaque interface iDRAC6.

**Tableau 5-11. Interfaces iDRAC6**

| Interface | Description |
|---|---|
| Interface Web | Fournit un accès à distance à iDRAC6 à l'aide d'une interface utilisateur graphique. L'interface Web est intégrée au micrologiciel iDRAC6 et est accessible via l'interface de NIC d'un navigateur Web pris en charge sur la station de gestion. |

**Tableau 5-11. Interfaces iDRAC6 *(suite)***

| Interface | Description |
|---|---|
| RACADM. | Fournit un accès à distance à iDRAC6 à l'aide d'une interface de ligne de commande. La RACADM utilise l'adresse IP d'iDRAC6 pour exécuter les commandes RACADM.<br>**REMARQUE :** la capacité à distance de la racadm est prise en charge uniquement sur les stations de gestion. Pour plus d'informations, voir « Utilisation de la RACADM à distance », à la page 117.<br>**REMARQUE :** lors de l'utilisation de la capacité à distance de la 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, par exemple :<br>`racadm getconfig -f <nom de fichier>`<br>ou :<br>`sous-commandes racadm sslcertupload -t 1 -f c:\cert\cert.txt` |
| Console Telnet | Donne accès à iDRAC6 et permet la prise en charge des commandes série et la RACADM, y compris les commandes **powerdown**, **powerup**, **powercycle** et **hardreset**.<br>**REMARQUE :** telnet n'est pas un protocole sécurisé. Il transmet toutes les données, y compris les mots de passe, non cryptées. Pour transmettre des informations critiques, utilisez l'interface SSH. |
| Interface SSH | Fournit les mêmes capacités que la console Telnet en utilisant une couche de transport cryptée pour une sécurité accrue. |
| Interface IPMI | Fournit l'accès via iDRAC6 aux fonctionnalités de gestion de base du système distant. L'interface inclut IPMI sur LAN, IPMI sur communications série et Communications série sur LAN. Pour plus d'informations, voir le Guide d'utilisation de *Dell OpenManage Baseboard Management Controller Utilities* à l'adresse **support.dell.com\manuals**. |

**REMARQUE :** le nom d'utilisateur par défaut d'iDRAC6 est `root` et le mot de passe par défaut est `calvin`.

Vous pouvez accéder à l'interface Web d'iDRAC6 via le NIC d'iDRAC6 en utilisant un navigateur Web pris en charge, Server Administrator ou IT Assistant.

Pour accéder à l'interface d'accès à distance d'iDRAC6 avec Server Administrator, procédez comme suit :

- Lancez Server Administrator.
- 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 Server Administrator*.

# Utilisation de la RACADM à distance

**REMARQUE :** configurez l'adresse IP sur votre iDRAC6 avant d'utiliser la capacité d'accès à distance de la RACADM. Pour plus d'informations sur la configuration de votre iDRAC6 et une liste des documents connexes, voir « Installation de base d'iDRAC6 », à la page 35.

La RACADM fournit 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 virtuelle ou d'une station de gestion distante. 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 d'iDRAC6.

**REMARQUE :** si le système depuis lequel vous accédez au système distant ne comporte pas de certificat iDRAC6 dans sa réserve de certificats par défaut, un message apparaît lorsque vous tapez une commande RACADM. Pour plus d'informations sur les certificats iDRAC6, voir « Sécurisation des communications iDRAC6 à l'aide de certificats SSL et numériques », à la page 66.

```
Alerte de sécurité : le certificat est invalide :
le nom sur le certificat est invalide ou ne
correspond pas au nom du site

Continuer l'exécution. Utilisez l'option -S pour
que la racadm interrompe l'exécution sur les
erreurs liées au certificat.
```

La RACADM continue d'exécuter la commande. Toutefois, si vous utilisez l'option `–S`, la RACADM arrête d'exécuter la commande et affiche le message suivant :

```
Alerte de sécurité : le certificat est invalide :
le nom sur le certificat est invalide ou ne
correspond pas au nom du site

racadm interrompt l'exécution de la commande.

ERREUR : impossible de se connecter à iDRAC6 à
l'adresse IP spécifiée
```

Sur les systèmes Linux, assurez-vous de suivre les étapes intermédiaires suivantes afin que la validation des certificats réussisse à l'aide de la RACADM distante :

1. Convertissez le certificat du format DER au format PEM (à l'aide de l'outil openssl cmdline) :

   ```
   openssl x509 -inform pem -in
   <yourdownloadedderformatcert.crt> –outform pem -
   out <outcertfileinpemformat.pem> –text
   ```

2. Trouvez l'emplacement du groupe de certificats de l'autorité de certification par défaut sur la station de gestion. Par exemple, pour RHEL5 64 bits, il s'agit de /etc/pki/tls/cert.pem.
3. Ajoutez le certificat de l'autorité de certification PEM formaté au certificat de l'autorité de certification de la station de gestion.

   Par exemple, utilisez la commande cat :

   ```
   - cat testcacert.pem >> cert.pem
   ```

### Synopsis de la RACADM

```
racadm -r <adresse IP iDRAC6> -u <nom d'utilisateur> -
p <mot de passe> <sous-commande> <options de la sous-
commande>

racadm -i -r <adresse IP iDRAC6> <sous-commande>
<options de la sous-commande>
```

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 d'iDRAC6 a été remplacé par un port personnalisé autre que le port par défaut (443), la syntaxe suivante doit être utilisée :

```
racadm -r <adresse IP d'iDRAC6>:<port> -u <nom
d'utilisateur> -p <mot de passe> <sous-commande>
<options de la sous-commande>
```

```
racadm -i -r <adresse IP d'iDRAC6>:<port> <sous-
commande> <options de la sous-commande>
```

## Options de la RACADM

Le Tableau 5-12 énumère les options de la commande RACADM.

**Tableau 5-12. Options de la commande racadm**

| Option | Description |
|---|---|
| **-r** <*racIpAddr*> | Spécifie l'adresse IP distante du contrôleur. |
| **-r** <*racIpAddr*>: <*numéro de port*> | Utilisez <*numéro de port*> si le numéro de port iDRAC6 n'est pas le port par défaut (443) |
| **-i** | Ordonne à la RACADM de demander de manière interactive à l'utilisateur son nom d'utilisateur et son mot de passe. |
| **-u** <*usrName*> | Spécifie le nom d'utilisateur qui est utilisé pour authentifier la transaction de commande. Si l'option **-u** est utilisée, l'option **-p** doit être utilisée 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. |
| **-S** | Indique que la RACADM doit contrôler les erreurs de certificat non valide. La RACADM interrompt l'exécution de la commande avec un message d'erreur si elle détecte un certificat non valide. |

# Activation et désactivation de la fonctionnalité distante de RACADM

**REMARQUE :** il est recommandé d'exécuter ces commandes sur votre système local.

Par défaut, la capacité d'accès à distance de la RACADM est activée. Si elle est désactivée, tapez la commande RACADM suivante pour l'activer :

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

Pour désactiver la capacité d'accès à distance, tapez :

```
racadm config -g cfgRacTuning -o
cfgRacTuneRemoteRacadmEnable 0
```

## Sous-commandes RACADM

Le Tableau 5-13 fournit une description de chaque sous-commande RACADM que vous pouvez exécuter dans la RACADM. Pour accéder à la liste détaillée des sous-commandes RACADM, y compris la syntaxe et les entrées valides, voir le *Guide de référence de la ligne de commande RACADM pour iDRAC6 et CMC* disponible sur le site Web du support de Dell à l'adresse **dell.com/support/manuals**.

Lorsque vous saisissez une sous-commande RACADM, utilisez comme préfixe de commande `racadm`, par exemple :

```
racadm help
```

**Tableau 5-13. Sous-commandes RACADM**

| Commande | Description |
|---|---|
| **help** | Répertorie les sous-commandes iDRAC6. |
| **help** <*sous-commande*> | Répertorie les instructions d'utilisation pour 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. |
| **clearasrscreen** | Efface l'écran du dernier plantage (dernier écran bleu). |
| **clrraclog** | Efface le journal iDRAC6. Une entrée unique est effectuée pour indiquer l'utilisateur et l'heure à laquelle le journal a été effacé. |

**Tableau 5-13. Sous-commandes RACADM *(suite)***

| Commande | Description |
|---|---|
| **config** | Configure iDRAC6. |
| **getconfig** | Affiche les propriétés de configuration iDRAC6 actuelles. |
| **coredump** | Affiche le dernier vidage de mémoire d'iDRAC6. |
| **coredumpdelete** | Supprime le vidage de mémoire stocké sur iDRAC6. |
| **fwupdate** | Exécute ou affiche la condition des mises à jour du micrologiciel iDRAC6. |
| **getssninfo** | Affiche des informations sur les sessions actives. |
| **getsysinfo** | Affiche des informations générales concernant l'iDRAC6 et le système. |
| **getractime** | Affiche l'heure iDRAC6. |
| **ifconfig** | Affiche la configuration IP iDRAC6 actuelle. |
| **netstat** | Affiche la table de routage et les connexions actuelles. |
| **ping** | Vérifie que l'adresse IP de destination est accessible à partir d'iDRAC6 avec le contenu actuel de la table de routage. |
| **setniccfg** | Définit la configuration IP du contrôleur. |
| **sshpkauth** | Vous permet de téléverser jusqu'à 4 clés publiques SSH différentes, de supprimer des clés existantes et d'afficher les clés déjà présentes dans iDRAC6. |
| **getniccfg** | Affiche la configuration IP actuelle du contrôleur. |
| **getsvctag** | Affiche les numéros de service du système. |
| **racdump** | Vide les informations de condition et d'état d'iDRAC6 pour le débogage de la mémoire. |
| **racreset** | Réinitialise iDRAC6. |
| **racresetcfg** | Réinitialise la configuration par défaut d'iDRAC6. |
| **serveraction** | Effectue des opérations de gestion de l'alimentation sur le système géré. |
| **getraclog** | Affiche le journal d'iDRAC6. |
| **clrsel** | Efface les entrées du journal des événements système. |
| **gettracelog** | Affiche le journal de suivi d'iDRAC6. Si elle est utilisée avec `-i`, la commande affiche le nombre d'entrées du journal de suivi d'iDRAC6. |

**Tableau 5-13. Sous-commandes RACADM *(suite)***

| Commande | Description |
|---|---|
| **sslcsrgen** | Génère et télécharge la RSC SSL. |
| **sslcertupload** | Téléverse un certificat d'autorité de certification ou un certificat de serveur vers iDRAC6. |
| **sslcertdownload** | Télécharge un certificat d'autorité de certification. |
| **sslcertview** | Affiche un certificat d'autorité de certification ou un certificat de serveur dans iDRAC6. |
| **sslkeyupload** | Téléverse la clé SSL du client vers iDRAC6. |
| **testtrap** | Contraint iDRAC6 à envoyer une interruption SNMP test sur le NIC d'iDRAC6 pour vérifier la configuration de l'interruption. |
| **vmdisconnect** | Force la déconnexion du média virtuel. |
| **closessn** | Ferme une session de communication sur le périphérique. |
| **getsel** | Affiche les entrées du journal SEL. |
| **krbkeytabupload** | Téléverse le fichier keytab Kerberos. |
| **localConRedirDisable** | Désactive la console du serveur. Il n'existe aucune sortie vidéo du port vidéo du serveur. |
| **testemail** | Teste la fonctionnalité d'alertes par e-mail du RAC. |
| **usercertupload** | Téléverse un certificat d'utilisateur ou un certificat d'autorité de certification d'utilisateur du client vers iDRAC6. |
| **usercertview** | Affiche le certificat d'utilisateur ou le certificat d'autorité de certification d'utilisateur qui existe sur iDRAC6. |
| **vflashsd** | Initialise ou obtient la condition de la carte SD vflash. |
| **vflashpartition** | Crée, supprime, répertorie ou affiche la condition des partitions d'une carte SD vFlash initialisée. |

### Questions les plus fréquentes sur les messages d'erreur de la RACADM

**Une fois iDRAC6 réinitialisé (avec la commande racadm racreset), j'envoie une commande et le message suivant s'affiche :**

```
ERREUR : impossible de se connecter au RAC à
l'adresse  IP spécifiée.
```

**Qu'est-ce que ce message signifie ?**

Vous devez attendre qu'iDRAC6 soit entièrement réinitialisé avant d'émettre une autre commande.

**Lorsque j'utilise les commandes et les sous-commandes racadm, il y a des erreurs que je  ne comprends pas.**

Une ou plusieurs des erreurs suivantes peuvent survenir lorsque vous utilisez les commandes et les sous-commandes RACADM :

- Messages d'erreur de la RACADM locale : problèmes de syntaxe, d'erreurs typographiques et de noms incorrects.
- Messages d'erreur de la RACADM distante : problèmes d'adresse IP incorrecte, de nom d'utilisateur incorrect ou de mot de passe incorrect.

**Lorsque j'utilise ping pour l'adresse IP d'iDRAC6 de mon système, puis commute mon iDRAC6 entre les modes Dédié et Partagé pendant la réponse ping, je ne reçois aucune réponse.**

Effacez la table ARP sur votre système.

**La RACADM distante ne parvient pas à se connecter à iDRAC à partir de SUSE Linux Enterprise Server (SLES) 11 SP1**

Vérifiez que vous avez installé les versions openssl et libopenssl officielles. Exécutez la commande suivante pour installer les paquetages RPM :

```
rpm -ivh --force <nom de fichier>
```

où `<nom de fichier>` correspond au fichier du paquetage rpm openssl ou libopenssl.

Par exemple :

```
rpm -ivh --force openssl-0.9.8h-30.22.21.1.x86_64.rpm
rpm -ivh --force libopenssl0_9_8-0.9.8h-
30.22.21.1.x86_64.rpm
```

# Configuration de plusieurs contrôleurs iDRAC6

À l'aide de la RACADM, vous pouvez configurer un ou plusieurs contrôleurs iDRAC6 avec des propriétés identiques. Lorsque vous émettez une requête sur un contrôleur iDRAC6 spécifique à l'aide de sa référence de groupe et d'objet, la RACADM crée le fichier de configuration **.cfg** à partir des informations récupérées. Le nom de fichier est spécifié par l'utilisateur, par exemple **racadm.cfg**. En exportant le fichier vers un ou plusieurs iDRAC6, vous pouvez configurer vos contrôleurs avec des propriétés identiques en un minimum de temps.

**REMARQUE :** certains fichiers de configuration contiennent des informations iDRAC6 uniques (comme l'adresse IP statique) qui doivent être modifiées avant d'exporter le fichier vers d'autres iDRAC6.

Pour configurer plusieurs contrôleurs iDRAC6, procédez de la manière suivante :

1. Utilisez la RACADM pour effectuer une requête sur l'iDRAC6 cible qui contient la configuration appropriée.

   **REMARQUE :** le fichier **.cfg** généré ne contient pas de mots de passe utilisateur.

   Ouvrez une invite de commande et tapez :

   ```
   racadm getconfig -f myfile.cfg
   ```

   **REMARQUE :** la redirection d'une configuration iDRAC6 vers un fichier à l'aide de **getconfig-f** est seulement prise en charge avec les interfaces de la RACADM locale et distante.

2. Modifiez le fichier de configuration à l'aide d'un simple éditeur de texte **(facultatif)**.

3. Utilisez le nouveau fichier de configuration pour modifier un iDRAC6 cible.

   À l'invite de commande, tapez :

   ```
   racadm config –f myfile.cfg
   ```

4. Réinitialisez l'iDRAC6 cible qui a été configuré.

   À l'invite de commande, tapez :

   ```
   racadm racreset
   ```

La sous-commande `getconfig -f racadm.cfg` demande la configuration d'iDRAC6 et génère le fichier **racadm.cfg**. Si nécessaire, vous pouvez configurer le fichier avec un autre nom.

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

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

La sous-commande **config** charge les informations dans l'autre iDRAC6. Utilisez **config** pour synchroniser la base de données des utilisateurs et des mots de passe avec Server Administrator.

Le nom du fichier de configuration initial, **racadm.cfg**, est défini par l'utilisateur. Dans l'exemple suivant, le fichier de configuration s'appelle **myfile.cfg**. Pour créer ce fichier, tapez la commande suivante à l'invite de commande :

```
racadm getconfig -f myfile.cfg
```

**PRÉCAUTION : il est recommandé de modifier ce fichier avec un simple éditeur de texte. L'utilitaire RACADM utilise un analyseur de texte ASCII. Tout formatage peut troubler l'analyseur et ainsi corrompre la base de données de la RACADM.**

### Création d'un fichier de configuration iDRAC6

Le fichier de configuration iDRAC6, **<*nom de fichier*>.cfg,** est utilisé avec la commande `racadm config -f <nom de fichier>.cfg`. Vous pouvez utiliser le fichier de configuration pour créer un fichier de configuration (similaire à un fichier **.ini**) et configurer iDRAC6 à partir de ce fichier. Vous pouvez utiliser n'importe quel nom de fichier et le fichier ne nécessite pas d'extension **.cfg** (bien qu'il y soit fait référence par ce nom d'extension dans cette sous-section).

Le fichier **.cfg** peut être :

- Créé
- obtenu à partir de la commande `racadm getconfig -f <nom de fichier>.cfg`,
- obtenu à partir de la commande `racadm getconfig -f <nom de fichier>.cfg`, puis modifié.

**REMARQUE :** pour des informations sur la commande **getconfig**, voir la commande getconfig du *Guide de référence de la ligne de commande RACADM pour iDRAC6 et CMC* disponible sur le site Web du support Dell à l'adresse **dell.com/support/manuals**.

Le fichier **.cfg** est d'abord analysé pour vérifier si des noms de groupe et d'objet valides sont présents et si quelques règles de syntaxe simples ont été observées. Les erreurs sont indiquées avec le numéro de ligne dans laquelle l'erreur a été détectée et un message simple explique le problème. Le fichier entier est analysé pour vérifier son exactitude et toutes les erreurs sont affichées. Les commandes d'écriture ne sont pas transmises à l'iDRAC6 si une erreur est trouvée dans le fichier **.cfg**. L'utilisateur doit corriger *toutes* les erreurs pour que la configuration ait lieu. L'option **-c** peut être utilisée avec la sous-commande **config** qui ne vérifie que la syntaxe et n'effectue *pas* d'opération d'écriture sur iDRAC6.

Suivez les instructions ci-dessous lorsque vous créez un fichier **.cfg** :

- Si l'analyseur rencontre un groupe indexé, l'index du groupe fait office d'ancre. Toutes les modifications apportées aux objets au sein du groupe indexé sont également associées à la valeur d'index.

  Par exemple :

  ```
  [cfgUserAdmin]

  # cfgUserAdminIndex=11

  cfgUserAdminUserName=

  # cfgUserAdminPassword=******** (Write-Only)

  cfgUserAdminEnable=0

  cfgUserAdminPrivilege=0x00000000

  cfgUserAdminIpmiLanPrivilege=15

  cfgUserAdminIpmiSerialPrivilege=15

  cfgUserAdminSolEnable=0
  ```

- Les index sont en lecture seule et ne peuvent pas être modifiés. Les objets du groupe indexé sont liés à l'index sous lequel ils sont répertoriés, et toute configuration valide de la valeur de l'objet s'applique uniquement à cet index spécifique.

- Un jeu d'index prédéfini est disponible pour chaque groupe indexé. Pour des informations supplémentaires, voir le *Guide de référence de la ligne de commande RACADM pour iDRAC6 et CMC* disponible sur le site Web du support de Dell à l'adresse **dell.com/support/manuals**.
- Utilisez la sous-commande **racresetcfg** pour réinitialiser iDRAC6 sur 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 requis.

**PRÉCAUTION : utilisez la sous-commande racresetcfg pour réinitialiser la base de données et les paramètres du NIC d'iDRAC6 sur les paramètres par défaut d'origine et supprimer tous les utilisateurs et les configurations utilisateur. Pendant que l'utilisateur root est disponible, les paramètres par défaut des autres utilisateurs sont également réinitialisés.**

## Règles d'analyse

- Toutes les lignes commençant par « # » sont traitées comme des commentaires.

  Une ligne de commentaire *doit* commencer dans la première colonne. Un caractère « # » dans une autre colonne est traité comme un caractère « # ».

  Certains paramètres de modem peuvent inclure les caractères # dans leur chaîne. Un caractère d'échappement n'est pas exigé. 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 iDRAC6 sans ajouter de caractères d'échappement.

  **Exemple** :

```
#

# Il s'agit d'un commentaire

[cfgUserAdmin]

cfgUserAdminPageModemInitString=<Init modem #
n'est pas un commentaire>
```

- Toutes les entrées de groupe doivent être entourées des caractères « [ » et « ] ».

  Le caractère de début « [ » indiquant un nom de groupe *doit* commencer dans la première colonne. 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 sont organisées en groupes, comme défini dans le *Guide de référence de la ligne de commande RACADM pour iDRAC6 et CMC* disponible sur le site Web du support de Dell à l'adresse **dell.com/support/manuals**.

  L'exemple suivant affiche un nom de groupe, un objet et la valeur de propriété de l'objet.

  **Exemple** :

  ```
  [cfgLanNetworking] - {nom de groupe}
  ```

  ```
  cfgNicIpAddress=143.154.133.121 {nom d'objet}
  ```

- 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. Les caractères à droite de « = » sont pris tels quels (par exemple, un second « = » ou un « # », « [ », « ] », etc.). Ces caractères sont des caractères de script de conversation de modem valides.

  Voir l'exemple de la puce précédente.

  La commande `racadm getconfig-f <nom de fichier>.cfg` place un commentaire devant les objets d'index, ce qui permet à l'utilisateur de voir les commentaires inclus.

  Pour voir le contenu d'un groupe indexé, utilisez la commande suivante :

  ```
  racadm getconfig -g <nom de groupe> -i
  <index 1-16>
  ```

- Pour les groupes indexés, l'ancre de l'objet *doit* être le premier objet après la paire « [ ] ». Voici des exemples de groupes indexés actuels :

  ```
  [cfgUserAdmin]
  ```

  ```
  cfgUserAdminIndex=11
  ```

Si vous tapez `racadm getconfig -f <monexemple>.cfg`, la commande construit un fichier **.cfg** pour la configuration iDRAC6 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 iDRAC6

Lorsque vous modifiez l'adresse IP iDRAC6 dans le fichier de configuration, supprimez toutes les entrées **<*variable*>=valeur** inutiles. Seul le nom du groupe variable réel avec « [ » et « ] » demeure, avec les deux entrées **<*variable*>= valeur** correspondant au changement d'adresse IP.

Par exemple :

```
#
#   Groupe d'objet « cfgLanNetworking »
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.10.110
cfgNicGateway=10.35.10.1
```

Ce fichier est mis à jour comme suit :

```
#
#   Groupe d'objet « cfgLanNetworking »
#
[cfgLanNetworking]
cfgNicIpAddress=10.35.9.143
# commentaire, le reste de cette ligne est ignoré
cfgNicGateway=10.35.9.1
```

La commande **racadm config-f myfile.cfg** analyse le fichier et identifie les erreurs par numéro de ligne. Un fichier correct met à jour les entrées appropriées. En outre, vous pouvez utiliser la commande **getconfig** utilisée dans l'exemple précédent pour confirmer la mise à jour.

Utilisez ce fichier pour télécharger des modifications à l'échelle de la société ou pour configurer de nouveaux systèmes sur le réseau.

**REMARQUE :** « ancre » est un terme interne et ne doit pas être utilisé dans le fichier.

### Configuration des propriétés réseau iDRAC6

Pour générer une liste des propriétés réseau disponibles, tapez la commande suivante :

```
racadm getconfig -g cfgLanNetworking
```

Pour utiliser DHCP pour obtenir une adresse IP, utilisez la commande suivante pour écrire l'objet **cfgNicUseDhcp** et activer cette fonctionnalité :

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

Les commandes fournissent la même fonctionnalité de configuration que l'utilitaire de configuration d'iDRAC6 au démarrage lorsque vous êtes invité à taper <Ctrl><E>. Pour plus d'informations sur la configuration des propriétés du réseau à l'aide de l'utilitaire de configuration d'iDRAC6, voir « Configuration de votre système pour utiliser un iDRAC6 », à la page 36.

L'exemple suivant montre comment la commande peut être utilisée pour configurer les propriétés réseau du LAN souhaitées.

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

racadm config -g cfgLanNetworking -o cfgNicIpAddress
192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicNetmask
255.255.255.0

racadm config -g cfgLanNetworking -o cfgNicGateway
192.168.0.120

racadm config -g cfgLanNetworking -o cfgNicUseDhcp 0

racadm config -g cfgLanNetworking -o
cfgDNSServersFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSServer1
192.168.0.5
```

```
racadm config -g cfgLanNetworking -o cfgDNSServer2
192.168.0.6

racadm config -g cfgLanNetworking -o
cfgDNSRegisterRac 1

racadm config -g cfgLanNetworking -o cfgDNSRacName
RAC-EK00002

racadm config -g cfgLanNetworking -o
cfgDNSDomainNameFromDHCP 0

racadm config -g cfgLanNetworking -o cfgDNSDomainName
MYDOMAIN
```

**REMARQUE :** si la commande **cfgNicEnable** est définie sur **0**, le LAN iDRAC6 est désactivé, même si DHCP est activé.

### Modes iDRAC6

iDRAC6 peut être configuré dans l'un des quatre modes :

- Dédié
- Partagé
- Partagé avec basculement LOM2
- Partagé avec basculement tous les LOM

Le Tableau 5-14 fournit une description de chaque mode.

**Tableau 5-14. Configurations du NIC d'iDRAC6**

| Mode | Description |
|---|---|
| Dédié | iDRAC6 utilise son propre NIC (connecteur RJ-45) et l'adresse MAC d'iDRAC pour le trafic réseau. |
| Partagé | iDRAC6 utilise LOM1 sur le planaire. |
| Partagé avec basculement LOM2 | iDRAC6 utilise LOM1 et LOM2 comme groupe pour le basculement. Le groupe utilise l'adresse MAC iDRAC6. |
| Partagé avec basculement tous les LOM | iDRAC6 utilise LOM1, LOM2, LOM3 et LOM4 comme groupe pour le basculement. Le groupe utilise l'adresse MAC iDRAC6. |

# Questions les plus fréquentes concernant la sécurité réseau

**Lorsque j'accède à l'interface Web iDRAC6, un avertissement de sécurité s'affiche et indique que le nom d'hôte du certificat SSL ne correspond pas au nom d'hôte d'iDRAC6.**

iDRAC6 est doté d'un certificat de serveur iDRAC6 par défaut qui assure la sécurité du réseau pour l'interface Web et les fonctionnalités de la RACADM distante. Lorsque ce certificat est utilisé, le navigateur Web affiche un avertissement de sécurité, car le certificat par défaut est émis sur le **certificat par défaut iDRAC6**, lequel ne correspond pas au nom d'hôte d'iDRAC6 (l'adresse IP, par exemple).

Pour résoudre ce problème de sécurité, téléversez un certificat de serveur iDRAC6 émis sur l'adresse IP ou le nom iDRAC d'iDRAC6. Lors de la génération d'une requête de signature de certificat (RSC) utilisée pour émettre le certificat, assurez-vous que le nom de domaine (CN) de la RSC correspond à l'adresse IP (**si le certificat est émis sur IP**) d'iDRAC6 (par exemple, 192.168.0.120) ou au nom iDRAC6 DNS enregistré (**si le certificat est émis au nom enregistré d'iDRAC**).

Afin de vous assurer que la RSC corresponde bien au nom iDRAC6 DNS enregistré :

1. Dans l'arborescence du **Système**, cliquez sur **Paramètres iDRAC**.
2. Cliquez sur l'onglet **Réseau/Sécurité**, puis sur **Réseau**.
3. Dans le tableau **Paramètres communs** :
   a. Sélectionnez la case à cocher **Enregistrer iDRAC sur DNS**.
   b. Dans le champ **Nom IDRAC DNS**, saisissez le nom d'iDRAC6.
4. Cliquez sur **Appliquer les modifications**.

Voir « Sécurisation des communications iDRAC6 à l'aide de certificats SSL et numériques », à la page 381 pour plus d'informations sur la génération de RSC et l'émission de certificats.

**RACADM distante et les services Web ne sont plus disponibles lorsque les propriétés sont modifiées. Pourquoi ?**

Lorsque vous réinitialisez le serveur Web iDRAC6, il peut s'écouler un certain temps avant que les services de la RACADM distante et l'interface Web ne redeviennent disponibles.

Le serveur Web iDRAC6 est réinitialisé dans les cas suivants :

- les propriétés de configuration réseau ou de sécurité réseau sont modifiées à l'aide de l'interface utilisateur Web d'iDRAC6,
- quand la propriété **cfgRacTuneHttpsPort** est modifiée (y compris lorsqu'une commande config -f <*fichier config*> la modifie),
- quand on utilise **racresetcfg,**
- iDRAC6 est réinitialisé,
- quand un nouveau certificat de serveur SSL est téléversé.

**Mon serveur DNS n'enregistre pas mon iDRAC6. Pourquoi ?**

certains serveurs DNS ne peuvent enregistrer que des noms de 31 caractères maximum.

**Lorsque j'accède à l'interface Web iDRAC6, un avertissement de sécurité s'affiche ; il m'informe que le certificat SSL a été émis par une autorité de certification (AC) qui n'est pas fiable.**

iDRAC6 est doté d'un certificat de serveur iDRAC6 par défaut qui assure la sécurité du réseau pour l'interface Web et les fonctionnalités de la RACADM distante. Ce certificat n'a pas été émis par une AC de confiance. Pour résoudre ce problème de sécurité, téléversez un certificat de serveur iDRAC6 émis par une AC de confiance (Microsoft Certificate Authority, Thawte ou Verisign, par exemple). Voir « Sécurisation des communications iDRAC6 à l'aide de certificats SSL et numériques », à la page 381 pour plus d'informations sur l'émission de certificats.

# 6

# Ajout et configuration d'utilisateurs iDRAC6

Pour gérer votre système avec iDRAC6 et maintenir la sécurité du système, créez des utilisateurs uniques avec des droits d'administrateur 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.

## Utilisation de l'interface Web pour configurer des utilisateurs iDRAC6

### Ajout et configuration d'utilisateurs iDRAC6

Pour gérer votre système avec iDRAC6 et maintenir la sécurité du système, créez des utilisateurs uniques avec des droits d'administrateur spécifiques (ou *autorité basée sur les rôles*).

Pour ajouter et configurer des utilisateurs iDRAC6, effectuez les étapes suivantes :

**REMARQUE :** vous devez disposer du droit **Configurer des utilisateurs** pour configurer un utilisateur iDRAC.

1. Cliquez sur **Paramètres iDRAC→ Réseau/Sécurité→ Utilisateurs**.

   La page **Utilisateurs** (voir le Tableau 6-1) affiche les informations suivantes pour les utilisateurs d'iDRAC6 : **Réf. utilisateur**, **État** (Activé/Désactivé), **Nom d'utilisateur**, **iDRAC**, **LAN**, **Port série** et **Communications série sur le LAN** (Activé/Désactivé).

**REMARQUE :** utilisateur 1 est réservé pour l'utilisateur anonyme IPMI et vous ne pouvez pas changer cette configuration.

2. Dans la colonne **Réf. utilisateur**, cliquez sur un numéro de référence utilisateur.

Sur la page **Menu principal utilisateur** (voir le Tableau 6-2 et le Tableau 6-7), vous pouvez configurer un utilisateur, afficher ou téléverser un certificat d'utilisateur, téléverser un certificat d'une autorité de certification (AC) de confiance, afficher un certificat d'une AC de confiance, téléverser un fichier de clé publique SSH (Secure Shell) ou afficher ou supprimer une clé SSH spécifiée ou toutes les clés SSH.

Si vous sélectionnez **Configurer l'utilisateur** et cliquez sur **Suivant**, la page **Configuration de l'utilisateur** apparaît.

3 Dans la page **Configuration de l'utilisateur**, configurez les éléments suivants :

- Nom d'utilisateur, mot de passe et droits d'accès pour un nouvel utilisateur iDRAC ou un utilisateur iDRAC existant. Le Tableau 6-3 décrit les **Paramètres généraux de l'utilisateur**.
- Les privilèges IPMI de l'utilisateur.Le Tableau 6-4 décrit les **Privilèges d'utilisateur IPMI** pour la configuration des privilèges LAN de l'utilisateur.
- Les privilèges d'utilisateur iDRAC.Le Tableau 6-5 décrit les **Privilèges d'utilisateur iDRAC**.
- Les droits d'accès du groupe iDRAC.Le Tableau 6-6 décrit les **Droits d'accès du groupe iDRAC**.

4 Lorsque vous avez terminé, cliquez sur **Appliquer les changements**.

5 Cliquez sur **Retourner à la page des utilisateurs** pour retourner à la page des utilisateurs.

**Tableau 6-1. États et droits d'utilisateur**

| Paramètre | Description |
|---|---|
| **Réf. utilisateur** | Affiche la liste séquentielle des numéros de référence utilisateur. Chaque champ sous **Réf. utilisateur** contient l'un des 16 numéros de référence utilisateur prédéfinis. Ce champ ne peut pas être modifié. |
| **State (État)** | Affiche l'état d'ouverture de session de l'utilisateur : Activé ou Désactivé. (Désactivé est la valeur par défaut.)<br>**REMARQUE :** l'utilisateur 2 est activé par défaut. |

**Tableau 6-1. États et droits d'utilisateur *(suite)***

| Paramètre | Description |
|---|---|
| Nom d'utilisateur | Affiche le nom d'ouverture de session de l'utilisateur. Spécifie un nom d'utilisateur iDRAC6 contenant jusqu'à 16 caractères. Chaque utilisateur doit avoir un nom d'utilisateur unique.<br>**REMARQUE :** Si le nom d'utilisateur est modifié, le nouveau nom n'apparaît pas dans l'interface utilisateur jusqu'à la prochaine ouverture de session utilisateur. |
| iDRAC | Définit le groupe (niveau de privilège) auquel l'utilisateur est affecté (Administrateur, Opérateur, Lecture seule ou Aucun). |
| LAN | Affiche le niveau de privilège LAN IPMI auquel l'utilisateur est affecté (Administrateur, Opérateur, Lecture seule ou Aucun). |
| Serial Port (Port série) | Affiche le niveau de privilège de port série IPMI auquel l'utilisateur est affecté (Administrateur, Opérateur, Lecture seule ou Aucun). |
| Serial Over LAN (Série sur LAN) | Permet ou interdit à l'utilisateur d'utiliser les communications série sur le LAN IPMI. |

**Tableau 6-2. Options de configuration de la carte à puce**

| Option | Description |
|---|---|
| Téléverser le certificat d'utilisateur | Permet à l'utilisateur de téléverser le certificat d'utilisateur vers iDRAC6 et de l'importer dans le profil utilisateur. |
| Consulter le Certificat de l'utilisateur | Affiche la page Certificat de l'utilisateur qui a été téléversée vers iDRAC. |
| Télécharger le Certificat CA de confiance | Vous permet de téléverser le certificat d'une autorité de certification de confiance sur iDRAC et de l'importer dans le profil utilisateur. |
| Afficher le certificat d'une autorité de certification de confiance | Affiche le certificat d'une autorité de certification de confiance qui a été téléversé vers iDRAC. Le certificat d'une autorité de certification de confiance est émis par l'AC qui est autorisée à émettre des certificats aux utilisateurs. |

**Tableau 6-3. Paramètres généraux de l'utilisateur**

| | |
|---|---|
| **Réf. utilisateur** | Un des 16 numéros de référence utilisateur prédéfinis. |
| **Activer l'utilisateur** | Lorsqu'elle est cochée, cette case indique que l'accès de l'utilisateur à iDRAC6 est activé. Lorsqu'elle est décochée, l'accès utilisateur est désactivé. |
| **Nom d'utilisateur** | Nom d'utilisateur comportant jusqu'à 16 caractères.<br>Les caractères suivants sont pris en charge :<br>• 0-9<br>• A-Z<br>• a-z<br>• Caractères spéciaux :<br>+ % ) ' > : $ [ \|<br>! & = * , - { ] §<br># ( ? < ; _ } I |
| **Modifier le mot de passe** | Active les champs **Nouveau mot de passe** et **Confirmer le nouveau mot de passe**. Lorsque cette option n'est pas sélectionnée, le mot de passe de l'utilisateur ne peut pas être modifié. |
| **Nouveau mot de passe** | Entrez un **mot de passe** avec un maximum de 16 caractères. Les caractères ne s'affichent pas et sont masqués.<br>Les caractères suivants sont pris en charge :<br>• 0-9<br>• A-Z<br>• a-z<br>• Caractères spéciaux :<br>+ & ? > - } \| .<br>! ( ' , _ [ ». @<br># ) * ; $ ] / §<br>% = < : { I \ |
| **Confirmer le nouveau mot de passe** | Retapez le mot de passe de l'utilisateur iDRAC pour le confirmer. |

**Tableau 6-4. Privilèges d'utilisateur IPMI**

| Propriété | Description |
|---|---|
| **Privilège maximal de l'utilisateur accordé sur le LAN** | Spécifie le privilège maximal de l'utilisateur sur le canal LAN IPMI sur l'un des groupes d'utilisateurs suivants : **Administrateur**, **Opérateur**, **Utilisateur** ou **Aucun**. |
| **Privilège maximal de l'utilisateur accordé sur le port série** | Spécifie le privilège maximal de l'utilisateur sur le canal série IPMI sur l'un des groupes d'utilisateurs suivants : **Administrateur**, **Opérateur**, **Utilisateur** ou **Aucun**. |
| **Activation des communications série sur LAN** | Permet à l'utilisateur d'utiliser les communications série sur LAN IPMI. Lorsque cette option est cochée, ce privilège est activé. |

**Tableau 6-5. Privilèges utilisateur iDRAC**

| Propriété | Description |
|---|---|
| Roles (Rôles) | Spécifie le privilège maximal d'utilisateur iDRAC de l'utilisateur sur l'un des privilèges suivants : **Administrateur**, **Opérateur**, **Lecture seule** ou **Aucun**. Voir le Tableau 6-6 pour connaître les **Droits du groupe iDRAC**. |
| Ouvrir une session sur iDRAC | Permet à l'utilisateur d'ouvrir une session sur iDRAC. |
| Configurer iDRAC | Permet à l'utilisateur de configurer iDRAC. |
| Configurer les utilisateurs | Permet à l'utilisateur de permettre à des utilisateurs spécifiques d'accéder au système.<br>**PRÉCAUTION : ce privilège est généralement réservé aux utilisateurs membres du rôle Administrateur sur iDRAC. Toutefois, les utilisateurs du rôle « Opérateur » peuvent se voir attribuer ce privilège. Un utilisateur doté de ce privilège est en mesure de modifier la configuration de n'importe quel utilisateur. Ceci inclut la création ou la suppression de n'importe quel utilisateur, la gestion des clés SSH pour les utilisateurs, etc. Pour ces raisons, attribuez ce privilège avec vigilance.** |
| Effacer des journaux | Permet à l'utilisateur d'effacer les journaux iDRAC. |

**Tableau 6-5. Privilèges utilisateur iDRAC *(suite)***

| Propriété | Description |
|---|---|
| Exécuter les commandes de contrôle du serveur | Permet à l'utilisateur d'exécuter des commandes de contrôle du serveur. |
| Accéder à la console virtuelle | Permet à l'utilisateur d'exécuter la console virtuelle. |
| Accéder au média virtuel | Permet à l'utilisateur d'exécuter et d'utiliser le média virtuel. |
| Alertes test | Permet à l'utilisateur d'envoyer des alertes test (par e-mail et PET) à un utilisateur spécifique. |
| Exécuter des commandes de diagnostic | Permet à l'utilisateur d'exécuter des commandes de diagnostic. |

**Tableau 6-6. Droits du groupe iDRAC**

| Groupe d'utilisateurs | Droits accordés |
|---|---|
| Administrateur | Ouvrir une session iDRAC, Configurer iDRAC, Configurer les utilisateurs, Effacer les journaux, Exécuter des commandes de contrôle du serveur, Accéder à la console virtuelle, Accès au média virtuel, Tester les alertes, Exécution des commandes de diagnostic |
| Opérateur | Sélectionne parmi les autorisations suivantes : Ouvrir une session iDRAC, Configurer iDRAC, Configurer les utilisateurs, Effacer les journaux, Exécuter des commandes d'action du serveur, Accéder à la console virtuelle, Accès au média virtuel, Tester les alertes, Exécution des commandes de diagnostic |
| Lecture uniquement | Ouvrir une session sur iDRAC |
| None (Aucune) | Aucun droit attribué |

## Authentification par clé publique sur SSH

iDRAC6 prend en charge l'authentification par clé publique (PKA) sur SSH. Cette méthode d'authentification améliore l'automatisation avec script SSH en éliminant la nécessité d'intégrer ou de demander la réf. utilisateur/le mot de passe.

#### Avant de commencer

Vous pouvez configurer jusqu'à 4 clés publiques *par utilisateur* qui peuvent être utilisées sur une 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. Lorsque PKA sur SSH est configuré et utilisé correctement, vous n'avez pas à saisir le nom d'utilisateur ou le mot de passe lorsque vous ouvrez une session sur iDRAC6. Ceci peut s'avérer très utile pour configurer des scripts automatisés pour exécuter diverses fonctions.

Lorsque vous êtes prêt à configurer cette fonctionnalité, tenez compte des points suivants :

- Vous pouvez gérer cette fonctionnalité à l'aide de la RACADM et également depuis l'interface utilisateur.
- Lorsque vous ajoutez des clés publiques, vérifiez que les clés existantes ne figurent pas déjà dans l'index dans lequel la nouvelle clé est ajoutée. iDRAC6 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.

#### Génération de clés publiques pour Windows

Avant d'ajouter un compte, le système qui accèdera à iDRAC6 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. L'utilitaire de la CLI *ssh-keygen* est disponible par défaut sur toutes les installations standard.

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. RSA et DSA sont les seuls algorithmes de génération de clé pris en charge. Saisissez le nombre de bits de la clé. Ce nombre doit être compris entre 768 et 4 096 bits pour RSA et 1 024 bits pour DSA.

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 enregistrer la clé publique dans un fichier à l'aide de l'option « Enregistrer la clé publique » en vue de son téléversement ultérieur. Toutes les clés téléversées doivent être au format RFC 4716 ou openssh. Si ce n'est pas le cas, vous devez les convertir dans ce format.

#### 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 à l'invite shell, entrez :

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

**REMARQUE :** Les options sont sensibles à la casse.

où

l'option **-t** peut 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.

Suivez les instructions. Une fois la commande exécutée, téléversez le fichier public.

**PRÉCAUTION : les clés générées à partir de Linux Management Station avec ssh-keygen ne sont pas au format 4716. Convertissez les clés au format 4716 via** `ssh-keygen -e -f /root/.ssh/id_rsa.pub > std_rsa.pub`. **Ne modifiez pas les droits du fichier de clé. La conversion ci-dessus doit être effectuée à l'aide des droits par défaut.**

**REMARQUE :** iDRAC6 ne prend pas en charge le transfert des clés via ssh-agent.

#### Ouverture de session avec l'authentification par clé publique

Une fois les clés publiques téléversées, vous pouvez ouvrir une session sur iDRAC6 sur SSH sans saisir de 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 la RACADM distante, car la session se termine une fois la commande exécutée.

Par exemple :

**Ouverture de session :**

```
ssh username@<domaine>
```

Ou bien,

```
ssh username@<adresse_IP>
```

où adresse_IP correspond à l'adresse IP d'iDRAC6.

**Envoi de commandes racadm :**

```
ssh username@<domaine> racadm getversion
ssh username@<domaine> racadm getsel
```

### Téléversement, affichage et suppression de clés SSH avec l'interface Web iDRAC6

1. Cliquez sur **Paramètres iDRAC→ Réseau/Sécurité→ Utilisateurs**. La page **Utilisateurs** s'affiche.
2. Dans la colonne **Réf. utilisateur**, cliquez sur un numéro de référence utilisateur. La page **Menu principal utilisateur** s'affiche.
3. Utilisez les options **Configurations de clé SSH** pour téléverser, afficher ou supprimer une ou des clés SSH.

**PRÉCAUTION : La capacité à téléverser, à afficher et/ou à supprimer les clés SSH repose sur le privilège utilisateur « Configurer les utilisateurs ». Ce privilège permet aux utilisateurs de configurer la clé SSH de n'importe quel autre utilisateur. Vous devez octroyer ce privilège avec vigilance. Pour plus d'informations sur les privilèges utilisateur, voir « Ajout et configuration d'utilisateurs iDRAC6 », à la page 135.**

**Tableau 6-7. Configurations de clé SSH**

| Option | Description |
|---|---|
| **Téléverser une ou des clés SSH** | Permet à l'utilisateur local de téléverser un fichier de clé publique SSH (Secure Shell). Si une clé est téléversée, le contenu du fichier de clé s'affiche dans une zone de texte non modifiable de la page **Configuration de l'utilisateur**. |
| **Afficher/Supprimer une ou des clés SSH** | Permet à l'utilisateur local d'afficher ou de supprimer une clé SSH spécifiée ou toutes les clés SSH. |

La page **Téléverser une ou des clés SSH** vous permet de téléverser un fichier de clé publique SSH (Secure Shell). Si une clé est téléversée, le contenu du fichier de clé s'affiche dans une zone de texte non modifiable sur la page **Afficher/Supprimer une ou des clés SSH**

**Tableau 6-8. Téléverser une ou des clés SSH**

| Option | Description |
|---|---|
| **Fichier/Texte** | Sélectionnez l'option **Fichier** et tapez le chemin de l'emplacement de la clé. Vous pouvez également sélectionner l'option **Texte** et coller le contenu du fichier de clé dans la zone. Vous pouvez téléverser de nouvelles clés ou écraser des clés existantes. Pour téléverser un fichier de clé, cliquez sur **Parcourir**, sélectionnez le fichier, puis cliquez sur le bouton **Appliquer**. |
| **Parcourir** | Cliquez sur ce bouton pour identifier le chemin complet et le nom de fichier de la clé. |

La page **Afficher/Supprimer une ou des clés SSH** vous permet d'afficher ou de supprimer les clés publiques SSH de l'utilisateur.

**Tableau 6-9. Afficher/Supprimer une ou des clés SSH**

| Option | Description |
|---|---|
| **Supprimer** | La clé téléversée s'affiche dans la zone. Sélectionnez l'option Supprimer et cliquez sur **Appliquer** pour supprimer la clé existante. |

### Téléversement, affichage et suppression de clés SSH avec la RACADM

**Téléverser**

Le mode Téléversement vous permet de téléverser un fichier de clé ou de copier le texte de clé sur la ligne de commande. Vous ne pouvez pas téléverser et copier une clé simultanément.

*RACADM locale et RACADM distante :*

```
racadm sshpkauth -i <2 à 16> -k <1 à 4> -f
<nom de fichier>

racadm sshpkauth -i <2 à 16> -k <1 à 4> -t

<texte de clé>
```

*RACADM Telnet/SSH/série :*

```
racadm sshpkauth -i <2 à 16> -k <1 à 4> -t

<texte de clé>
```

*Exemple :*

Téléversez une clé valide sur l'utilisateur 2 d'iDRAC6 dans l'espace de la première clé à l'aide d'un fichier :

```
$ racadm sshpkauth -i 2 -k 1 -f pkkey.key
```

Le fichier de clé d'authentification SSH PK est téléversé avec succès vers le RAC.

**PRÉCAUTION : l'option « texte de clé » n'est pas prise en charge sur la RACADM locale et distante. L'option « fichier » n'est pas prise en charge sur la RACADM Telnet/ssh/série.**

**Afficher**

Le mode Affichage permet à l'utilisateur d'afficher une clé spécifiée par l'utilisateur ou toutes les clés.

```
racadm sshpkauth -i <2 à 16> -v -k <1 à 4>

racadm sshpkauth -i <2 à 16> -v -k all
```

**Supprimer**

Le mode Suppression permet à l'utilisateur de supprimer une clé spécifiée par l'utilisateur ou toutes les clés.

```
racadm sshpkauth -i <2 à 16> -d -k <1 à 4>

racadm sshpkauth -i <2 à 16> -d -k all
```

Pour des informations sur les options de sous-commande, voir la sous-commande `sshpkauth` du *Guide de référence de la ligne de commande pour iDRAC6 et CMC* disponible sur le site Web du support de Dell à l'adresse **dell.com/support/manuals**.

# Utilisation de l'utilitaire de la RACADM pour configurer les utilisateurs iDRAC6

**REMARQUE :** vous devez avoir ouvert une session en tant qu'utilisateur **root** pour exécuter les commandes RACADM sur un système Linux distant.

Un ou plusieurs utilisateurs iDRAC6 peuvent être configurés avec la ligne de commande RACADM installée avec les agents iDRAC6 sur le système géré.

Pour configurer plusieurs iDRAC6 avec des paramètres de configuration identiques, effectuez l'une des procédures suivantes :

- Utilisez les exemples de RACADM indiqués dans cette section comme guide pour créer un fichier séquentiel de commandes RACADM, puis exécutez le fichier séquentiel sur chaque système géré.
- Créez le fichier de configuration iDRAC6 tel que décrit dans le *Guide de référence de la ligne de commande pour iDRAC6 et CMC* disponible sur le site Web du support de Dell à l'adresse **dell.com/support/manuals** et exécutez la sous-commande **racadm config** sur chaque système géré par le biais du même fichier de configuration.

## Avant de commencer

Vous pouvez configurer jusqu'à 16 utilisateurs dans la base de données de propriétés iDRAC6. Avant d'activer manuellement un utilisateur iDRAC6, vérifiez s'il existe des utilisateurs actuels. si vous configurez un nouvel iDRAC6 ou si vous avez exécuté la commande **racadm racresetcfg**, le seul utilisateur actuel est `root` avec le mot de passe `calvin`. La sous-commande **racresetcfg** réinitialise les valeurs par défaut d'origine d'iDRAC6.

**PRÉCAUTION : soyez prudent lorsque vous utilisez la commande racresetcfg, car les valeurs par défaut de *tous* les paramètres de configuration sont réinitialisées. Toute modification précédente est perdue.**

**REMARQUE :** les utilisateurs peuvent être activés et désactivés à tout moment. Par conséquent, un utilisateur peut avoir un numéro d'index différent sur chaque iDRAC6.

Pour déterminer si un utilisateur existe, tapez la commande suivante à l'invite de commande :

```
racadm getconfig -u <nom d'utilisateur>
```

OU

tapez la commande suivante une fois pour chaque index de 1 à 16 :

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

**REMARQUE :** vous pouvez également taper `racadm getconfig -f <monfichier.cfg>` et afficher ou modifier le fichier **monfichier.cfg** qui contient tous les paramètres de configuration d'iDRAC6.

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 « = », cet 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 avec 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/d'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 pour configurer plusieurs iDRAC6 avec les mêmes paramètres.

### Ajout d'un utilisateur iDRAC6

Pour ajouter un nouvel utilisateur à la configuration du RAC, quelques commandes de base peuvent être utilisées. En général, effectuez les procédures suivantes :

1. Définissez le nom d'utilisateur.
2. Définissez le mot de passe.
3. Spécifiez les privilèges d'utilisateur suivants :
   - iDRAC
   - LAN

- Serial Port (Port série)
- Serial Over LAN (Série sur LAN)

4 Activez l'utilisateur.

**Exemple**

L'exemple suivant décrit comment ajouter un nouvel utilisateur appelé « John » avec un mot de passe « 123456 » et des privilèges d'ouverture de session au RAC.

```
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
cfgUserAdminIpmiLanPrivilege 4

racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminIpmiSerialPrivilege 4

racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminSolEnable 1

racadm config -g cfgUserAdmin -i 2 -o
cfgUserAdminEnable 1
```

Pour vérifier, utilisez l'une des commandes suivantes :

```
racadm getconfig -u john

racadm getconfig -g cfgUserAdmin -i 2
```

## Suppression d'un utilisateur iDRAC6

Lorsque vous utilisez la RACADM, les utilisateurs doivent être désactivés manuellement et individuellement. Les utilisateurs ne peuvent pas être supprimés à l'aide d'un fichier de configuration.

L'exemple suivant illustre la syntaxe de commande qui peut être utilisée pour supprimer un utilisateur iDRAC6 :

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName
-i <index> ""
```

Une chaîne de guillemets nulle ("") donne l'ordre à iDRAC6 de supprimer la configuration de l'utilisateur à l'index indiqué et de réinitialiser les valeurs d'usine d'origine de la configuration de l'utilisateur.

### Activation d'un utilisateur iDRAC6 avec 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 », à la page 146. Ensuite, tapez les lignes de commande suivantes avec le nouveau nom d'utilisateur et le nouveau mot de passe.

**REMARQUE :** Pour accéder à la liste des valeurs de masque binaire valides pour des privilèges utilisateur spécifiques, voir le *Guide de référence de la ligne de commande pour iDRAC6 et CMC* disponible sur le site Web du support de Dell à l'adresse **dell.com/support/manuals**. La valeur de privilège par défaut est 0, indiquant que l'utilisateur n'a aucun privilège activé.

```
racadm config -g cfgUserAdmin -o
cfgUserAdminPrivilege -i <index> <valeur de masque
binaire du privilège d'utilisateur>
```

# 7

# Utilisation du service de répertoire iDRAC6

Un service de répertoire permet de maintenir une base de données commune afin d'y stocker des informations concernant les utilisateurs, les ordinateurs, les imprimantes, etc. d'un réseau. Si votre société utilise le logiciel Microsoft Active Directory ou le logiciel de service d'annuaire LDAP, vous pouvez le configurer pour accéder à iDRAC6, ce qui vous permet d'ajouter et de contrôler les privilèges utilisateur iDRAC6 pour les utilisateurs existants au sein de votre service de répertoire.

## Utilisation d'iDRAC6 avec Microsoft Active Directory

**REMARQUE :** L'utilisation d'Active Directory pour la reconnaissance des utilisateurs iDRAC6 est prise en charge sur les systèmes d'exploitation Microsoft Windows 2000, Windows Server 2003 et Windows Server 2008.

Vous pouvez configurer l'authentification utilisateur via Microsoft Active Directory afin d'ouvrir une session iDRAC6. Vous pouvez également octroyer l'autorité selon les rôles, ce qui permet à un administrateur de configurer des privilèges spécifiques pour chaque utilisateur. Pour des informations supplémentaires, consultez les sections suivantes.

Le Tableau 7-1 affiche les privilèges utilisateur Active Directory iDRAC6.

**Tableau 7-1. Privilèges utilisateur iDRAC6**

| Privilège | Description |
|---|---|
| **Ouvrir une session sur iDRAC** | Permet à l'utilisateur d'ouvrir une session sur iDRAC6 |
| **Configurer iDRAC** | Permet à l'utilisateur de configurer iDRAC6 |
| **Configurer les utilisateurs** | Permet à l'utilisateur de permettre à des utilisateurs spécifiques d'accéder au système |

**Tableau 7-1. Privilèges utilisateur iDRAC6 *(suite)***

| Privilège | Description |
|---|---|
| **Effacer des journaux** | Permet à l'utilisateur d'effacer les journaux iDRAC6 |
| **Exécuter les commandes de contrôle du serveur** | Permet à l'utilisateur d'exécuter des commandes RACADM |
| **Accéder à la console virtuelle** | Permet à l'utilisateur d'exécuter la console virtuelle |
| **Accéder au média virtuel** | Permet à l'utilisateur d'exécuter et d'utiliser le média virtuel |
| **Alertes test** | Permet à l'utilisateur d'envoyer des alertes test (par e-mail et PET) à un utilisateur spécifique |
| **Exécuter des commandes de diagnostic** | Permet à l'utilisateur d'exécuter des commandes de diagnostic |

Vous pouvez utiliser Active Directory pour ouvrir une session sur iDRAC6 via une des méthodes suivantes :

- Interface Web
- RACADM distante
- Console série ou Telnet

La syntaxe d'ouverture de session est la même pour les trois méthodes :

`<nom d'utilisateur@domaine>`

Ou bien,

`<domaine>\<nom d'utilisateur>` ou `<domaine>/<nom d'utilisateur>`

où *nom d'utilisateur* est une chaîne ASCII de 1 à 256 octets.

Les espaces blancs et les caractères spéciaux (comme \, / ou @) ne peuvent pas être utilisés pour le nom d'utilisateur ou le nom de domaine.

**REMARQUE :** Vous ne pouvez pas spécifier de noms de domaine NetBIOS, tels que Amériques, car ces noms ne peuvent pas être résolus.

Si vous ouvrez une session depuis l'interface Web et que vous avez configuré des domaines utilisateur, la page d'ouverture de session de l'interface Web indique tous les domaines utilisateur parmi lesquels vous pouvez choisir dans le menu déroulant. Si vous sélectionnez un domaine utilisateur depuis le menu déroulant, il vous suffit de saisir le nom d'utilisateur. Si vous sélectionnez **Cet iDRAC**, vous pouvez toujours ouvrir une session en tant qu'utilisateur Active Directory en utilisant la syntaxe d'ouverture de session décrite ci-dessus dans cette section.

Vous pouvez également ouvrir une session iDRAC6 par carte à puce ou connexion directe. Pour plus d'informations, voir « Configuration d'iDRAC6 en vue de l'ouverture de session par connexion directe ou carte à puce », à la page 201.

**REMARQUE :** le serveur?Windows 2008 Active Directory prend uniquement en charge la chaîne <*nom_d'utilisateur*>@<*nom_de_domaine*> avec 256 caractères maximum.

# Conditions requises pour l'activation de l'authentification Microsoft Active Directory pour iDRAC6

Pour utiliser la fonctionnalité Authentification Active Directory d'iDRAC6, vous devez déjà avoir déployé une infrastructure Active Directory. Consultez le site Web de Microsoft pour des informations sur la configuration d'une infrastructure Active Directory si vous n'en avez pas déjà une.

iDRAC6 utilise le mécanisme d'infrastructure à clé publique (PKI) standard pour s'authentifier en toute sécurité sur Active Directory ; vous aurez donc également besoin d'une PKI intégrée dans l'infrastructure Active Directory. Consultez le site Web de Microsoft pour plus d'informations sur la configuration de PKI.

Pour vous authentifier correctement sur tous les contrôleurs de domaine, vous devez également activer Secure Socket Layer (SSL) sur tous les contrôleurs de domaine auxquels se connecte iDRAC6. Pour des informations plus spécifiques, voir « Activation de SSL sur un contrôleur de domaine », à la page 154.

### Activation de SSL sur un contrôleur de domaine

Lorsque iDRAC authentifie les utilisateurs par rapport à un contrôleur de domaine d'Active Directory, il démarre une session SSL avec le contrôleur de domaine. À ce stade, le contrôleur de domaine doit publier un certificat signé par l'autorité de certification (AC), dont le certificat racine est également téléversé vers iDRAC. En d'autres termes, pour qu'iDRAC soit capable de s'authentifier sur *n'importe quel* contrôleur de domaine, qu'il s'agisse du contrôleur de domaine racine ou enfant, ce contrôleur de domaine doit avoir un certificat activé SSL signé par l'AC du domaine.

Si vous utilisez l'AC racine d'entreprise Microsoft pour attribuer *automatiquement* un certificat SSL à tous vos contrôleurs de domaine, effectuez les étapes suivantes pour activer SSL sur chaque contrôleur de domaine :

Activez SSL sur chacun de vos contrôleurs de domaine en installant le certificat SSL pour chaque contrôleur.

1. Cliquez sur **Démarrer→ Outils d'administration→ Règle de sécurité du domaine**.
2. Développez le dossier **Règles de clé publique**, cliquez avec le bouton droit de la souris sur **Paramètres de requête automatique de certificat** et cliquez sur **Requête automatique de certificat**.
3. Dans l'**Assistant Configuration de requêtes automatiques de certificats**, cliquez sur **Suivant** et sélectionnez **Contrôleur de domaine**.
4. Cliquez sur **Suivant**, puis sur **Terminer**.

### Exportation du certificat d'autorité de certification racine du contrôleur de domaine sur iDRAC6

**REMARQUE :** si votre système fonctionne sous Windows 2000 ou si vous utilisez une autorité de certification autonome, les étapes suivantes peuvent varier.

1. Localisez le contrôleur de domaine qui exécute le service AC d'entreprise Microsoft.
2. Cliquez sur **Démarrer→ Exécuter**.
3. Dans le champ **Exécuter**, tapez `mmc` et cliquez sur **OK**.
4. Dans la fenêtre **Console 1** (MMC), cliquez sur **Fichier** (ou **Console** pour les systèmes Windows 2000) et sélectionnez **Ajouter/Supprimer un snap-in**.

5 Dans la fenêtre **Ajouter/Supprimer un snap-in**, cliquez sur **Ajouter**.

6 Dans la fenêtre **Snap-in autonome**, sélectionnez **Certificats** et cliquez sur **Ajouter**.

7 Sélectionnez le **compte Ordinateur** et cliquez sur **Suivant**.

8 Sélectionnez **Ordinateur local** et cliquez sur **Terminer**.

9 Cliquez sur **OK**.

10 Dans la fenêtre **Console 1**, développez le dossier **Certificats**, puis le dossier **Personnel** et cliquez sur le dossier **Certificats**.

11 Repérez et cliquez-droite sur le certificat d'autorité de certification racine, sélectionnez **Toutes les tâches** et cliquez sur **Exporter...**

12 Dans l'**Assistant Exportation de certificat**, cliquez sur **Suivant** et sélectionnez **Ne pas exporter la clé privée**.

13 Cliquez sur **Suivant** et sélectionnez **Codé en base 64 X.509 (.cer)** comme format.

14 Cliquez sur **Suivant** et enregistrez le certificat dans un répertoire de votre système.

15 Téléversez le certificat que vous avez enregistré dans l'étape 14 vers iDRAC.

Pour téléverser le certificat à l'aide de la RACADM, voir « Configuration de Microsoft Active Directory avec le schéma étendu avec l'interface Web iDRAC6 », à la page 173 ou « Configuration de Microsoft Active Directory avec le schéma standard à l'aide de la RACADM », à la page 185.

Pour téléverser le certificat à l'aide de l'interface Web, voir « Configuration de Microsoft Active Directory avec le schéma étendu avec l'interface Web iDRAC6 », à la page 173 ou « Configuration de Microsoft Active Directory avec le schéma standard avec l'interface Web iDRAC6 », à la page 181.

## Importation du certificat SSL du micrologiciel iDRAC6

**REMARQUE :** si le serveur Active Directory est défini pour authentifier le client lors de la phase d'initialisation d'une session SSL, vous devez également téléverser le certificat du serveur iDRAC6 vers le contrôleur de domaine Active Directory. Cette étape supplémentaire n'est pas nécessaire si Active Directory ne procède pas à l'authentification du client lors de la phase d'initialisation d'une session SSL.

Utilisez la procédure suivante pour importer le certificat SSL du micrologiciel iDRAC6 dans toutes les listes de certificats de confiance de contrôleur de domaine.

**REMARQUE :** Si votre système exécute Windows 2000, les étapes suivantes peuvent varier.

**REMARQUE :** si le certificat SSL du micrologiciel iDRAC6 est signé par une AC connue et si le certificat de cette AC est déjà dans la liste des autorités de certification racine de confiance du contrôleur de domaine, vous n'avez pas besoin d'effectuer les étapes décrites dans cette section.

Le certificat SSL iDRAC6 est le même que celui utilisé pour le serveur Web iDRAC6. Tous les contrôleurs iDRAC sont livrés avec un certificat auto-signé par défaut.

Pour télécharger le certificat SSL iDRAC6, exécutez la commande RACADM suivante :

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

1. Sur le contrôleur de domaine, ouvrez une fenêtre **Console MMC** et sélectionnez **Certificats→ Autorités de certification racines de confiance**.
2. Cliquez avec le bouton droit de la souris sur **Certificats**, sélectionnez **Toutes les tâches** et cliquez sur **Importer**.
3. Cliquez sur **Suivant** et naviguez vers le fichier de certificat SSL.
4. Installez le certificat SSL iDRAC6 dans l'**Autorité de certification racine de confiance** de chaque contrôleur de domaine.

   Si vous avez installé votre propre certificat, assurez-vous que l'AC qui signe votre certificat est dans la liste des **autorités de certification racines de confiance**. Si elle ne l'est pas, vous devez l'installer sur tous vos contrôleurs de domaine.
5. Cliquez sur **Suivant** et choisissez si vous voulez que Windows sélectionne automatiquement le magasin de certificats en fonction du type de certificat ou naviguez vers un magasin de votre choix.
6. Cliquez sur **Terminer,** puis sur **OK**.

# Mécanismes d'authentification Active Directory pris en charge

Vous pouvez utiliser Active Directory pour définir l'accès utilisateur sur iDRAC6 au moyen de deux méthodes : vous pouvez utiliser la solution de *schéma étendu* que Dell a personnalisée pour y ajouter des objets Active Directory définis par Dell. Ou vous pouvez utiliser la solution de *schéma standard* qui utilise uniquement les objets du groupe Active Directory. Consultez les sections suivantes pour plus d'informations sur ces solutions.

Lorsque vous utilisez Active Directory pour configurer l'accès à iDRAC6, vous devez choisir la solution de schéma étendu ou schéma standard.

La solution de schéma étendu présente les avantages suivants :

- Tous les objets de contrôle d'accès sont maintenus dans Active Directory.
- La configuration de l'accès utilisateur sur différents iDRAC6 dont les niveaux de privilèges diffèrent est assurée.

La solution de schéma standard comporte l'avantage suivant : aucune extension de schéma n'est requise, car toutes les classes d'objets nécessaires sont fournies par la configuration par défaut de Microsoft du schéma Active Directory.

# Présentation d'Active Directory avec le schéma étendu

L'utilisation de la solution de schéma étendu nécessite l'extension de schéma Active Directory, comme indiqué dans la section suivante.

## 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 stockée dans la base de données. Quelques exemples d'attributs de la classe utilisateur peuvent être le prénom de l'utilisateur, son nom de famille, son numéro de téléphone, etc. Les sociétés peuvent étendre la base de données d'Active Directory en y ajoutant leurs propres attributs et classes pour répondre aux besoins de leur environnement. 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 que les références soient uniques dans toute l'industrie, Microsoft maintient une base de données d'identifiants d'objets (OID) Active Directory de sorte que lorsque des sociétés ajoutent des extensions au schéma, elles sont sûres que ces extensions sont uniques et ne créent pas de conflits entre elles. Pour étendre le schéma dans Microsoft Active Directory, Dell a reçu des OID uniques, des extensions de noms uniques et des références d'attributs liées de manière unique pour les attributs et les classes ajoutés au service de répertoire.

Extension de Dell : dell

OID de base de Dell : 1.2.840.113556.1.8000.1280

Plage des ID de liens du RAC :12070 to 12079

## Présentation des extensions de schéma d'iDRAC

Pour offrir la plus grande flexibilité face à la multitude des environnements clients, Dell fournit un groupe de propriétés qui peut être configuré par l'utilisateur en fonction des résultats souhaités. Dell a étendu le schéma pour inclure les propriétés Association, Périphérique et Privilège. La propriété Association est utilisée pour associer les utilisateurs ou les groupes à un ensemble spécifique de privilèges pour un ou plusieurs périphériques iDRAC. Ce modèle offre à l'administrateur un maximum de flexibilité sur les différentes combinaisons d'utilisateurs, de privilèges iDRAC et de périphériques iDRAC sur le réseau, sans ajouter trop de complexité.

## Présentation des objets Active Directory

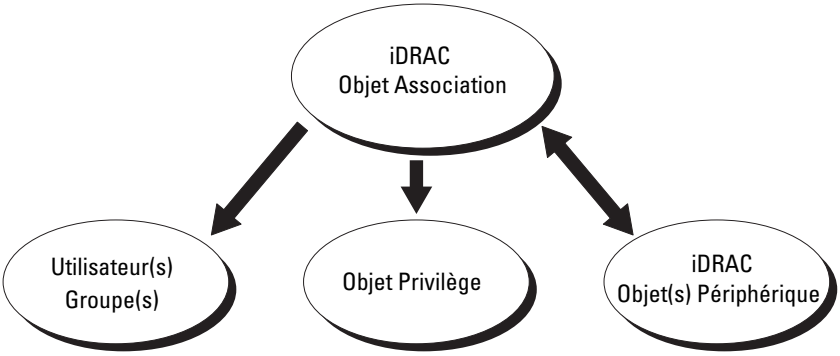
Pour chacun des iDRAC physiques présents sur le réseau que vous voulez intégrer à Active Directory en vue de l'authentification et de l'autorisation, créez au moins un objet Association et un objet Périphérique iDRAC. Vous pouvez créer plusieurs objets Association et chaque objet Association peut être lié à autant d'utilisateurs, de groupes d'utilisateurs ou d'objets Périphérique iDRAC que nécessaire. Les utilisateurs et les groupes d'utilisateurs iDRAC 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 iDRAC) qu'à un seul objet Privilège. Cet exemple permet à un administrateur de contrôler les privilèges de chaque utilisateur sur des iDRAC spécifiques.

L'objet Périphérique iDRAC est le lien vers le micrologiciel iDRAC pour demander à Active Directory d'effectuer une authentification et une autorisation. Lorsqu'un iDRAC est ajouté au réseau, l'administrateur doit configurer l'iDRAC et son objet 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 l'iDRAC à au moins un objet Association pour que les utilisateurs puissent s'authentifier.

La Figure 7-1 illustre le fait que l'objet Association fournit la connexion nécessaire pour toute authentification et autorisation.

**Figure 7-1. Configuration type pour les objets Active Directory**



Vous pouvez créer autant d'objets Association que vous le souhaitez. Cependant, vous devez créer au moins un objet Association et vous devez avoir un objet Périphérique iDRAC pour chaque iDRAC du réseau que vous voulez intégrer à Active Directory pour effectuer l'authentification et l'autorisation avec l'iDRAC.

L'objet Association inclut autant d'utilisateurs et/ou de groupes que d'objets Périphérique iDRAC. 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 iDRAC.

L'extension Dell sur le snap-in Utilisateurs et ordinateurs Active Directory de la MMC permet seulement l'association de l'objet Privilège et des objets iDRAC du même domaine avec l'objet Association. L'extension Dell ne permet pas l'ajout d'un groupe ou d'un objet iDRAC d'autres domaines en tant que membre produit de l'objet Association.

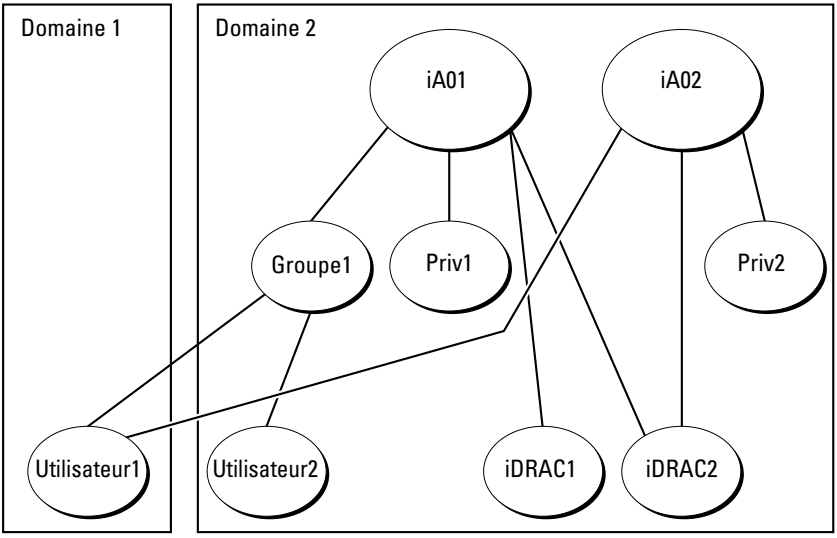
Les utilisateurs, groupes d'utilisateurs ou groupes d'utilisateurs imbriqués depuis tout domaine peuvent être ajoutés dans l'objet Association. Les solutions de schéma étendu prennent en charge tout type de groupe d'utilisateurs et toute imbrication de groupes d'utilisateurs à travers plusieurs domaines autorisés par Microsoft Active Directory.

### Accumulation de privilèges à l'aide du schéma étendu

Le mécanisme d'authentification du schéma étendu prend en charge l'accumulation de privilèges depuis différents objets Privilège associés au même utilisateur via différents objets Association. En d'autres termes, l'authentification du schéma étendu accumule les privilèges pour accorder à l'utilisateur le super ensemble de tous les privilèges attribués correspondant aux différents objets Privilège associés au même utilisateur.

La Figure 7-2 fournit un exemple d'accumulation de privilèges à l'aide du schéma étendu.

**Figure 7-2. Accumulation de privilèges pour un utilisateur**




La figure montre deux objets Association : iA01 et iA02. Utilisateur1 est associé à iDRAC2 via les deux objets Association. Par conséquent, Utilisateur1 a accumulé des privilèges résultant de l'association de l'ensemble des privilèges pour les objets Priv1 et Priv2 sur iDRAC2.

Par exemple, Priv1 possède les privilèges Ouvrir une session, Média virtuel et Effacer les journaux, et Privr2 a les privilèges Ouvrir une session sur iDRAC, Configurer iDRAC et Alertes test. Par conséquent, Utilisateur1 a maintenant l'ensemble des privilèges (Ouvrir une session sur iDRAC, Média virtuel, Effacer les journaux, Configurer iDRAC et Alertes test) qui correspond à l'ensemble de privilèges associé de Priv1 et Priv2.

L'authentification du schéma étendu accumule les privilèges pour accorder à l'utilisateur l'ensemble maximal de privilèges possibles, en tenant compte des privilèges attribués des différents objets Privilège associés au même utilisateur.

Dans cette configuration, Utilisateur1 possède les privilèges Priv1 et Priv2 sur iDRAC2. Utilisateur1 possède seulement les privilèges Priv1 sur iDRAC1. Utilisateur2 possède les privilèges Priv1 sur iDRAC1 et iDRAC2. En outre, cette figure illustre que Utilisateur1 peut être dans un domaine différent et être associé par un groupe imbriqué.

# Configuration du schéma étendu d'Active Directory pour accéder à votre iDRAC6

Pour pouvoir utiliser Active Directory pour accéder à votre iDRAC6, configurez le logiciel Active Directory et iDRAC6 en effectuant les étapes suivantes :

1. Développez le schéma Active Directory (consultez « Extension du schéma Active Directory », à la page 162).
2. Développez le snap-in Utilisateurs et ordinateurs Active Directory (voir « Installation de l'extension Dell sur le snap-in Utilisateurs et ordinateurs Microsoft Active Directory », à la page 169).
3. Ajoutez des utilisateurs iDRAC6 et leurs privilèges à Active Directory (voir « Ajout d'utilisateurs iDRAC et de leurs privilèges à Microsoft Active Directory », à la page 170).
4. Configurez les propriétés Active Directory d'iDRAC6 via l'interface Web iDRAC6 ou la RACADM (voir « Configuration de Microsoft Active Directory avec le schéma étendu avec l'interface Web iDRAC6 », à la page 173 ou « Configuration de Microsoft Active Directory avec le schéma étendu avec la RACADM », à la page 176).

## Extension du schéma Active Directory

**Important :** l'extension de schéma de ce produit diffère de celle des générations précédentes des produits de gestion à distance de Dell. Vous devez étendre le nouveau schéma et installer le nouveau snap-in Utilisateurs et ordinateurs Active Directory de la console MMC (Microsoft Management Console) dans votre répertoire. L'ancien schéma n'est pas compatible avec ce produit.

**REMARQUE :** l'extension du nouveau schéma ou l'installation de la nouvelle extension sur le snap-in Utilisateurs et ordinateurs Active Directory n'a aucun impact sur les produits précédents.

L'extension de schéma et l'extension snap-in MMC Utilisateurs et ordinateurs Active Directory sont disponibles sur le DVD *Dell Systems Management Tools and Documentation*. Pour plus d'informations sur l'installation de ces dernières, consultez « Installation de l'extension Dell sur le snap-in Utilisateurs et ordinateurs Microsoft Active Directory », à la page 169. Pour plus de détails sur l'extension du schéma pour iDRAC6 et l'installation du snap-in MMC Utilisateurs et ordinateurs Active Directory, consultez le *Guide d'utilisation Installation et Sécurité de Dell OpenManage* disponible à l'adresse **dell.com/support/manuals**.

**REMARQUE :** lorsque vous créez des objets Association iDRAC ou des objets Périphérique iDRAC, assurez-vous de sélectionner **Objet avancé Gestion à distance Dell**.

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 Administrateur de schéma pour le propriétaire de rôle FSMO (Flexible Single Master Operation) de maître de schéma de la forêt de domaine.

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

- l'utilitaire Dell Schema Extender ;
- 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 se trouvent sur votre DVD *Dell Systems Management Tools and Documentation* dans les répertoires respectifs suivants :

- *Lecteur de DVD* :**\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files**
- **<Lecteur de *DVD*> :\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\Schema_Extender**

**REMARQUE :** le dossier **Remote_Management** est dédié à l'extension du schéma sur les produits d'accès à distance antérieurs tels que DRAC 4 et DRAC 5, tandis que le dossier **Remote_Management_Advanced** est dédié à l'extension du schéma sur iDRAC6.

Pour utiliser les fichiers LDIF, consultez les instructions du fichier « Lisez-moi » qui se trouve dans le répertoire **LDIF_Files**. Pour utiliser l'utilitaire Dell Schema Extender pour étendre le schéma Active Directory, voir « Utilisation de Dell Schema Extender », à la page 164.

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

### Utilisation de Dell Schema Extender

**REMARQUE :** L'utilitaire Dell Schema Extender utilise le fichier SchemaExtenderOem.ini. Pour que l'utilitaire Dell Schema Extender fonctionne correctement, ne modifiez 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 MMC et le snap-in du schéma Active Directory pour vérifier ce qui suit :

   - Classes (consultez Tableau 7-2 à Tableau 7-7)
   - Attributs (Tableau 7-8)

Consultez votre documentation Microsoft pour des détails sur l'utilisation de la MMC et du snap-in du schéma Active Directory.

**Tableau 7-2. Définitions de classe pour les classes ajoutées au schéma Active Directory**

| Nom de classe | Numéro d'identification d'objet (OID) attribué |
|---|---|
| delliDRACDevice | 1.2.840.113556.1.8000.1280.1.7.1.1 |
| delliDRACAssociation | 1.2.840.113556.1.8000.1280.1.7.1.2 |
| dellRAC4Privileges | 1.2.840.113556.1.8000.1280.1.1.1.3 |
| dellPrivileges | 1.2.840.113556.1.8000.1280.1.1.1.4 |
| dellProduct | 1.2.840.113556.1.8000.1280.1.1.1.5 |

**Tableau 7-3. Classe dellRacDevice**

| OID | 1.2.840.113556.1.8000.1280.1.7.1.1 |
|---|---|
| Description | Représente le périphérique iDRAC de Dell. Le périphérique iDRAC doit être configuré comme dellRacDevice dans Active Directory. Cette configuration permet à iDRAC d'envoyer des requêtes LDAP (Lightweight Directory Access Protocol) à Active Directory. |
| Type de classe | Classe structurelle |
| SuperClasses | dellProduct |
| Attributs | dellSchemaVersion<br>dellRacType |

**Tableau 7-4. Classe delliDRACAssociationObject**

| OID | 1.2.840.113556.1.8000.1280.1.7.1.2 |
|---|---|
| Description | Représente l'objet Association de Dell. L'objet Association fournit la connexion entre les utilisateurs et les périphériques. |
| Type de classe | Classe structurelle |
| SuperClasses | Groupe |
| Attributs | **dellProductMembers**<br>**dellPrivilegeMember** |

**Tableau 7-5. Classe dellRAC4Privileges**

| OID | 1.2.840.113556.1.8000.1280.1.1.1.3 |
|---|---|
| Description | Permet de définir les privilèges (droits d'autorisation) du périphérique iDRAC. |
| Type de classe | Classe auxiliaire |
| SuperClasses | None (Aucune) |

**Tableau 7-5. Classe dellRAC4Privileges *(suite)***

| OID | 1.2.840.113556.1.8000.1280.1.1.1.3 |
|---|---|
| Attributs | **dellIsLoginUser** |
| | **dellIsCardConfigAdmin** |
| | **dellIsUserConfigAdmin** |
| | **dellIsLogClearAdmin** |
| | **dellIsServerResetUser** |
| | **dellIsConsoleRedirectUser** |
| | **dellIsVirtualMediaUser** |
| | **dellIsTestAlertUser** |
| | **dellIsDebugCommandAdmin** |

**Tableau 7-6. Classe dellPrivileges**

| OID | 1.2.840.113556.1.8000.1280.1.1.1.4 |
|---|---|
| Description | Fait office de classe de conteneurs pour les privilèges Dell (droits d'autorisation). |
| Type de classe | Classe structurelle |
| SuperClasses | User (Utilisateur) |
| Attributs | **dellRAC4Privileges** |

**Tableau 7-7. 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 7-8. Liste des attributs ajoutés au schéma Active Directory**

| Nom/Description de l'attribut | OID attribué/Identifiant d'objet de syntaxe | Valeur unique |
|---|---|---|
| **dellPrivilegeMember**<br>Liste des objets dellPrivilege qui appartiennent à cet attribut. | 1.2.840.113556.1.8000.1280.1.1.2.1<br>Nom distingué (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12) | FALSE |
| **dellProductMembers**<br>Liste des objets dellRacDevice et DelliDRACDevice qui appartiennent à ce rôle. Cet attribut est le lien vers l'avant vers le lien vers l'arrière dellAssociationMembers.<br>Numéro de lien : 12070 | 1.2.840.113556.1.8000.1280.1.1.2.2<br>Nom distingué (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12) | FALSE |
| **dellIsLoginUser**<br>TRUE si l'utilisateur a les droits Ouvrir une session sur le périphérique. | 1.2.840.113556.1.8000.1280.1.1.2.3<br>Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellIsCardConfigAdmin**<br>TRUE si l'utilisateur a les droits Configuration de carte sur le périphérique. | 1.2.840.113556.1.8000.1280.1.1.2.4<br>Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellIsUserConfigAdmin**<br>TRUE si l'utilisateur a les droits Configuration utilisateur sur le périphérique. | 1.2.840.113556.1.8000.1280.1.1.2.5<br>Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **delIsLogClearAdmin**<br>TRUE si l'utilisateur a les droits Effacement de journal sur le périphérique. | 1.2.840.113556.1.8000.1280.1.1.2.6<br>Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellIsServerResetUser**<br>TRUE si l'utilisateur a les droits Réinitialisation de serveur sur le périphérique. | 1.2.840.113556.1.8000.1280.1.1.2.7<br>Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |

**Tableau 7-8. Liste des attributs ajoutés au schéma Active Directory *(suite)***

| Nom/Description de l'attribut | OID attribué/Identifiant d'objet de syntaxe | Valeur unique |
|---|---|---|
| **dellIsConsoleRedirectUser**<br>TRUE si l'utilisateur a les droits Console virtuelle sur le périphérique. | 1.2.840.113556.1.8000.1280.1.1.2.8<br>Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellIsVirtualMediaUser**<br>TRUE si l'utilisateur a les droits Média virtuel sur le périphérique. | 1.2.840.113556.1.8000.1280.1.1.2.9<br>Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellIsTestAlertUser**<br>TRUE si l'utilisateur a les droits Utilisateur pour l'alerte test sur le périphérique. | 1.2.840.113556.1.8000.1280.1.1.2.10<br>Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellIsDebugCommandAdmin**<br>TRUE si l'utilisateur a les droits Administrateur pour la commande de débogage sur le périphérique. | 1.2.840.113556.1.8000.1280.1.1.2.11<br>Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7) | TRUE |
| **dellSchemaVersion**<br>La version de schéma actuelle est utilisée pour mettre à jour le schéma. | 1.2.840.113556.1.8000.1280.1.1.2.12<br>Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905) | TRUE |
| **dellRacType**<br>Cet attribut est le type de RAC actuel pour l'objet delliDRACDevice et le lien vers l'arrière vers le lien vers l'avant dellAssociationObjectMembers. | 1.2.840.113556.1.8000.1280.1.1.2.13<br>Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905) | TRUE |

**Tableau 7-8. Liste des attributs ajoutés au schéma Active Directory *(suite)***

| Nom/Description de l'attribut | OID attribué/Identifiant d'objet de syntaxe | Valeur unique |
|---|---|---|
| **dellAssociationMembers** | 1.2.840.113556.1.8000.1280.1.1.2.14 | FALSE |
| Liste des dellAssociationObjectMembers appartenant à ce produit. Cet attribut est le lien vers l'arrière vers l'attribut lié dellProductMembers.<br>ID de lien : 12071 | Nom distingué (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12) | |

## Installation de l'extension Dell sur le snap-in Utilisateurs et ordinateurs Microsoft Active Directory

Lorsque vous étendez le schéma dans Active Directory, vous devez également étendre le snap-in Utilisateurs et ordinateurs Active Directory pour que l'administrateur puisse gérer les périphériques iDRAC, les utilisateurs et les groupes d'utilisateurs, les associations iDRAC et les privilèges iDRAC.

Lorsque vous installez votre logiciel Systems Management Software à l'aide du DVD *Dell Systems Management Tools and Documentation*, vous pouvez installer le snap-in en sélectionnant l'option **Snap-in Utilisateurs et ordinateurs Active Directory** pendant la procédure d'installation. Consultez le *Guide d'installation rapide du logiciel Dell OpenManage* pour des instructions supplémentaires sur l'installation du logiciel Systems Management Software. Pour les systèmes d'exploitation Windows 64 bits, le programme d'installation du snap-in se trouve sous **<lecteur de DVD>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64**

Pour des informations supplémentaires sur le snap-in Utilisateurs et ordinateurs Active Directory, consultez votre documentation Microsoft.

### Installation du pack administrateur

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

Reportez-vous à la section « Ouverture du snap-in Utilisateurs et ordinateurs Microsoft Active Directory », à la page 170 pour en savoir plus.

#### Ouverture du snap-in Utilisateurs et ordinateurs Microsoft 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**.

   La MMC s'affiche.

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** et cliquez sur **Ajouter**.
5. Cliquez sur **Fermer**, puis sur **OK**.

### Ajout d'utilisateurs iDRAC et de leurs privilèges à Microsoft Active Directory

Le snap-in Utilisateurs et ordinateurs Active Directory étendu par Dell permet d'ajouter des utilisateurs iDRAC et des privilèges en créant des objets iDRAC, Association et Privilège. Pour ajouter chaque type d'objet, effectuez les procédures suivantes :

- Créer un objet Périphérique iDRAC
- Créer un objet Privilège
- Créer un objet Association
- Configuration d'un objet Association

#### Création d'un objet Périphérique iDRAC

1. Dans la fenêtre **Racine de la console** MMC, cliquez avec le bouton droit de la souris sur un conteneur.
2. Sélectionnez **Nouveau→ Objet avancé Gestion à distance Dell**.

   La fenêtre **Nouvel objet** s'affiche.
3. Entrez un nom pour le nouvel objet. Ce nom doit être identique au nom iDRAC que vous taperez à l'étape A de « Configuration de Microsoft Active Directory avec le schéma étendu avec l'interface Web iDRAC6 », à la page 173.
4. Sélectionnez **Objet Périphérique iDRAC**.
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 avancé Gestion à distance Dell**.

   La fenêtre **Nouvel objet** s'affiche.
3. Entrez 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 de gestion à distance** et sélectionnez les privilèges que vous souhaitez donner à l'utilisateur.

#### Création d'un objet Association

**REMARQUE :** l'objet Association iDRAC provient d'un groupe et sa portée est définie sur Domaine local.

1. Dans la fenêtre **Racine de la console** (MMC), cliquez avec le bouton droit de la souris sur un conteneur.

2 Sélectionnez **Nouveau→ Objet avancé Gestion à distance Dell**.

Cette action ouvre la fenêtre **Nouvel objet**.

3 Entrez un nom pour le nouvel objet.

4 Sélectionnez **Objet Association**.

5 Cliquez sur **OK**.

#### Configuration d'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 iDRAC.

Vous pouvez ajouter des groupes d'utilisateurs. 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 Entrez 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 iDRAC. 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 Entrez le nom de l'objet Privilège et cliquez sur **OK**.

Cliquez sur l'onglet **Produits** pour ajouter un périphérique iDRAC connecté au réseau qui est disponible pour les utilisateurs ou groupes d'utilisateurs définis. Vous pouvez ajouter plusieurs périphériques iDRAC à un objet Association.

#### Ajout de périphériques iDRAC

Pour ajouter des périphériques iDRAC :

1. Sélectionnez l'onglet **Produits** et cliquez sur **Ajouter**.
2. Tapez le nom du périphérique iDRAC et cliquez sur **OK**.
3. Dans la fenêtre **Propriétés**, cliquez sur **Appliquer**, puis sur **OK**.

### Configuration de Microsoft Active Directory avec le schéma étendu avec l'interface Web iDRAC6

1. Ouvrez une fenêtre d'un navigateur Web pris en charge.
2. Ouvrez une session sur l'interface Web iDRAC6.
3. Accédez à **Paramètres iDRAC**→ onglet **Réseau/Sécurité**→ onglet **Service de répertoire**→ **Microsoft Active Directory**.
4. Allez à la fin de la page **Configuration et gestion d'Active Directory** et cliquez sur **Configurer Active Directory**.

   La page **Configuration et gestion d'Active Directory Étape 1/4** s'affiche.
5. Sous **Paramètres du certificat**, cochez **Activer la validation de certificats** si vous voulez valider le certificat SSL de vos serveurs Active Directory ; sinon, passez à l'étape 9.
6. Sous **Téléverser le certificat d'autorité de certification d'Active Directory**, tapez le chemin de fichier du certificat ou naviguez pour trouver le fichier du certificat.

   **REMARQUE :** vous devez taper le chemin de fichier absolu, y compris le chemin et le nom de fichier complets et l'extension du fichier.
7. Cliquez sur **Téléverser**.

   Les informations concernant le certificat d'autorité de certification d'Active Directory que vous avez téléversé apparaissent.
8. **(Facultatif : pour l'authentification Active Directory uniquement)** Sous **Téléverser le fichier Keytab Kerberos**, tapez le chemin du fichier keytab ou naviguez pour accéder au fichier. Cliquez sur **Téléverser**. Le fichier keytab Kerberos est téléversé vers iDRAC6.
9. Cliquez sur **Suivant**. La page **Configuration et gestion d'Active Directory Étape 2/4** s'affiche.
10. Sélectionnez **Activer Active Directory**.

**PRÉCAUTION : Dans cette version, la fonctionnalité Authentification bifactorielle (TFA) articulée autour de la carte à puce n'est pas prise en charge si Active Directory est configuré pour le schéma étendu. La fonctionnalité Connexion directe (SSO) est prise en charge par le schéma standard et le schéma étendu.**

11 Cliquez sur **Ajouter** pour saisir le nom de domaine utilisateur.

12 Tapez le nom de domaine utilisateur dans l'invite, puis cliquez sur **OK**.

**REMARQUE :** cette étape est optionnelle. Si vous configurez une liste de domaines utilisateur, la liste sera disponible dans l'écran d'ouverture de session de l'interface Web. Vous pouvez choisir dans la liste, puis vous devez seulement taper le nom d'utilisateur.

13 Dans le champ **Délai d'attente**, tapez la durée (en secondes) qui doit s'écouler avant qu'iDRAC puisse recevoir les réponses émanant d'Active Directory. La valeur par défaut est 120 secondes.

14 Sélectionnez l'une des options suivantes :

a Sélectionnez l'option **Rechercher les contrôleurs de domaine avec DNS** pour obtenir les contrôleurs de domaine Active Directory émanant d'une recherche DNS. Les adresses 1 à 3 du serveur de contrôleur de domaine sont ignorées. Sélectionnez **Domaine utilisateur de l'ouverture de session** pour effectuer la recherche DNS avec le nom de domaine de l'utilisateur d'ouverture de session. Vous pouvez également sélectionner **Spécifier un domaine** et saisir le nom de domaine à utiliser dans le cadre de la recherche DNS. iDRAC6 tente de se connecter à chacune des adresses (les 4 premières adresses renvoyées par la recherche DNS) l'une après l'autre jusqu'à ce qu'une connexion soit établie. Si **Schéma étendu** est sélectionné, les contrôleurs de domaine sont ceux où se trouvent l'objet Périphérique iDRAC6 et les objets Association.

b Sélectionnez l'option **Spécifier les adresses du contrôleur de domaine** pour permettre à iDRAC6 d'utiliser les adresses du serveur de contrôleur de domaine Active Directory spécifiées. La recherche DNS n'est pas effectuée. Spécifiez l'adresse IP?ou le nom de domaine pleinement qualifié (FQDN) des contrôleurs de domaine. Lorsque l'option **Spécifier les adresses du contrôleur de domaine** est sélectionnée, au moins l'une des trois adresses doit être configurée. iDRAC6 tente de se connecter à chacune des adresses configurées une par une jusqu'à ce qu'une connexion soit établie. Si **Schéma étendu**

est sélectionné, il s'agit des adresses des contrôleurs de domaine où se trouvent l'objet Périphérique iDRAC6 et les objets Association.

**REMARQUE :** le FQDN ou l'adresse IP que vous spécifiez dans le champ **Adresse du serveur de contrôleur de domaine** doit correspondre au champ Objet ou Autre nom de l'objet de votre certificat de contrôleur de domaine si la validation de certificat est activée.

15 Cliquez sur **Suivant**. La page **Configuration et gestion d'Active Directory Étape 3/4** s'affiche.

16 Sous **Sélection du schéma**, sélectionnez **Schéma étendu**.

17 Cliquez sur **Suivant**. La page **Configuration et gestion d'Active Directory Étape 4/4** s'affiche.

18 Sous **Paramètres du schéma étendu**, tapez le **nom iDRAC** et le **nom de domaine iDRAC** pour configurer l'objet Périphérique iDRAC. Le nom de domaine d'iDRAC est le domaine dans lequel l'objet?iDRAC est créé.

19 Cliquez sur **Terminer** pour enregistrer les paramètres du schéma étendu d'Active Directory.

Le serveur Web iDRAC6 vous renvoie automatiquement à la page **Configuration et gestion d'Active Directory**.

20 Cliquez sur **Paramètres de test** pour vérifier les paramètres du schéma étendu d'Active Directory.

21 Tapez votre nom d'utilisateur et votre mot de passe Active?Directory.

Les résultats du test et le journal du test sont affichés. Pour de plus amples informations, reportez-vous à la section « Test de vos configurations », à la page 189.

**REMARQUE :** vous devez posséder un serveur DNS correctement configuré sur iDRAC pour prendre en charge l'ouverture de session Active Directory. Cliquez sur **Paramètres iDRAC→ Réseau/Sécurité→** page **Réseau** pour configurer manuellement le(s) serveur(s) DNS ou utiliser DHCP pour obtenir le(s) serveur(s) DNS.

Vous avez terminé la configuration d'Active Directory avec le schéma étendu.

### Configuration de Microsoft Active Directory avec le schéma étendu avec la RACADM

Utilisez les commandes suivantes pour configurer la fonctionnalité Microsoft Active Directory iDRAC6 avec le schéma étendu à l'aide de l'outil CLI RACADM plutôt que l'interface Web.

1 Ouvrez une invite de commande et tapez les commandes RACADM suivantes :

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

racadm config -g cfgActiveDirectory -o cfgADType 1

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

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

racadm config -g cfgActiveDirectory -o
cfgADDomainController1 <nom de domaine pleinement
qualifié ou adresse IP du contrôleur de domaine>

racadm config -g cfgActiveDirectory -o
cfgADDomainController2 <nom de domaine pleinement
qualifié ou adresse IP du contrôleur de domaine>

racadm config -g cfgActiveDirectory -o
cfgADDomainController3 <nom de domaine pleinement
qualifié ou adresse IP du contrôleur de domaine>
```

**REMARQUE :** au moins l'une des 3 adresses doit être configurée. iDRAC tente de se connecter à chacune des adresses configurées une par une jusqu'à ce qu'une connexion soit établie. Lorsque l'option Schéma étendu est sélectionnée, ces adresses sont les FQDN ou les adresses IP des contrôleurs de domaine où se trouve ce périphérique iDRAC. En mode schéma étendu, les serveurs de catalogue global ne sont pas du tout utilisés.

**REMARQUE :** le FQDN ou l'adresse IP que vous spécifiez dans ce champ doit correspondre au champ Objet ou Autre nom de l'objet de votre certificat du contrôleur de domaine si la validation de certificat est activée.

**PRÉCAUTION : Dans cette version, la fonctionnalité Authentification bifactorielle (TFA) articulée autour de la carte à puce n'est pas prise en charge si Active Directory est configuré pour le schéma étendu. La fonctionnalité Connexion directe (SSO) est prise en charge par le schéma standard et le schéma étendu.**

Si vous souhaitez utiliser la recherche DNS pour obtenir l'adresse du serveur de contrôleur de domaine Active Directory, tapez la commande suivante :

```
racadm config -g cfgActiveDirectory -o
cfgADDcSRVLookupEnable=1
```

- Pour effectuer la recherche DNS avec le nom de domaine de l'utilisateur d'ouverture de session :

  ```
  racadm config -g cfgActiveDirectory -o
  cfgADDcSRVLookupbyUserdomain=1
  ```

- Pour spécifier le nom de domaine à utiliser dans le cadre de la recherche DNS :

  ```
  racadm config -g cfgActiveDirectory -o
  cfgADDcSRVLookupDomainName <nom de domaine à
  utiliser dans le cadre de la recherche DNS>
  ```

Pour désactiver la validation de certificat durant l'établissement de liaisons SSL, tapez la commande RACADM suivante :

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

Dans ce cas, il n'est pas nécessaire de téléverser un certificat d'autorité de certification.

Pour faire appliquer la validation de certificat durant l'établissement de liaisons SSL, tapez la commande RACADM suivante :

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

Dans ce cas, vous devez téléverser un certificat d'autorité de certification en utilisant la commande RACADM suivante :

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

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

L'utilisation de la commande RACADM suivante peut être facultative. Pour plus d'informations, voir « Importation du certificat SSL du micrologiciel iDRAC6 », à la page 155.

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

2 Si vous souhaitez spécifier la durée, en secondes, devant s'écouler pour permettre aux requêtes Active Directory (AD) de se terminer avant l'expiration du délai, tapez la commande suivante :

```
racadm config -g cfgActiveDirectory -o
cfgADAuthTimeout <durée en secondes>
```

3 Si DHCP est activé sur iDRAC et que vous voulez utiliser le DNS fourni par le serveur DHCP, tapez la commande RACADM suivante :

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

4 Si DHCP est désactivé sur iDRAC ou si vous voulez entrer manuellement votre adresse IP DNS, tapez les commandes RACADM 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>
```

5 Si vous voulez configurer une liste de domaines utilisateur afin que vous ayez seulement besoin de saisir le nom d'utilisateur durant l'ouverture de session sur l'interface Web iDRAC6, tapez la commande suivante :

```
racadm config -g cfgUserDomain -o
cfgUserDomainName -i <index>
```

Vous pouvez configurer jusqu'à 40 domaines utilisateur avec des numéros d'index compris entre 1 et 40.

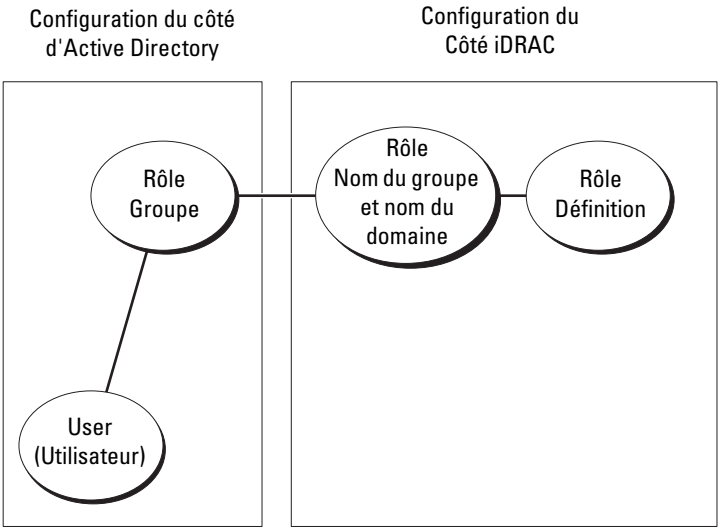
Consultez la section « Service de répertoire LDAP générique », à la page 190 pour obtenir des détails sur les domaines utilisateur.

6 Appuyez sur **Entrée** pour terminer la configuration d'Active Directory avec le schéma étendu.

# Présentation d'Active Directory avec le schéma standard

Comme illustré dans Figure 7-3, l'utilisation du schéma standard pour l'intégration d'Active Directory nécessite une configuration sur Active Directory et sur l'iDRAC6.

**Figure 7-3. Configuration d'iDRAC avec Microsoft Active Directory et le schéma standard**



Du côté d'Active Directory, un objet Groupe standard est utilisé comme groupe de rôles. Un utilisateur ayant accès à iDRAC6 sera membre du groupe de rôles. Pour octroyer à cet utilisateur l'accès à un iDRAC6 spécifique, le nom du groupe de rôles et son nom de domaine doivent être configurés sur cet iDRAC6. Contrairement à la solution du schéma étendu, le rôle et le niveau de privilège sont définis sur chaque iDRAC6, et non pas dans Active Directory. Vous pouvez configurer et définir un maximum de cinq groupes de rôles sur chaque iDRAC. Tableau 7-9 affiche les privilèges par défaut des groupes de rôles.

**REMARQUE :** le niveau des privilèges par défaut des groupes de rôles pour les cinq groupes de rôles est **Aucun**. Vous devez choisir un des privilèges par défaut des groupes de rôles dans le menu déroulant.

**Tableau 7-9. Privilèges par défaut des groupes de rôles**

| Niveau des privilèges | Droits accordés | Masque binaire |
|---|---|---|
| Administrateur | Ouvrir une session iDRAC, Configurer iDRAC, Configurer les utilisateurs, Effacer les journaux, Exécuter des commandes de contrôle du serveur, Accéder à la console virtuelle, Accès au média virtuel, Tester les alertes, Exécution des commandes de diagnostic | 0x000001ff |
| Opérateur | Ouvrir une session iDRAC, Configurer iDRAC, Exécuter des commandes de contrôle du serveur, Accéder à la console virtuelle, Accès au média virtuel, Tester les alertes, Exécution des commandes de diagnostic | 0x000000f9 |
| Lecture uniquement | Ouvrir une session sur iDRAC | 0x00000001 |
| None (Aucune) | Aucun droit attribué | 0x00000000 |

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

### Scénario à domaine unique et scénario à plusieurs domaines

Si tous les utilisateurs d'ouverture de session et groupes de rôles ainsi que les groupes imbriqués se trouvent dans le même domaine, seules les adresses des contrôleurs de domaine doivent être configurées sur iDRAC6. Dans ce scénario à domaine unique, tous les types de groupes sont pris en charge.

Si tous les utilisateurs d'ouverture de session et groupes de rôles, ou l'un des groupes imbriqués, proviennent de domaines multiples, les adresses du serveur de catalogue global doivent être configurées sur iDRAC6. Dans ce scénario à plusieurs domaines, tous les groupes de rôles et groupes imbriqués, le cas échéant, doivent être du type Groupe universel.

## Configuration du schéma standard de Microsoft Active Directory pour accéder à iDRAC6

Vous devez effectuer les étapes suivantes pour configurer Active Directory pour qu'un utilisateur Active Directory puisse accéder à iDRAC6 :

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. Ajoutez l'utilisateur Active Directory comme membre du groupe Active Directory pour avoir accès à iDRAC6.
3. Configurez le nom du groupe et le nom de domaine sur iDRAC6 via l'interface Web ou la RACADM. Pour en savoir plus, voir « Configuration de Microsoft Active Directory avec le schéma standard avec l'interface Web iDRAC6 », à la page 181 ou « Configuration de Microsoft Active Directory avec le schéma standard à l'aide de la RACADM », à la page 185.

### Configuration de Microsoft Active Directory avec le schéma standard avec l'interface Web iDRAC6

1. Ouvrez une fenêtre d'un navigateur Web pris en charge.
2. Ouvrez une session sur l'interface Web iDRAC6.
3. Accédez à **Paramètres iDRAC**→ onglet **Réseau/Sécurité**→ onglet **Service de répertoire**→ **Microsoft Active Directory**.

4 Allez à la fin de la page **Configuration et gestion d'Active Directory** et cliquez sur **Configurer Active Directory**.

La page **Configuration et gestion d'Active Directory Étape 1/4** s'affiche.

5 Sous **Paramètres du certificat**, cochez la case **Activer la validation de certificats** si vous voulez valider le certificat SSL de vos serveurs Active Directory ; sinon, passez à l'étape 9.

6 Sous **Téléverser le certificat d'autorité de certification**, parcourez le menu pour trouver le fichier de certification.

7 Cliquez sur **Téléverser**.

Les informations concernant le certificat d'autorité de certification d'Active Directory valide s'affichent.

8 **(Facultatif : pour l'authentification Active Directory uniquement)** Sous **Téléverser le fichier Keytab Kerberos**, tapez le chemin du fichier keytab ou naviguez pour accéder au fichier. Cliquez sur **Téléverser**. Le fichier keytab Kerberos est téléversé vers iDRAC6.

9 Cliquez sur **Suivant**. La page **Configuration et gestion d'Active Directory Étape 2/4** s'affiche.

10 Sélectionnez **Activer Active Directory**.

11 Sélectionnez **Activer la connexion directe** si vous souhaitez ouvrir une session sur iDRAC6 sans saisir vos références d'authentification utilisateur de domaine, par exemple le nom d'utilisateur et le mot de passe.

12 Cliquez sur **Ajouter** pour saisir le nom de domaine utilisateur.

13 Tapez le nom de domaine utilisateur dans l'invite, puis cliquez sur **OK**.

14 Dans les champs **Délai d'attente**, tapez la durée (en secondes) qui doit s'écouler avant qu'iDRAC puisse recevoir les réponses émanant d'Active Directory. La valeur par défaut est 120 secondes.

15 Sélectionnez l'une des options suivantes :

a Sélectionnez l'option **Rechercher les contrôleurs de domaine avec DNS** pour obtenir les contrôleurs de domaine Active Directory émanant d'une recherche DNS. Les adresses 1 à 3 du serveur de contrôleur de domaine sont ignorées. Sélectionnez **Domaine utilisateur de l'ouverture de session** pour effectuer la recherche DNS avec le nom de domaine de l'utilisateur d'ouverture de session. Vous pouvez également sélectionner **Spécifier un domaine** et saisir le nom de domaine à utiliser dans le cadre de la recherche DNS. iDRAC6 tente de se connecter à chacune des adresses (les 4 premières adresses renvoyées par la recherche DNS) l'une après l'autre jusqu'à ce qu'une connexion soit établie. Si **Schéma standard** est sélectionné, les contrôleurs de domaine sont ceux où se trouvent les comptes d'utilisateurs et les groupes de rôles.

b Sélectionnez l'option **Spécifier les adresses du contrôleur de domaine** pour permettre à iDRAC6 d'utiliser les adresses du serveur de contrôleur de domaine Active Directory spécifiées. La recherche DNS n'est pas effectuée. Spécifiez l'adresse IP?ou le nom de domaine pleinement qualifié (FQDN) des contrôleurs de domaine. Lorsque l'option **Spécifier les adresses du contrôleur de domaine** est sélectionnée, au moins l'une des trois adresses doit être configurée. iDRAC6 tente de se connecter à chacune des adresses configurées une par une jusqu'à ce qu'une connexion soit établie. Si **Schéma standard** est sélectionné, il s'agit des adresses des contrôleurs de domaine où se trouvent les comptes d'utilisateur et les groupes de rôles.

**REMARQUE :** le FQDN ou l'adresse IP que vous spécifiez dans ce champ doit correspondre au champ Objet ou Autre nom de l'objet de votre certificat du contrôleur de domaine si la validation de certificat est activée.

16 Cliquez sur **Suivant**. La page **Configuration et gestion d'Active Directory Étape 3/4** s'affiche.

17 Sous **Sélection du schéma**, sélectionnez **Schéma standard**.

18 Cliquez sur **Suivant**. La page **Configuration et gestion d'Active Directory Étape 4a/4** s'affiche.

19 Sélectionnez l'une des options suivantes :

- Sélectionnez l'option **Rechercher les serveurs de catalogue global avec DNS** et saisissez le **nom de domaine racine** à utiliser dans le cadre d'une recherche DNS pour obtenir les serveurs de catalogue global Active Directory. Les adresses 1 à 3 du serveur de catalogue global sont ignorées. iDRAC6 tente de se connecter à chacune des adresses (les 4 premières adresses renvoyées par la recherche DNS) l'une après l'autre jusqu'à ce qu'une connexion soit établie. Un serveur de catalogue global est exigé pour le schéma standard uniquement lorsque les comptes d'utilisateur et les groupes de rôles se trouvent dans des domaines différents.
- Sélectionnez l'option **Spécifier les adresses du serveur de catalogue global** et saisissez l'adresse IP ou le nom de domaine pleinement qualifié (FQDN) du ou des serveur(s) de catalogue global. La recherche DNS n'est pas effectuée. Au moins l'une des trois adresses doit être configurée. iDRAC6 tente de se connecter à chacune des adresses configurées une par une jusqu'à ce qu'une connexion soit établie. Le serveur de catalogue global est exigé pour le schéma standard uniquement lorsque les comptes d'utilisateur et les groupes de rôles se trouvent dans des domaines différents.

**REMARQUE :** le FQDN ou l'adresse IP que vous spécifiez dans le champ **Adresse du serveur de catalogue global** doit correspondre au champ Objet ou Autre nom de l'objet de votre certificat de contrôleur de domaine si la validation de certificat est activée.

**REMARQUE :** le serveur de catalogue global n'est requis que pour le schéma standard pour le cas où les comptes d'utilisateur et les groupes de rôles seraient dans des domaines différents. De plus, dans ce scénario à plusieurs domaines, seul le groupe universel peut être utilisé.

20 Sous **Groupes de rôles**, cliquez sur un **Groupe de rôles**.

La page **Configuration et gestion d'Active Directory Étape 4b/4** s'affiche.

21 Spécifiez le **Nom du groupe de rôles**.

Le **Nom du groupe de rôles** identifie le groupe des rôles d'Active Directory avec lequel l'iDRAC est associé.

22 Spécifiez **le Domaine du groupe de rôles**, qui est le domaine du groupe de rôles.

23 Spécifiez les **Privilèges du groupe de rôles** en sélectionnant le **Niveau de privilège du groupe de rôles**. Par exemple, si vous sélectionnez **Administrateur**, tous les privilèges sont sélectionnés pour ce niveau de droit.

24 Cliquez sur **Appliquer** pour enregistrer les paramètres du groupe de rôles.

Le serveur Web iDRAC6 vous renvoie automatiquement à la page **Étape 4a sur 4 Configuration et gestion d'Active Directory** où vos paramètres sont affichés.

25 Configurez des groupes de rôles supplémentaires, le cas échéant.

26 Cliquez sur **Terminer** pour revenir à la page **Configuration et gestion d'Active Directory**.

27 Cliquez sur **Paramètres de test** pour vérifier les paramètres du schéma standard d'Active Directory.

28 Tapez votre nom d'utilisateur et votre mot de passe iDRAC6.

Les résultats du test et le journal du test sont affichés. Pour de plus amples informations, reportez-vous à la section « Test de vos configurations », à la page 189.

**REMARQUE :** vous devez posséder un serveur DNS correctement configuré sur iDRAC pour prendre en charge l'ouverture de session Active Directory. Cliquez sur **Paramètres iDRAC→ Réseau/Sécurité→** page **Réseau** pour configurer manuellement le(s) serveur(s) DNS ou utiliser DHCP pour obtenir le(s) serveur(s) DNS.

Vous avez terminé la configuration d'Active Directory avec le schéma standard.

## Configuration de Microsoft Active Directory avec le schéma standard à l'aide de la RACADM

Utilisez les commandes suivantes pour configurer la fonctionnalité Active Directory iDRAC avec le schéma standard à l'aide de la CLI RACADM plutôt que l'interface Web.

1 Ouvrez une invite de commande et tapez les commandes RACADM suivantes :

```
racadm config -g cfgActiveDirectory -o
cfgADEnable 1
racadm config -g cfgActiveDirectory -o cfgADType 2
```

```
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 de masque
binaire pour
les droits utilisateur spécifiques>
```

**REMARQUE :** Pour connaître les valeurs de numéro de masque binaire, consultez le *Guide de référence de la ligne de commande RACADM pour iDRAC6 et CMC* disponible sur le site Web du support de Dell à l'adresse dell.com/support/manuals.

```
racadm config -g cfgActiveDirectory -o
cfgADDomainController1 <nom de domaine pleinement
qualifié ou adresse IP du contrôleur de domaine>
```

```
racadm config -g cfgActiveDirectory -o
cfgADDomainController2 <nom de domaine pleinement
qualifié ou adresse IP du contrôleur de domaine>
```

```
racadm config -g cfgActiveDirectory -o
cfgADDomainController3 <nom de domaine pleinement
qualifié ou adresse IP du contrôleur de domaine>
```

**REMARQUE :** le FQDN ou l'adresse IP que vous spécifiez dans ce champ doit correspondre au champ Objet ou Autre nom de l'objet de votre certificat du contrôleur de domaine si la validation de certificat est activée.

**REMARQUE :** saisissez le FQDN du contrôleur de domaine, *et non* le FQDN du domaine uniquement. Par exemple, saisissez `servername.dell.com` au lieu de `dell.com`.

**REMARQUE :** Au moins une des 3 adresses doit être configurée. iDRAC6 tente de se connecter à chacune des adresses configurées une par une jusqu'à ce qu'une connexion soit établie. Avec le schéma standard, il s'agit des adresses des contrôleurs de domaine où les comptes d'utilisateur et les groupes de rôles sont situés.

Si vous souhaitez utiliser la recherche DNS pour obtenir l'adresse du serveur de contrôleur de domaine Active Directory, tapez la commande suivante :

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

- Pour effectuer la recherche DNS avec le nom de domaine de l'utilisateur d'ouverture de session :

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

- Pour spécifier le nom de domaine à utiliser dans le cadre de la recherche DNS :

  ```
  racadm config -g cfgActiveDirectory -o
  cfgADDcSRVLookupDomainName <nom de domaine à
  utiliser dans le cadre de la recherche DNS>
  ```

Pour spécifier l'adresse du serveur de catalogue global, tapez la commande suivante :

```
racadm config -g cfgActiveDirectory -o cfgADGlobal
Catalog1 <nom de domaine pleinement qualifié ou
adresse IP du contrôleur de domaine>
racadm config -g cfgActiveDirectory -o cfgADGlobal
Catalog2 <nom de domaine pleinement qualifié ou
adresse IP du contrôleur de domaine>
racadm config -g cfgActiveDirectory -o cfgADGlobal
Catalog3 <nom de domaine pleinement qualifié ou
adresse IP du contrôleur de domaine>
```

**REMARQUE :** le serveur de catalogue global n'est requis que pour le schéma standard pour le cas où les comptes d'utilisateur et les groupes de rôles seraient dans des domaines différents. De plus, dans ce scénario à plusieurs domaines, seul le groupe universel peut être utilisé.

**REMARQUE :** le FQDN ou l'adresse IP que vous spécifiez dans ce champ doit correspondre au champ Objet ou Autre nom de l'objet de votre certificat du contrôleur de domaine si la validation de certificat est activée.

Si vous souhaitez utiliser la recherche DNS pour obtenir l'adresse du serveur de catalogue global Active Directory, tapez la commande suivante :

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

```
racadm config -g cfgActiveDirectory -o
cfgADGcRootDomain <Domain Name>
```

Pour désactiver la validation de certificat durant l'établissement de liaisons SSL, tapez la commande RACADM suivante :

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

Dans ce cas, aucun certificat d'autorité de certification (AC) ne doit être téléversé.

Pour faire appliquer la validation de certificat durant l'établissement de liaisons SSL, tapez la commande RACADM suivante :

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

Dans ce cas, vous devez également téléverser le certificat d'autorité de certification en utilisant la commande RACADM suivante :

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

L'utilisation de la commande RACADM suivante peut être facultative. Pour plus d'informations, voir « Importation du certificat SSL du micrologiciel iDRAC6 », à la page 155.

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

2 Si vous souhaitez spécifier la durée, en secondes, devant s'écouler pour permettre aux requêtes Active Directory (AD) de se terminer avant l'expiration du délai, tapez la commande suivante :

```
racadm config -g cfgActiveDirectory -o
cfgADAuthTimeout <durée en secondes>
```

3 Si DHCP est activé sur iDRAC6 et que vous voulez utiliser le DNS fourni par le serveur DHCP, tapez les commandes RACADM suivantes :

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

4 Si DHCP est désactivé sur iDRAC6 ou que vous voulez entrer manuellement votre adresse IP DNS, tapez les commandes RACADM 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>
```

5 Si vous voulez configurer une liste de domaines utilisateur afin de n'avoir à entrer que le nom d'utilisateur durant l'ouverture de session sur l'interface Web, tapez la commande suivante :

```
racadm config -g cfgUserDomain -o
cfgUserDomainName -i <index>
```

Jusqu'à 40 domaines utilisateur peuvent être configurés avec des numéros d'index allant de 1 à 40. Voir « Service de répertoire LDAP générique », à la page 190 pour des informations détaillées sur les domaines utilisateur.

# Test de vos configurations

Pour vérifier si votre configuration fonctionne ou pour établir un diagnostic de l'échec de votre ouverture de session Active Directory, vous pouvez tester vos paramètres depuis l'interface Web iDRAC6.

Une fois la configuration des paramètres terminée dans l'interface Web iDRAC6, cliquez sur **Paramètres de test** au bas de la page. Il vous sera demandé de saisir un nom d'utilisateur de test (par exemple, nom d'utilisateur@domaine.com) et un mot de passe pour exécuter le test. Selon votre configuration, l'exécution de toutes les étapes du test et l'affichage des résultats de chaque étape peuvent prendre un certain temps. Un journal de test détaillé s'affiche au bas de la page de résultats.

En cas d'échec d'une étape, examinez les détails dans le journal de test pour identifier le problème et une éventuelle solution. Pour les erreurs les plus courantes, consultez « Questions les plus fréquentes concernant Active Directory », à la page 196.

Si vous devez apporter des modifications à vos paramètres, cliquez sur l'onglet **Active Directory**, puis modifiez la configuration pas à pas.

# Service de répertoire LDAP générique

iDRAC6 fournit une solution générique visant à prendre en charge l'authentification LDAP (Lightweight Directory Access Protocol). Cette fonctionnalité ne nécessite aucune extension de schéma au sein de vos services de répertoire.

Pour rendre l'implémentation LDAP iDRAC6 générique, les points communs entre les différents services de répertoire sont utilisés pour regrouper les utilisateurs, puis mapper la relation utilisateur-groupe. Le schéma constitue l'action spécifique au service de répertoire. Par exemple, ils peuvent avoir différents noms d'attribut pour le groupe, l'utilisateur et le lien entre l'utilisateur et le groupe. Ces actions peuvent être configurées dans iDRAC6.

## Syntaxe d'ouverture de session (utilisateur de répertoire et utilisateur local)

Contrairement à Active Directory, les caractères spéciaux (« @ », « \ » et « / ») ne sont pas utilisés pour différencier un utilisateur LDAP d'un utilisateur local. L'utilisateur d'ouverture de session doit uniquement saisir le nom d'utilisateur, à l'exclusion du nom de domaine. iDRAC6 adopte le nom d'utilisateur tel quel et ne le scinde pas en nom d'utilisateur et nom de domaine. Lorsque LDAP générique est activé, iDRAC6 tente d'abord de connecter l'utilisateur en tant qu'utilisateur de répertoire. En cas d'échec, la recherche d'utilisateur local est activée.

**REMARQUE :** Aucun changement de comportement n'a lieu au niveau de la syntaxe d'ouverture de session Active Directory. Lorsque LDAP générique est activé, la page d'ouverture de session d'IUG affiche uniquement « Cet iDRAC » dans le menu déroulant.

**REMARQUE :** les caractères « < » et « > » ne sont pas autorisés dans le nom d'utilisateur pour les services de répertoire openLDAP et OpenDS.

### Configuration du service de répertoire LDAP générique avec l'interface Web iDRAC6

1. Ouvrez une fenêtre d'un navigateur Web pris en charge.
2. Ouvrez une session sur l'interface Web iDRAC6.
3. Accédez à **Paramètres iDRAC**→ onglet **Réseau/Sécurité**→ onglet **Service de répertoire**→ **Service de répertoire LDAP générique**.

   La page **Configuration et gestion de LDAP générique** affiche les paramètres LDAP générique iDRAC6 actuels. Faites défiler vers le bas de la page **Configuration et gestion de LDAP générique** et cliquez sur **Configurer LDAP générique**.

   La page **Configuration et gestion LDAP génériques Étape 1/3** s'affiche. Utilisez cette page pour configurer le certificat numérique utilisé lors de l'établissement des connexions SSL au cours de la communication avec un serveur LDAP générique. Ces communications utilisent LDAP sur SSL (LDAPS). Si vous activez la validation de certificat, téléversez le certificat de l'autorité de certification (AC) qui a émis le certificat utilisé par le serveur LDAP lors de l'établissement des connexions SSL. Le certificat de l'AC est utilisé pour valider l'authenticité du certificat fourni par le serveur LDAP lors de l'établissement des connexions SSL.

   **REMARQUE :** Dans cette version, toute liaison LDAP basée sur un port autre que le port SSL n'est pas prise en charge. Seul LDAP sur SSL est pris en charge.

4. Sous **Paramètres du certificat**, cochez **Activer la validation de certificats** pour activer la validation de certificat. En cas d'activation, iDRAC6 utilise le certificat d'une autorité de certification pour valider le certificat du serveur LDAP lors de l'établissement de liaisons SSL (Secure Socket Layer) ; en cas de désactivation, iDRAC6 ignore l'étape de validation de certificat de l'établissement de liaisons SSL. Vous pouvez désactiver la validation de certificat au cours du test ou si votre administrateur système choisit de faire confiance aux contrôleurs de domaine dans l'étendue de sécurité sans valider leurs certificats SSL.

   **PRÉCAUTION : Veillez à ce que CN = FQDN LDAP ouvert soit défini (par exemple, CN= openldap.lab) dans le champ Objet du certificat de serveur LDAP lors de la génération du certificat. Le champ Adresse du serveur LDAP d'iDRAC6 doit être défini pour correspondre à la même adresse FQDN afin que la validation de certificat puisse fonctionner.**

5 Sous **Téléverser le certificat d'autorité de certification du service de répertoire**, tapez le chemin de fichier du certificat ou naviguez pour trouver le fichier du certificat.

**REMARQUE :** Vous devez taper le chemin de fichier absolu, y compris le chemin et le nom de fichier complets et l'extension du fichier.

6 Cliquez sur **Téléverser**.

Le certificat de l'AC racine qui signe tous les certificats de serveur SSL (Security Socket Layer) des contrôleurs de domaine est téléversé.

7 Cliquez sur **Suivant**. La page **Configuration et gestion LDAP génériques Étape 2/3** s'affiche. Utilisez cette page pour configurer les informations d'emplacement concernant les serveurs LDAP générique et les comptes d'utilisateur.

**REMARQUE :** dans cette version, les fonctionnalités Authentification bifactorielle (TFA) articulée autour de la carte à puce et Connexion directe (SSO) ne sont pas prises en charge dans le service d'annuaire LDAP générique.

8 Entrez les informations suivantes :

- Sélectionnez **Activer LDAP générique**.

**REMARQUE :** Dans cette version, le groupe imbriqué n'est pas pris en charge. Le micrologiciel recherche le membre direct du groupe pour le faire correspondre au nom unique d'utilisateur. En outre, seul le domaine unique est pris en charge. Le domaine croisé n'est pas pris en charge.

- Sélectionnez l'option **Utiliser le nom unique pour rechercher l'appartenance au groupe** afin d'utiliser le nom unique comme membres du groupe. iDRAC6 compare le nom unique d'utilisateur récupéré dans le répertoire aux membres du groupe. Si cette option est décochée, le nom d'utilisateur fourni par l'utilisateur d'ouverture de session est utilisé afin de le comparer aux membres du groupe.
- Dans le champ **Adresse du serveur LDAP**, saisissez le nom de domaine pleinement qualifié (FQDN) 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. iDRAC6 tente de se connecter à chaque serveur l'un après l'autre jusqu'à ce qu'une connexion soit établie.
- Saisissez le port utilisé pour LDAP sur SSL dans le champ **Port du serveur LDAP**. Le port par défaut est 636.

- Dans le champ **Nom unique de liaison**, saisissez le nom unique d'un utilisateur utilisé afin d'établir la liaison au serveur lors de la recherche du nom unique de l'utilisateur d'ouverture de session. S'il n'est pas spécifié, une liaison anonyme est utilisée.
- Saisissez le **mot de passe de liaison** à utiliser en conjonction avec le **nom unique de liaison**. Ceci est obligatoire si la liaison anonyme n'est pas autorisée.
- Dans le champ **Nom unique de base à rechercher**, saisissez le nom unique de la branche du répertoire à partir duquel toutes les recherches doivent débuter.
- Dans le champ **Attribut de l'ouverture de session utilisateur**, saisissez l'attribut d'utilisateur à rechercher. L'attribut par défaut est UID. Il est recommandé de s'assurer de son unicité au sein du nom unique de base choisi, sinon un filtre de recherche doit être configuré afin de garantir l'unicité de l'utilisateur d'ouverture de session. Si le nom unique d'utilisateur ne peut pas être identifié de manière unique par la combinaison de recherche de l'attribut et du filtre de recherche, l'ouverture de session échoue.
- Dans le champ **Attribut d'appartenance au groupe**, spécifiez quel attribut LDAP doit être utilisé pour rechercher l'appartenance au groupe. Il doit s'agir d'un attribut de la classe de groupe. S'il n'est pas spécifié, iDRAC6 utilise les attributs *member* et *uniquemember*.
- Dans le champ **Filtre de recherche**, saisissez un filtre de recherche LDAP valide. Utilisez le filtre 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*=*, ce qui recherche tous les objets de l'arborescence. Ce filtre de recherche supplémentaire configuré par l'utilisateur s'applique uniquement à la recherche du nom unique d'utilisateur, et non à la recherche d'appartenance au groupe.

**9** Cliquez sur **Suivant**. La page **Configuration et gestion LDAP génériques Étape 3a/3** s'affiche. Utilisez cette page pour configurer les groupes de privilèges utilisés pour autoriser les utilisateurs. Lorsque LDAP générique est activé, le ou les groupes de rôles sont utilisés pour spécifier la stratégie d'autorisation applicable aux utilisateurs iDRAC6.

**REMARQUE :** dans cette version, contrairement à AD, il n'est pas nécessaire d'avoir recours aux caractères spéciaux (« @ », « \ » et « / ») pour différencier un utilisateur LDAP d'un utilisateur local. Vous devez uniquement saisir votre nom d'utilisateur pour ouvrir une session et ne vous devez pas inclure le nom de domaine.

10 Sous **Groupes de rôles**, cliquez sur un **Groupe de rôles**.

La page **Configuration et gestion LDAP génériques Étape 3b/3** s'affiche. Utilisez cette page pour configurer chaque groupe de rôles utilisé pour contrôler la règle d'autorisation applicable aux utilisateurs.

11 Dans le champ **Nom unique du groupe**, entrez le nom unique du groupe qui identifie le groupe de rôles dans le service d'annuaire LDAP générique associé à iDRAC6.

12 Dans la section **Privilèges du groupe de rôles**, spécifiez les privilèges associés au groupe en sélectionnant le **niveau de privilège du groupe de rôles**. Par exemple, si vous sélectionnez **Administrateur**, tous les privilèges sont sélectionnés pour ce niveau de droit.

13 Cliquez sur **Appliquer** pour enregistrer les paramètres du groupe de rôles.

Le serveur Web iDRAC6 vous renvoie automatiquement à la page **Configuration et gestion LDAP génériques Étape 3a/3** où vos paramètres Groupe de rôles sont affichés.

14 Configurez des groupes de rôles supplémentaires, le cas échéant.

15 Cliquez sur **Terminer** pour revenir à la page récapitulative **Configuration et gestion de LDAP générique**.

16 Cliquez sur **Paramètres de test** pour vérifier les paramètres LDAP générique.

17 Saisissez le nom d'utilisateur et le mot de passe d'un utilisateur de répertoire choisi pour tester les paramètres LDAP. Le format dépend de l'*attribut d'ouverture de session utilisateur* utilisé et le nom d'utilisateur saisi doit correspondre à la valeur de l'attribut choisi.

Les résultats du test et le journal du test sont affichés. Vous avez terminé la configuration du service de répertoire LDAP générique.

### Configuration du service de répertoire LDAP générique avec la RACADM

```
racadm config -g cfgldap -o cfgLdapEnable 1
```

```
racadm config -g cfgldap -o cfgLdapServer <FQDN ou
adresse-IP>
```

```
racadm config -g cfgldap -o cfgLdapPort <Numéro
de port>
```

```
racadm config -g cfgldap -o cfgLdapBaseDN dc=
common,dc=com
```

```
racadm config -g cfgldap -o
cfgLdapCertValidationenable 0
```

```
racadm config -g cfgldaprolegroup -i 1 -o
cfgLdapRoleGroupDN 'cn=everyone,ou=groups,dc=
common,dc=com'
```

```
racadm config -g cfgldaprolegroup -i 1 -o
cfgLdapRoleGroupPrivilege 0x0001
```

Affichez les paramètres à l'aide des commandes ci-dessous

```
racadm getconfig -g cfgldap
```

```
racadm getconfig -g cfgldaprolegroup -i 1
```

Utilisez la RACADM pour confirmer si l'ouverture de session est possible

```
racadm -r <iDRAC6-IP> -u user.1 -p password getractime
```

Paramètres supplémentaires pour tester l'option Nom unique de liaison

```
racadm config -g cfgldap -o cfgLdapBindDN "cn=
idrac_admin,ou=iDRAC_admins,ou=People,dc=common,
dc=com"
```

```
racadm config -g cfgldap -o cfgLdapBindPassword
password
```

**REMARQUE :** configurez iDRAC6 pour qu'il utilise un serveur de nom de domaine qui permettra de résoudre le nom d'hôte du serveur LDAP utilisé par iDRAC6 dans l'adresse de serveur LDAP. Le nom d'hôte doit correspondre au « CN » ou à l'« Objet » dans le certificat du serveur LDAP.

# Questions les plus fréquentes concernant Active Directory

**Mon ouverture de session Active Directory a échoué. Comment puis-je résoudre le problème ?**

L'iDRAC6 offre un outil de diagnostic dans l'interface Web. Ouvrez une session en tant qu'utilisateur local avec des droits Administrateur depuis l'interface Web. Cliquez sur **Paramètres iDRAC→ onglet Réseau/Sécurité→ Service de répertoire→ Microsoft Active Directory**. Allez à la fin de la page **Configuration et gestion d'Active Directory** et cliquez sur **Paramètres de test**. Saisissez un nom d'utilisateur et un mot de passe de test, puis cliquez sur **Démarrer le test**. iDRAC6 lance les tests étape par étape et affiche les résultats de chaque étape. Un résultat de test détaillé est également journalisé pour vous aider à résoudre tout problème. Retournez à la page **Configuration et gestion d'Active Directory**. Allez à la fin de la page et cliquez sur **Configurer Active Directory** pour modifier votre configuration et exécuter de nouveau le test jusqu'à ce que l'utilisateur du test réussisse l'étape d'authentification.

**J'ai activé la validation de certificat, mais mon ouverture de session Active Directory a échoué. J'ai exécuté les diagnostics depuis l'IUG et les résultats du test affichent le message d'erreur suivant :**

**ERREUR : impossible de contacter le serveur LDAP, erreur : 14090086:routines SSL :SSL3_GET_SERVER_CERTIFICATE : échec de la vérification du certificat : veuillez vérifier que le certificat de l'AC correct a été téléversé vers iDRAC. Veuillez également vérifier que la date d'iDRAC est comprise dans la période de validité des certificats et que l'adresse du contrôleur de domaine configurée dans iDRAC correspond à l'objet du certificat de serveur de répertoire.**

**Quel peut être le problème et comment le résoudre ?**

Si la validation de certificat est activée, iDRAC6 utilise le certificat d'autorité de certification téléversé pour vérifier le certificat du serveur de répertoire lorsqu'iDRAC6 établit la connexion SSL avec le serveur de répertoire. Les raisons les plus courantes de l'échec de la validation de certificat sont :

1. La date d'iDRAC6 n'est pas comprise dans la période de validité du certificat de serveur ou du certificat d'autorité de certification. Vérifiez l'heure d'iDRAC6 et la période de validité de votre certificat.

2 Les adresses du contrôleur de domaine configurées dans iDRAC6 ne correspondent pas à l'objet ou à l'autre nom de l'objet du certificat de serveur de répertoire. Si vous utilisez une adresse IP, veuillez lire la question et la réponse suivantes. Si vous utilisez un FQDN, veuillez vous assurer que vous utilisez le FQDN du contrôleur de domaine, et non le domaine, par exemple, `nomduserveur.exemple.com` au lieu de `exemple.com`.

**J'utilise une adresse IP comme adresse de contrôleur de domaine et je ne suis pas parvenu à valider le certificat. Quel est le problème ?**

Cochez le champ Objet ou Autre nom de l'objet du certificat de votre contrôleur de domaine. Active Directory utilise généralement le nom d'hôte, et non l'adresse IP, du contrôleur de domaine dans le champ Objet ou Autre nom de l'objet du certificat du contrôleur de domaine. Vous pouvez résoudre le problème de plusieurs façons :

1 Configurer le nom d'hôte (FQDN) du contrôleur de domaine en tant qu'*adresse(s) du contrôleur de domaine* sur iDRAC6 afin de correspondre à l'objet ou à l'autre nom de l'objet du certificat de serveur.

2 Émettre à nouveau le certificat de serveur pour utiliser une adresse IP dans le champ Objet ou Autre nom de l'objet afin que celui-ci corresponde à l'adresse IP configurée dans iDRAC6.

3 Désactiver la validation de certificats si vous choisissez de faire confiance à ce contrôleur de domaine sans validation de certificat durant l'établissement de liaisons SSL.

**J'utilise un schéma étendu dans un environnement à domaines multiples. Comment dois-je configurer les adresses du contrôleur de domaine ?**

Utilisez le nom d'hôte (FQDN) ou l'adresse IP du ou des contrôleurs de domaine desservant le domaine dans lequel l'objet iDRAC6 réside.

**Dois-je configurer la ou les adresses du catalogue global ?**

Si vous utilisez un schéma étendu, l'adresse du catalogue global n'est pas utilisée.

Si vous utilisez le schéma standard et que les utilisateurs et les groupes de rôles proviennent de domaines différents, une ou des adresses du catalogue global sont requises. Dans ce cas, seul le groupe universel peut être utilisé.

Si vous utilisez le schéma standard et que tous les utilisateurs et groupes de rôles proviennent du même domaine, une ou des adresses du catalogue global ne sont pas requises.

**Comment fonctionne la requête de schéma standard ?**

iDRAC6 se connecte tout d'abord à ou aux adresses du contrôleur de domaine configurées et si l'utilisateur et les groupes de rôles sont dans ce domaine, les privilèges seront enregistrés.

Si une ou des adresses de contrôleur global sont configurées, iDRAC6 continue d'interroger le catalogue global. Si des privilèges supplémentaires sont récupérés du catalogue global, ces privilèges sont accumulés.

**iDRAC6 utilise-t-il toujours LDAP sur SSL ?**

Oui. Tous les transports se font via le port sécurisé 636 et/ou 3269.

Durant la *définition du test*, iDRAC6 effectue une connexion LDAP CONNECT uniquement pour aider à isoler le problème, mais il n'effectue pas de liaison LDAP BIND sur une connexion non sécurisée.

**Pourquoi iDRAC6 active-t-il la validation de certificat par défaut ?**

iDRAC6 renforce la sécurité afin d'assurer l'identité du contrôleur de domaine auquel iDRAC6 se connecte. À défaut de la validation de certificat, un pirate pourrait usurper un contrôleur de domaine et détourner la connexion SSL. Si vous choisissez de faire confiance à tous les contrôleurs de domaine de votre étendue de sécurité sans validation de certificat, vous pouvez la désactiver via l'IUG ou la CLI.

**iDRAC6 prend-il en charge le nom NetBIOS ?**

Pas dans cette version.

**Que dois-je vérifier si je ne parviens pas à ouvrir une session sur iDRAC6 avec Active Directory ?**

Vous pouvez diagnostiquer le problème en cliquant sur **Paramètres de test** au bas de la page **Configuration et gestion d'Active Directory** dans l'interface Web iDRAC6. Corrigez ensuite le problème spécifique indiqué par les résultats du test. Pour de plus amples informations, reportez-vous à la section « Test de vos configurations », à la page 189.

La plupart des problèmes courants sont expliqués dans cette section ; toutefois, en général, vous devez vérifier les points suivants :

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 iDRAC6 local, ouvrez une session sur iDRAC6 à l'aide de vos références locales.

Lorsque vous avez ouvert une session :

a Vérifiez que vous avez coché l'option **Activer Active Directory** dans la page **Configuration et gestion d'Active Directory** iDRAC6.

b Vérifiez que le paramètre DNS est correct sur la page Configuration de la mise en réseau iDRAC6.

c Assurez-vous que vous avez téléversé le bon certificat d'autorité de certification racine d'Active Directory vers iDRAC6 si vous avez activé la validation de certificat. Assurez-vous que l'heure d'iDRAC6 est comprise dans la période de validité du certificat d'autorité de certification.

d Si vous utilisez le schéma étendu, assurez-vous que le **nom d'i**DRAC6 et le **nom de domaine i**DRAC6 correspondent à la configuration de votre environnement Active Directory.

Si vous utilisez le schéma standard, assurez-vous que le **Nom du groupe** et le **Nom de domaine du groupe** correspondent à votre configuration Active Directory.

3 Vérifiez les certificats SSL du contrôleur de domaine pour vous assurer que l'heure iDRAC6 est comprise dans la période de validité du certificat.

# 8

# Configuration d'iDRAC6 en vue de l'ouverture de session par connexion directe ou carte à puce

Cette section fournit des informations permettant de configurer iDRAC6 en vue de l'ouverture de session par carte à puce dans le cas des utilisateurs locaux et des utilisateurs d'Active Directory, ainsi que de l'ouverture de session par connexion directe (SSO) dans le cas des utilisateurs d'Active Directory.

iDRAC6 prend en charge l'authentification Active Directory Kerberos afin de pouvoir accepter les ouvertures de session par connexion directe (SSO) et par carte à puce Active Directory.

## À propos de l'authentification Kerberos

Kerberos est un protocole d'authentification de réseau qui permet aux systèmes de communiquer en toute sécurité sur un réseau non sécurisé. Pour cela, les systèmes doivent prouver leur authenticité. Pour se conformer aux normes de mise en application d'authentification renforcées, l'iDRAC6 prend désormais en charge l'authentification Active Directory Kerberos afin de pouvoir accepter les ouvertures de session par connexion directe (SSO) et par carte à puce Active Directory.

Microsoft Windows 2000, Windows XP, Windows Server 2003, Windows Vista et Windows Server 2008 utilisent Kerberos comme méthode d'authentification par défaut.

iDRAC6 utilise Kerberos pour prendre en charge deux types de mécanisme d'authentification : les ouvertures de session par connexion directe (SSO) Active Directory et les ouvertures de session par carte à puce Active Directory. Pour l'ouverture de session par connexion directe (SSO), iDRAC6 utilise les références utilisateur mises en cache dans le système d'exploitation après que l'utilisateur a ouvert une session avec un compte Active Directory valide.

Pour l'ouverture de session par carte à puce Active Directory, iDRAC6 utilise l'authentification bifactorielle (TFA) s'articulant autour de la carte à puce comme références pour activer une ouverture de session Active Directory. Voici la fonctionnalité de suivi de l'authentification par carte à puce locale.

L'authentification Kerberos sur iDRAC6 échoue si l'heure d'iDRAC6 diffère de celle du contrôleur de domaine. Un décalage maximum de 5 minutes est autorisé. Pour que l'authentification réussisse, synchronisez l'heure du serveur avec celle du contrôleur de domaine, puis **réinitialisez** iDRAC6.

## Conditions requises en vue de la connexion directe et de l'authentification par carte à puce Active Directory

Les conditions requises en vue de la connexion directe et de l'authentification par carte à puce Active Directory sont les suivantes :

- Configurez iDRAC6 en vue de l'ouverture de session Active Directory. Pour plus d'informations, voir « Utilisation du service de répertoire iDRAC6 », à la page 151.
- Enregistrez iDRAC6 comme un ordinateur dans le domaine racine Active Directory. Pour ce faire :
  - **a** Cliquez sur **Paramètres iDRAC**→ onglet **Réseau/Sécurité** tab→ sous-onglet **Réseau**.
  - **b** Fournissez une adresse IP valide pour le **serveur DNS préféré/l'autre serveur DNS**. Cette valeur est l'adresse IP du DNS faisant partie du domaine racine et authentifiant les comptes Active Directory des utilisateurs.
  - **c** Sélectionnez **Enregistrer iDRAC auprès du DNS.**
  - **d** Spécifiez un **nom de domaine DNS** valide.

    Voir l'*aide en ligne d'iDRAC6* pour plus d'informations.
- Pour prendre en charge les deux nouveaux types de mécanisme d'authentification, iDRAC6 prend en charge la configuration pour se définir en tant que service « kerberisé » sur un réseau Windows Kerberos. La configuration Kerberos sur iDRAC6 requiert les mêmes étapes que celles effectuées pour la configuration d'un service autre que Windows Server Kerberos en tant que principe de sécurité au sein de Windows Server Active Directory.

L'outil **ktpass** Microsoft (fourni par Microsoft sur le CD/DVD d'installation du serveur) sert à créer les liaisons du nom du service principal (SPN) sur un compte d'utilisateur et à exporter les informations d'approbation dans un fichier *keytab* Kerberos de style MIT, permettant ainsi d'établir une relation de confiance entre un utilisateur ou système externe et le KDC (Key Distribution Centre). Le fichier keytab contient une clé cryptographique qui sert à crypter les informations entre le serveur et le KDC. L'outil ktpass permet aux services s'articulant autour d'UNIX qui prennent en charge l'authentification Kerberos d'utiliser les fonctionnalités d'interopérabilité fournies par un service KDC Windows Server Kerberos.

Le fichier keytab généré par l'utilitaire ktpass est mis à la disposition d'iDRAC6 en tant que téléversement de fichier et est activé pour devenir un service « kerberisé » sur le réseau.

Étant donné qu'iDRAC6 est un périphérique avec un système d'exploitation autre que Windows, exécutez l'utilitaire **ktpass** (qui fait partie de Microsoft Windows) sur le contrôleur de domaine (serveur Active Directory) où vous souhaitez mapper iDRAC6 à un compte d'utilisateur dans Active Directory.

Par exemple, utilisez la commande **ktpass** suivante pour créer le fichier keytab Kerberos :

```
C:\>ktpass -princ
HOST/dracname.domainname.com@DOMAINNAME.COM
-mapuser dracname -crypto DES-CBC-MD5 -ptype
KRB5_NT_PRINCIPAL -pass * -out c:\krbkeytab
```

Le type de cryptage qu'iDRAC6 utilise pour l'authentification Kerberos est DES-CBC-MD5. Le type principal est KRB5_NT_PRINCIPAL.
La propriété **Utiliser les types de cryptage DES pour ce compte** doit être activée pour les propriétés du compte d'utilisateur sur lequel est mappé le nom du service principal.

**REMARQUE :** il est recommandé d'utiliser le dernier utilitaire **ktpass** pour créer le fichier keytab.

Cette procédure génère un fichier keytab que vous devez téléverser vers iDRAC6.

**REMARQUE :** le fichier keytab contient une clé de cryptage et doit être conservé en lieu sûr.

Pour plus d'informations sur l'utilitaire **ktpass**, consultez le site Web de Microsoft à l'adresse : **http://technet2.microsoft.com/windowsserver/en/library/64042138-9a5a-4981-84e9-d576a8db0d051033.mspx?mfr=true**

- L'heure d'iDRAC6 doit être synchronisée avec celle du contrôleur de domaine Active Directory. Vous pouvez également utiliser la commande de décalage du fuseau horaire RACADM suivante pour synchroniser l'heure :

  ```
  racadm config -g cfgRacTuning -o

  cfgRacTuneTimeZoneOffset <valeur de décalage>
  ```

- Pour activer la connexion directe pour le schéma étendu, assurez-vous que l'option **Approuver cet utilisateur pour la délégation à tous les services (Kerberos uniquement)** est sélectionnée sur l'onglet **Délégation** de l'utilisateur du fichier keytab. Cet onglet est disponible uniquement une fois le fichier keytab créé à l'aide de l'utilitaire **ktpass**.

### Paramètres du navigateur afin d'activer la connexion directe Active Directory

Pour configurer les paramètres du navigateur pour Internet Explorer :

1. Ouvrez le navigateur Web Internet Explorer
2. Sélectionnez **Outils→ Options Internet→ Sécurité→ Intranet local**.
3. Cliquez sur **Sites**.
4. Sélectionnez les options suivantes uniquement :
   - Inclure tous les sites locaux (Intranet) non mentionnés dans d'autres zones.
   - Inclure tous les sites qui n'utilisent pas de serveur proxy.
5. Cliquez sur **Advanced** (Avancé).
6. Ajoutez tous les noms de domaine relatifs qui seront utilisés pour les instances Weblogic Server faisant partie intégrante de la configuration SSO (par exemple, monhôte.exemple.fr)
7. Cliquez sur **Fermer**, puis sur **OK**.
8. Cliquez sur **OK**.

Pour configurer les paramètres du navigateur pour Firefox :

1. Ouvrez le navigateur Web Firefox.
2. Dans la barre d'adresses, entrez `about:config`.
3. Dans **Filtre**, entrez `network.negotiate`.
4. Ajoutez le nom iDRAC à network.negotiate-auth.trusted-uris (à l'aide d'une liste séparée par des virgules).
5. Ajoutez le nom iDRAC à network.negotiate-auth.delegation-uris (à l'aide d'une liste séparée par des virgules).

# Utilisation de la connexion directe Microsoft Active Directory

La fonctionnalité Connexion directe vous permet d'ouvrir une session sur iDRAC6 directement après avoir ouvert une session sur votre station de travail sans saisir vos références d'authentification utilisateur de domaine, par exemple le nom d'utilisateur et le mot de passe. Pour ouvrir une session sur iDRAC6 à l'aide de cette fonctionnalité, vous devez déjà être connecté à votre système via un compte d'utilisateur Active Directory valide. En outre, vous devez déjà avoir configuré le compte d'utilisateur pour ouvrir une session sur iDRAC6 à l'aide des références d'Active Directory. iDRAC6 utilise les références d'Active Directory mises en cache pour ouvrir une session.

Vous pouvez activer l'iDRAC6 pour utiliser Kerberos, un protocole d'authentification réseau, afin de permettre la connexion directe. Pour plus d'informations, voir « À propos de l'authentification Kerberos », à la page 201. Assurez-vous d'avoir suivi les étapes répertoriées dans la section « Conditions requises en vue de la connexion directe et de l'authentification par carte à puce Active Directory », à la page 202 avant de configurer iDRAC6 en vue de l'ouverture de session par connexion directe.

## Configuration d'iDRAC6 en vue de l'utilisation de la connexion directe

Suivez les étapes suivantes pour configurer iDRAC6 en vue de la connexion directe via l'interface Web iDRAC :

1. Connectez-vous à l'interface Web iDRAC.
2. Accédez à **Paramètres iDRAC**→ onglet **Réseau/Sécurité**→ onglet **Service de répertoire**→ **Microsoft Active Directory**.

3 Cliquez sur **Configurer Active Directory**. La page **Configuration et gestion d'Active Directory Étape 1/4** s'affiche.

4 Téléversez le fichier keytab obtenu à partir du domaine racine Active Directory vers iDRAC6. Pour ce faire, sous **Téléverser le fichier keytab Kerberos**, entrez le chemin du fichier keytab ou cliquez sur **Parcourir** pour accéder au fichier. Cliquez sur **Téléverser**. Le fichier keytab Kerberos sera téléversé vers iDRAC6. Le fichier keytab est le même fichier que celui que vous avez créé lors de l'exécution des tâches répertoriées dans la section « Conditions requises en vue de la connexion directe et de l'authentification par carte à puce Active Directory », à la page 202.

5 Cliquez sur **Suivant**. La page **Configuration et gestion d'Active Directory Étape 2/4** s'affiche.

6 Sélectionnez **Activer la connexion directe** pour activer l'ouverture de session par connexion directe.

7 Cliquez sur **Suivant** jusqu'à ce que la dernière page s'affiche. Si Active Directory est configuré pour utiliser le schéma standard, la page **Configuration et gestion d'Active Directory Étape 4a/4** s'affiche alors. Si Active Directory est configuré pour utiliser le schéma étendu, la page **Configuration et gestion d'Active Directory Étape 4/4** s'affiche alors.

8 Cliquez sur **Terminer** pour appliquer les paramètres.

**Utilisation de RACADM** :

Vous pouvez téléverser le fichier keytab sur iDRAC6 à l'aide de la commande racadm CLI suivante :

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

où <nom de fichier> est le nom du fichier keytab. La commande racadm est prise en charge par la racadm locale et distante.

Pour activer la connexion directe à l'aide de la CLI, exécutez la commande racadm :

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

## Ouverture de session iDRAC6 via la connexion directe

1 Ouvrez une session sur votre système avec un compte Active Directory valide.

2 Pour accéder à la page Web d'iDRAC6, tapez :

`https://<adresse du nom de domaine complet>`

Si le numéro de port HTTPS par défaut (port 443) a été modifié, tapez :

`https://<adresse du nom de domaine complet>:<numéro de port>`

où *adresse du nom de domaine complet* correspond au nom de domaine complet d'iDRAC (nomdnsidrac.nom domaine) et *numéro de port* correspond au numéro de port HTTPS.

**REMARQUE :** si vous utilisez une adresse IP au lieu d'un nom de domaine complet, la connexion directe échoue.

iDRAC6 vous connecte à l'aide de vos références mises en cache dans le système d'exploitation lorsque vous avez ouvert une session avec votre compte Active Directory valide.

Vous avez ouvert une session sur iDRAC6 avec les privilèges Microsoft Active Directory appropriés si :

- vous êtes un utilisateur Microsoft Active Directory,
- vous êtes configuré dans iDRAC6 comme pouvant ouvrir une session Active Directory,
- iDRAC6 est activé pour l'authentification Active Directory Kerberos.

# Configuration de l'authentification par carte à puce

iDRAC6 prend en charge la fonctionnalité Authentification bifactorielle (TFA) en activant **la connexion par carte à puce**.

Les schémas d'authentification standard utilisent le nom d'utilisateur et le mot de passe pour authentifier les utilisateurs. Ils n'offrent qu'une sécurité minimale.

Pour sa part, la TFA offre un niveau accru de sécurité en exigeant que les utilisateurs fournissent deux facteurs d'authentification : ce qu'ils ont (la carte à puce, un périphérique physique) et ce qu'ils savent (un code secret tel qu'un mot de passe ou un code PIN).

L'authentification bifactorielle exige des utilisateurs qu'ils vérifient leur identité en fournissant *les deux* facteurs.

### Configuration des utilisateurs d'iDRAC6 local pour l'ouverture de session par carte à puce

Vous pouvez configurer les utilisateurs d'iDRAC6 local pour qu'ils ouvrent une session sur iDRAC6 au moyen de la carte à puce. Cliquez sur **Paramètres iDRAC → Réseau/Sécurité→ Utilisateurs**.

Toutefois, pour que l'utilisateur puisse ouvrir une session sur iDRAC6 avec la carte à puce, vous devez téléverser le certificat de la carte à puce de l'utilisateur et le certificat de l'autorité de certification (AC) de confiance vers iDRAC6.

**REMARQUE :** assurez-vous que la validation de certificat de l'autorité de certification est activée avant de configurer la carte à puce.

#### Exportation du certificat de la carte à puce

Vous pouvez obtenir le certificat de l'utilisateur en exportant le certificat de la carte à puce à l'aide du logiciel de gestion de carte (CMS) de la carte à puce vers un fichier sous le format encodé Base64. Vous pouvez généralement obtenir le CMS auprès du fournisseur de la carte à puce. Ce fichier encodé doit être téléversé en tant que certificat de l'utilisateur vers iDRAC6. L'autorité de certification de confiance qui émet les certificats utilisateur de carte à puce doit également exporter le Certificat d'une autorité de certification vers un fichier au format encodé Base64. Vous devez téléverser ce fichier en tant que certificat d'une AC de confiance pour l'utilisateur. Configurez l'utilisateur avec le nom d'utilisateur qui forme le nom de principe d'utilisateur (UPN) de l'utilisateur dans le certificat de la carte à puce.

**REMARQUE :** pour l'ouverture d'une session sur iDRAC6, le nom d'utilisateur que vous configurez dans iDRAC6 doit avoir la même casse que le nom de principe d'utilisateur (UPN) dans le certificat de la carte à puce.

Par exemple, si le certificat de la carte à puce a été émis pour l'utilisateur, « exempleutilisateur@domaine.com », le nom d'utilisateur doit être configuré comme « exempleutilisateur ».

### Configuration des utilisateurs d'Active Directory pour l'ouverture de session par carte à puce

Avant d'utiliser la fonctionnalité d'ouverture de session par carte à puce Active Directory, assurez-vous d'avoir déjà configuré iDRAC6 pour l'ouverture de session Active Directory et vérifiez que le compte d'utilisateur pour lequel la carte à puce a été émise a été activé en vue de l'ouverture de session Active Directory iDRAC6.

En outre, assurez-vous que vous avez activé le paramètre d'ouverture de session Active Directory. Voir « Utilisation du service de répertoire iDRAC6 », à la page 151 pour plus d'informations sur la configuration des utilisateurs Active Directory. Vous devez également activer iDRAC6 pour lui permettre de devenir un service « kerberisé » en téléversant un fichier *keytab* valide, obtenu auprès du domaine racine Active Directory, vers iDRAC6.

Pour configurer les utilisateurs d'Active Directory pour qu'ils ouvrent une session sur iDRAC6 au moyen de la carte à puce, l'administrateur d'iDRAC6 doit configurer le serveur DNS, téléverser le certificat d'autorité de certification Active Directory sur iDRAC6 et activer l'ouverture de session Active Directory. Voir « Utilisation du service de répertoire iDRAC6 », à la page 151 pour plus d'informations sur la configuration des utilisateurs Active Directory.

Vous pouvez configurer Active Directory depuis **Paramètres iDRAC→ Réseau/Sécurité→ Service de répertoire→Microsoft Active Directory.**

**REMARQUE :** assurez-vous que la validation de certificat de l'autorité de certification est activée avant de configurer la carte à puce.

### Configuration de la carte à puce à l'aide d'iDRAC6

**REMARQUE :** pour modifier ces paramètres, vous devez avoir le droit **Configurer iDRAC**.

1. Dans l'interface Web iDRAC6, accédez à **Paramètres iDRAC→ Réseau/Sécurité→** onglet **Carte à puce**.
2. Configurez les paramètres Ouverture de session par carte à puce.

   Le Tableau 8-1 fournit des informations sur les paramètres de la page **Carte à puce**.
3. Cliquez sur **Appliquer**.

**Tableau 8-1. Paramètres de la carte à puce**

| Paramètre | Description |
|---|---|
| Configurer l'ouverture de session par carte à puce | • **Désactivé :** désactive l'ouverture de session par carte à puce. Les ouvertures de session ultérieures depuis l'interface utilisateur graphique (IUG) affichent la page d'ouverture de session habituelle. Toutes les interfaces hors bande de la ligne de commande, y compris Secure Shell (SSH), Telnet, série et la RACADM distante sont définies sur leur état par défaut.<br>• **Activé :** active l'ouverture de session par carte à puce. Après avoir appliqué les modifications, fermez la session, insérez votre carte à puce, puis cliquez sur **Ouvrir une session** pour saisir le code PIN de votre carte à puce. L'activation de la connexion par carte à puce désactive toutes les interfaces hors bande de la CLI, y compris SSH, Telnet, série, la RACADM distante et IPMI sur le LAN car ces services prennent uniquement en charge l'authentification monofactorielle.<br>• **Activé avec la racadm distante :** active l'ouverture de session par carte à puce en même temps que la RACADM distante. Toutes les autres interfaces hors bande de la CLI sont désactivées.<br>Si vous sélectionnez **Activé** ou **Activé avec la Racadm distante**, vous êtes invité à ouvrir une session par carte à puce au cours des tentatives d'ouverture de session ultérieures via l'interface Web.<br>Il est recommandé à l'administrateur d'iDRAC6 d'utiliser le paramètre **Activer avec la Racadm distante** uniquement pour accéder à l'interface Web iDRAC6 afin d'exécuter des scripts à l'aide des commandes de la RACADM distante. Si l'administrateur n'a pas besoin d'utiliser la RACADM distante, il est recommandé d'utiliser le paramètre **Activé** pour la connexion par carte à puce. Assurez-vous que la configuration des utilisateurs locaux d'iDRAC6 et/ou la configuration d'Active Directory a été achevée avant d'activer la connexion par carte à puce.<br>**REMARQUE :** l'ouverture de session par carte à puce impose de configurer les utilisateurs d'iDRAC6 local avec les certificats appropriés. Si l'ouverture de session par carte à puce sert à ouvrir une session pour un utilisateur Microsoft Active Directory, vous devez vous assurer que vous avez bien configuré le certificat d'utilisateur Active Directory pour cet utilisateur. Vous pouvez configurer le certificat d'utilisateur dans la page **Utilisateurs→ Menu principal utilisateurs**. |

**Tableau 8-1. Paramètres de la carte à puce *(suite)***

| Paramètre | Description |
|---|---|
| Activer le contrôle CRL pour l'ouverture de session par carte à puce | Ce contrôle est disponible uniquement pour les utilisateurs locaux de la carte à puce. Sélectionnez cette option si vous souhaitez qu'iDRAC6 contrôle la liste de révocation de certificat (CRL) pour vérifier si le certificat de la carte à puce de l'utilisateur a été révoqué. Le certificat iDRAC de l'utilisateur, téléchargé depuis le serveur de distribution de la liste de révocation de certificat (CRL) est vérifié afin de déterminer s'il a été révoqué dans la CRL.<br><br>Les serveurs de distribution LRC sont répertoriés dans les certificats de la carte à puce des utilisateurs.<br><br>Pour que la fonctionnalité CRL puisse fonctionner, une adresse IP DNS valide doit être configurée sur iDRAC6 dans sa configuration réseau. Vous pouvez configurer l'adresse IP DNS dans iDRAC6 sous **Paramètres iDRAC→ Réseau/Sécurité→ Réseau**.<br><br>L'utilisateur n'est pas en mesure d'ouvrir une session si :<br>• Le certificat d'utilisateur est répertorié comme révoqué dans le fichier CRL.<br>• iDRAC6 n'est pas en mesure de communiquer avec le serveur de distribution CRL.<br>• iDRAC6 n'est pas en mesure de télécharger la CRL.<br><br>**REMARQUE :** vous devez configurer correctement l'adresse IP du serveur DNS dans la page **Réseau/Sécurité→ Réseau** pour que ce contrôle réussisse. |

## Ouverture de session sur iDRAC6 avec la carte à puce

L'interface Web d'iDRAC6 affiche la page Ouverture de session par carte à puce pour tous les utilisateurs qui sont configurés pour utiliser la carte à puce.

**REMARQUE :** assurez-vous que la configuration des utilisateurs locaux d'iDRAC6 et/ou la configuration d'Active Directory a été achevée avant d'activer l'ouverture de session par carte à puce pour l'utilisateur.

**REMARQUE :** selon les paramètres de votre navigateur, il se peut que vous soyez invité à télécharger et à installer le plug-in ActiveX du lecteur de carte à puce lorsque vous utilisez cette fonctionnalité pour la première fois.

1 Accédez à la page Web d'iDRAC6 avec https.

`https://<adresse IP>`

Si le numéro de port HTTPS par défaut (port 443) a été modifié, tapez :

`https://<adresse IP>:<numéro de port>`

où `<adresse IP>` est l'adresse IP d'iDRAC6 et *`numéro de port`* le numéro de port HTTPS.

La page Ouverture de session iDRAC6 apparaît et vous invite à insérer la carte à puce.

2 Insérez la carte à puce dans le lecteur et cliquez sur **Ouvrir une session**.

iDRAC6 vous invite à saisir le code PIN de la carte à puce.

3 Saisissez le code PIN?de la carte à puce pour les utilisateurs locaux de la carte à puce et si l'utilisateur n'est pas créé localement, iDRAC6 vous invite à saisir le mot de passe pour le compte Active Directory de l'utilisateur.

**REMARQUE :** si vous êtes un utilisateur d'Active Directory pour lequel **Activer le contrôle CRL pour l'ouverture de session par carte à puce** est sélectionné, iDRAC6 tente de télécharger la CRL et contrôle celle-ci pour le certificat de l'utilisateur. L'ouverture de session via Active Directory échoue si le certificat est répertorié comme révoqué dans la CRL ou si la CRL ne peut pas être téléchargée pour une raison quelconque.

Vous avez ouvert une session sur iDRAC6.

### Ouverture d'une session sur iDRAC6 avec l'authentification par carte à puce Active Directory

1 Ouvrez une session sur iDRAC6 avec https.

`https://<adresse IP>`

Si le numéro de port HTTPS par défaut (port 443) a été modifié, tapez :

`https://<adresse IP>:<numéro de port>` où *`adresse IP`* correspond à l'adresse IP de l'iDRAC6 et le *`numéro de port`* correspond au numéro de port HTTPS.

La page Ouverture de session iDRAC6 apparaît et vous invite à insérer la carte à puce.

2 Introduisez la carte à puce, puis cliquez sur **Ouverture de session**.

La boîte de dialogue contextuelle Code PIN s'affiche.

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

Vous avez ouvert une session sur iDRAC6 avec vos références telles qu'elles sont définies dans Active Directory.

# Dépannage de l'ouverture de session par carte à puce dans iDRAC6

Utilisez les astuces suivantes pour déboguer une carte à puce inaccessible :

#### Plug-in ActiveX 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 présents 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 PIN 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 l'iDRAC6 local

Si un utilisateur d'iDRAC6 local ne parvient pas à ouvrir une session, vérifiez si le nom d'utilisateur et les certificats d'utilisateur téléversés sur iDRAC6 ont expiré. Les journaux de suivi d'iDRAC6 peuvent fournir des messages de journal importants sur les erreurs bien que les messages d'erreur soient parfois intentionnellement ambigus pour des raisons de sécurité.

**Impossible d'ouvrir une session sur iDRAC6 en tant qu'utilisateur d'Active Directory**

- Si vous ne parvenez pas à ouvrir une session sur iDRAC6 en tant qu'utilisateur d'Active Directory, essayez d'ouvrir une session sur iDRAC6 sans activer l'ouverture de session par carte à puce. Si vous avez activé le contrôle CRL, essayez d'ouvrir une session sur Active Directory sans activer le contrôle CRL. Le journal de suivi d'iDRAC6 doit fournir des messages importants en cas de défaillance de la CRL.
- Vous avez également la possibilité de désactiver l'ouverture de session par carte à puce via la racadm locale à l'aide de la commande suivante : `racadm config -g cfgSmartCard -o cfgSmartCardLogonEnable 0`
- Pour les plateformes Windows 64 bits, le plug-in d'authentification iDRAC6 ne s'installe pas correctement si une version 64 bits du progiciel redistribuable Microsoft Visual C++ 2005 est déployée. Pour installer et exécuter le plug-in Active–X correctement, déployez la version 32 bits du progiciel redistribuable Microsoft Visual C++ 2005 SP1 (x86). Ce progiciel est requis pour lancer la session Console virtuelle sur un navigateur Internet Explorer.
- Si vous obtenez le message d'erreur suivant « `Impossible de charger le plug-in de carte à puce. Vérifiez vos paramètres IE. Il se peut également que vous ne disposiez pas de privilèges suffisants pour pouvoir utiliser le plug-in de carte à puce` », installez alors le progiciel redistribuable Microsoft Visual C++ 2005 SP1 (x86). Ce fichier est disponible sur le site Web de Microsoft à l'adresse **microsoft.com**. Deux versions distribuées du progiciel redistribuable C++ ont été testées et permettent le chargement du plug-in de carte à puce Dell. Voir Tableau 8-2.

**Tableau 8-2. Versions distribuées du progiciel redistribuable C++**

| Nom du fichier du progiciel redistribuable | Version | Date de mise sur le marché | Taille | Description |
|---|---|---|---|---|
| vcredist_x86.exe | 6.0.2900.2180 | 21 mars 2006 | 2,56 Mo | MS Redistributable 2005 |
| vcredist_x86.exe | 9.0.21022.8 | 7 novembre 2007 | 1,73 Mo | MS Redistributable 2008 |

- Vérifiez que la différence entre l'heure d'iDRAC6 et l'heure du contrôleur de domaine sur le serveur du contrôleur de domaine est de 5 minutes au plus afin que l'authentification Kerberos puisse fonctionner. Vérifiez l'**Heure RAC** sur la page **Système→ Paramètres iDRAC→ Propriétés→ Informations sur iDRAC** et l'heure du contrôleur de domaine en cliquant avec le bouton droit de la souris sur l'heure dans le coin inférieur droit de l'écran. Le décalage de fuseau horaire est affiché dans l'affichage contextuel. Pour l'heure normale du centre des États-Unis (CST), ce décalage est de - 6). Utilisez la commande de décalage du fuseau horaire RACADM suivante pour synchroniser l'heure d'iDRAC6 (via la RACADM distante ou Telnet/SSH) : `racadm config -g cfgRacTuning –o cfgRacTuneTimeZoneOffset <valeur du décalage en minutes>.` Par exemple, si l'heure système est GMT -6 (heure normale du centre des États-Unis) et que l'heure est 14h00, définissez l'heure d'iDRAC6 sur 18h00 GMT, ce qui vous oblige à saisir « 360 » dans la commande ci-dessus pour le décalage. Vous pouvez également utiliser *cfgRacTuneDaylightoffset* afin de prendre en compte la variation de l'heure d'été. Vous n'aurez ainsi plus à changer l'heure à ces deux périodes de l'année où les ajustements d'heures sont effectués ou prenez-les tout simplement en compte dans le décalage ci-dessus en utilisant 300 dans l'exemple ci-dessus.

# Questions les plus fréquentes concernant la connexion directe

**L'ouverture de session par SSO échoue sous Windows Server 2008 R2 x64. Que dois-je faire pour faire fonctionner SSO sous Windows Server 2008 R2 x64 ?**

1. Exécutez **http://technet.microsoft.com/en-us/library/dd560670(WS.10).aspx** pour le contrôleur de domaine et la règle de domaine. Configurez vos ordinateurs pour qu'ils utilisent la suite de cryptage DES-CBC-MD5. Ces paramètres peuvent avoir une incidence sur la compatibilité avec les ordinateurs ou services clients et les applications de votre environnement. Le paramètre de règle **Configurer les types de cryptage autorisés pour Kerberos** se trouve sous **Configuration ordinateur\Paramètres de sécurité\Règles locales\Options de sécurité**.
2. Les clients de domaine doivent disposer du GPO à jour. À la ligne de commande, tapez `gpupdate /force` et supprimez l'ancien fichier keytab grâce à la commande `klist purge`.
3. Une fois le GPO mis à jour, créez le nouveau fichier keytab.
4. Téléversez le fichier keytab vers iDRAC6.

Vous pouvez désormais ouvrir une session iDRAC via la connexion directe.

**L'ouverture de session par connexion directe échoue pour les utilisateurs AD dotés de Windows 7 et Windows Server 2008 R2. Que dois-je faire pour y remédier ?**

Vous devez activer les types de cryptage dédiés à Windows 7 et Windows Server 2008 R2. Pour activer les types de cryptage :

1. Ouvrez une session en tant qu'administrateur ou qu'utilisateur doté du privilège d'administration.
2. Allez à **Démarrer** et exécutez **gpedit.msc**. La fenêtre **Éditeur de stratégie de groupe local** s'affiche.
3. Naviguez vers **Paramètres de l'ordinateur local→ Paramètres Windows→ Paramètres de sécurité→ Stratégies locales→ Options de sécurité**.
4. Effectuez un clic droit sur **Sécurité réseau : Configurer les types de cryptage autorisés pour Kerberos** et sélectionnez **Propriétés**.

5. Activez toutes les options.
6. Cliquez sur **OK**. Vous pouvez désormais ouvrir une session iDRAC via la connexion directe.

Configurez les paramètres supplémentaires suivants pour le schéma étendu :

1. Dans la fenêtre **Éditeur de stratégie de groupe local**, naviguez vers **Paramètres de l'ordinateur local→ Paramètres Windows→ Paramètres de sécurité→ Stratégies locales→ Options de sécurité**.
2. Cliquez-droite sur **Sécurité réseau : Restreindre NTLM : trafic NTLM sortant vers le serveur distant** et sélectionnez **Propriétés**.
3. Sélectionnez **Tout autoriser**.
4. Cliquez sur **OK**, puis fermez la fenêtre **Éditeur de stratégie de groupe local**.
5. Allez dans **Démarrer** et exécutez **cmd**. La fenêtre d'**invite de commande** s'affiche.
6. Exécutez la commande `gpupdate /force`. Les stratégies de groupe sont mises à jour. Fermez la fenêtre d'**invite de commande**.
7. Allez dans **Démarrer** et exécutez **regedit**. La fenêtre **Éditeur du Registre** s'affiche.
8. Naviguez vers **HKEY_LOCAL_MACHINE→ Système→ CurrentControlSet→ Contrôle→ LSA**.
9. Dans le volet de droite, effectuez un clic droit et sélectionnez **Nouvelle→ Valeur DWORD (32 bits)**.
10. Nommez la nouvelle clé **SuppressExtendedProtection**.
11. Cliquez-droite sur **SuppressExtendedProtection** et cliquez sur **Modifier.**
12. Dans le champ **Données de la valeur**, tapez 1 et cliquez sur **OK**.
13. Fermez la fenêtre **Éditeur du Registre**. Vous pouvez désormais ouvrir une session iDRAC via la connexion directe.

**Si vous avez activé la connexion directe pour iDRAC et utilisez Internet Explorer pour ouvrir une session iDRAC, la connexion directe échoue, et le système vous invite à entrer vos nom d'utilisateur et mot de passe. Comment puis-je y remédier ?**

Assurez-vous que l'adresse IP iDRAC figure bien dans **Outils→ Options Internet→ Sécurité→ Sites de confiance**. Si elle n'y figure pas, la connexion directe échoue et le système vous invite à entrer votre nom d'utilisateur et votre mot de passe. Cliquez sur **Annuler** et poursuivez.

# 9

# Utilisation de la console virtuelle de l'interface utilisateur

Cette section fournit des informations sur l'utilisation de la fonctionnalité Console virtuelle iDRAC6.

## Présentation

La fonctionnalité Console virtuelle iDRAC6 vous permet d'accéder à la console locale à distance en mode graphique ou texte. À l'aide de la console virtuelle, vous pouvez contrôler un ou plusieurs systèmes compatibles iDRAC6 à partir d'un seul emplacement.

Vous n'avez pas besoin de vous installer devant chaque serveur pour effectuer l'ensemble des opérations de maintenance de routine. En effet, vous pouvez gérer les serveurs depuis n'importe quel endroit, à partir de votre bureau ou de votre ordinateur portable. Vous pouvez aussi partager les informations avec d'autres, à distance et instantanément.

## Utilisation de la console virtuelle

**REMARQUE :** lorsque vous ouvrez une session Console virtuelle, le serveur géré n'indique pas que la console a été redirigée.

**REMARQUE :** si une session de la console virtuelle est déjà ouverte depuis la station de gestion sur un iDRAC spécifique, toute tentative d'ouverture d'une nouvelle session depuis la même station de gestion sur cet iDRAC6 échouera.

**REMARQUE :** il est possible d'ouvrir simultanément des sessions Console virtuelle multiples à partir d'une station de gestion unique vers plusieurs contrôleurs iDRAC6.

La page **Console virtuelle** vous permet de gérer le système distant en utilisant le clavier, la vidéo et la souris de votre station de gestion locale pour contrôler les périphériques correspondants sur un serveur géré distant. Cette fonctionnalité peut être utilisée conjointement avec la fonctionnalité Média virtuel pour effectuer des installations de logiciels à distance.

Les règles suivantes s'appliquent à une session Console virtuelle :

- Quatre sessions Console virtuelle simultanées sont prises en charge au maximum. Toutes les sessions affichent la même console de serveur géré simultanément.
- À partir de la version 1.5, il est possible d'exécuter des sessions multiples vers plusieurs serveurs distants à partir du même client, en fonction de leur ordre d'ouverture. Si une session Console virtuelle utilisant le plug-in Java est ouverte, vous pouvez en ouvrir une autre qui utilise le plug-in ActiveX. Toutefois, si une session Console virtuelle de type ActiveX est ouverte, vous n'avez alors pas la possibilité d'ouvrir une autre session Console virtuelle utilisant le plug-in Java. Vous devez fermer la première session Console virtuelle pour pouvoir ouvrir une deuxième session Console virtuelle.
- Une session Console virtuelle ne doit pas être lancée à partir d'un navigateur Web sur le système géré.
- Une bande passante réseau disponible minimale de 1 Mo/s est exigée.
- La première session Console virtuelle vers iDRAC6 est une session à accès complet. Si un deuxième utilisateur sollicite une session Console virtuelle, le premier utilisateur est averti et l'option lui est offerte (approuver, rejeter ou autoriser en lecture seule) d'envoyer une requête de partage au deuxième utilisateur. Le deuxième utilisateur est averti qu'un autre utilisateur contrôle la session. Lorsque le premier utilisateur n'a pas répondu à chaque requête de partage ultérieure de l'utilisateur dans un délai de 30 secondes, l'accès à la console virtuelle est octroyé en fonction de la valeur définie pour l'objet `cfgRacTuneVirtualConsoleAuthorizeMultipleSessions`. Cet objet ne tient pas compte du type de plug-in (ActiveX ou Java) défini pour être utilisé dans la deuxième/troisième/quatrième session. Pour des informations supplémentaires sur cet objet, voir le *Guide de référence de la ligne de commande RACADM pour iDRAC6 et CMC* sur le site de support Dell à l'adresse **dell.com/support/manuals**.

  **REMARQUE :** ceci s'applique uniquement à la RACADM distante ou micrologicielle (SSH ou Telnet), et non à la RACADM locale.

### Configuration de votre station de gestion

Pour utiliser la console virtuelle sur votre station de gestion, procédez comme suit :

1. Installez et configurez un navigateur Web pris en charge. Consultez les sections suivantes pour plus d'informations :
   - « Navigateurs Web pris en charge », à la page 28
   - « Configuration d'un navigateur Web pris en charge », à la page 44
2. Si vous utilisez Firefox ou souhaitez utiliser le visualiseur Java avec Internet Explorer, installez un environnement d'exécution Java (JRE). Si vous utilisez le navigateur Internet Explorer, un contrôle ActiveX est fourni pour le visualiseur de console. Vous pouvez également utiliser le visualiseur de console Java avec Firefox si vous installez un JRE et configurez le visualiseur de console dans l'interface Web iDRAC6 avant de lancer le visualiseur.
3. Si vous utilisez Internet Explorer (IE), vérifiez que le navigateur est activé pour télécharger le contenu crypté comme suit :
   - Accédez à Options ou Paramètres d'Internet Explorer et sélectionnez **Outils→ Options Internet → Avancé**.
   - Faites défiler jusqu'à **Sécurité** et supprimez l'option suivante :

     `Ne pas enregistrer les pages cryptées sur le disque`
4. Si vous utilisez Internet Explorer pour lancer une session Console virtuelle à l'aide du plug-in Active-X, assurez-vous d'avoir ajouté l'IP ou le nom d'hôte iDRAC6 à la liste **Sites de confiance**. Vous devez également réinitialiser les paramètres personnalisés sur **Moyen-faible** ou modifier les paramètres afin de permettre l'installation de plug-ins Active-X signés. Pour plus d'informations, voir « Configurations du navigateur Internet Explorer pour les applications Console virtuelle et Média virtuel de type ActiveX », à la page 223.

**REMARQUE :** le plug-in ActiveX 64 bits n'est pas pris en charge pour lancer une session Console virtuelle via Internet Explorer.

5 Il est recommandé de configurer la résolution d'affichage de votre moniteur sur au moins 1 280 x 1 024 pixels.

**REMARQUE :** si votre serveur exécute un système d'exploitation Linux, une console X11 peut ne pas être affichable sur le moniteur local. Appuyez sur <Ctrl><Alt><F1> sur Console virtuelle iDRAC6 pour commuter Linux vers une console de texte.

**REMARQUE :** vous pouvez occasionnellement rencontrer l'erreur de compilation de script Java suivante : « `Attendu : ; ».` Pour résoudre ce problème, définissez les paramètres réseau sur **Connexion directe** dans JavaWebStart : **Edition→ Préférences→ Général→ Paramètres réseau** et sélectionnez **Connexion directe** au lieu de **Utiliser les paramètres du navigateur**.

### Effacer la mémoire cache de votre navigateur

Si vous rencontrez des problèmes lors de l'utilisation de la console virtuelle (erreurs hors plage, problèmes de synchronisation, etc.), effacez la mémoire cache du navigateur pour retirer ou supprimer les anciennes versions du visualiseur susceptibles d'être stockées sur le système, puis réessayez.

**REMARQUE :** Vous devez disposer du privilège Administrateur pour pouvoir effacer la mémoire cache du navigateur.

Pour supprimer les anciennes versions du visualiseur Active-X pour IE7, procédez comme suit :

1 Fermez Video Viewer et le navigateur Internet Explorer.

2 Ouvrez à nouveau le navigateur Internet Explorer et accédez à **Internet Explorer→ Outils→ Gérer les modules complémentaires** et cliquez sur **Activer ou désactiver les modules complémentaires**. La fenêtre **Gérer les modules complémentaires** s'affiche.

3 Sélectionnez **Modules complémentaires qui ont été utilisés par Internet Explorer** dans le menu déroulant **Afficher**.

4 Supprimez le module complémentaire *Video Viewer*.

Pour supprimer les anciennes versions du visualiseur Active-X pour IE8, procédez comme suit :

1 Fermez Video Viewer et le navigateur Internet Explorer.

2 Ouvrez à nouveau le navigateur Internet Explorer et accédez à **Internet Explorer→ Outils→ Gérer les modules complémentaires** et cliquez sur **Activer ou désactiver les modules complémentaires**. La fenêtre **Gérer les modules complémentaires** s'affiche.

3 Sélectionnez **Tous les modules complémentaires** dans le menu déroulant **Afficher**.

4 Sélectionnez le module complémentaire *Video Viewer* et cliquez sur le lien **Plus d'informations**.

5 Sélectionnez **Supprimer** dans la fenêtre **Plus d'informations**.

6 Fermez les fenêtres **Plus d'informations** et **Gérer les modules complémentaires**.

Pour supprimer les anciennes versions du visualiseur Java sous Windows ou Linux, procédez comme suit :

1 À l'invite de commande, exécutez `javaws-viewer` ou `javaws-uninstall`

2 Le **visualiseur Java Cache** s'affiche.

3 Supprimez les éléments intitulés *Client de console virtuelle iDRAC6*.

## Configurations du navigateur Internet Explorer pour les applications Console virtuelle et Média virtuel de type ActiveX

Cette section fournit des informations sur les paramètres du navigateur Internet Explorer requis pour lancer et exécuter les applications Console virtuelle et Média virtuel de type ActiveX.

**REMARQUE :** Effacez la mémoire cache du navigateur, puis implémentez les paramètres de configuration du navigateur. Pour plus d'informations, voir « Effacer la mémoire cache de votre navigateur », à la page 222.

### Paramètres communs aux systèmes d'exploitation Microsoft Windows

1 Dans Internet Explorer, accédez à **Outils**→ **Options Internet**→ onglet **Sécurité**.

2 Sélectionnez la zone que vous souhaitez utiliser pour exécuter l'application.

3 Cliquez sur **Personnaliser**. Si vous utilisez Internet Explorer 8, cliquez sur **Personnaliser le niveau**. La fenêtre **Paramètres de sécurité** s'affiche.

4 Sous **Contrôles ActiveX et plug-ins** :

- Sélectionnez l'option **Demander** pour **Télécharger les contrôles ActiveX signés**

- Sélectionnez l'option **Activé** ou **Demander** pour **Exécuter les contrôles ActiveX et les plug-ins**
- Sélectionnez l'option **Activé** ou **Demander** pour **Contrôles ActiveX reconnus sûrs pour l'écriture de scripts**
- Cliquez sur **OK** une première fois, puis une seconde fois.

#### Paramètres supplémentaires pour les systèmes d'exploitation Windows Vista ou Microsoft les plus récents

Les navigateurs Internet Explorer intégrés à Windows Vista ou aux systèmes d'exploitation les plus récents sont dotés d'une fonctionnalité de sécurité supplémentaire intitulée « Mode protégé ».

Vous pouvez lancer et exécuter des applications ActiveX dans les navigateurs Internet Explorer dotés de la fonctionnalité « Mode protégé » en procédant de l'une des manières suivantes :

- Allez dans **Program Files→ Internet Explorer**. Effectuez un clic droit sur **iexplore.exe** et cliquez sur **Exécuter en tant qu'administrateur**.
- Ajoutez l'adresse IP d'iDRAC à la zone Sites de confiance. Pour ce faire :

1. Dans Internet Explorer, accédez à **Outils→ Options Internet→ Sécurité→ Sites de confiance**.
2. Assurez-vous que l'option **Activer le mode protégé** n'est pas sélectionnée pour la zone Sites de confiance. Vous avez également la possibilité d'ajouter l'adresse iDRAC aux sites de la zone Intranet. Par défaut, le mode protégé est désactivé pour les sites des zones Intranet et Sites de confiance.
3. Cliquez sur **Sites**.
4. Dans le champ **Ajouter ce site Web à la zone**, ajoutez les adresses de votre iDRAC et cliquez sur **Ajouter**.
5. Cliquez sur **Fermer**, puis sur **OK**.
6. Fermez et redémarrez le navigateur pour que les paramètres soient pris en compte.

## Résolutions d'écran prises en charge et taux de rafraîchissement

Le Tableau 9-1 énumère les résolutions d'écran prises en charge et les taux de rafraîchissement correspondants pour une session Console virtuelle qui s'exécute sur le serveur géré.

**Tableau 9-1. Résolutions d'écran prises en charge et taux de rafraîchissement**

| Résolution d'écran | Taux de rafraîchissement (Hz) |
|---|---|
| 720x400 | 70 |
| 640x480 | 60, 72, 75, 85 |
| 800x600 | 60, 70, 72, 75, 85 |
| 1024x768 | 60, 70, 72, 75, 85 |
| 1280x1024 | 60 |

## Configuration de la console virtuelle dans l'interface Web iDRAC6

Pour configurer la console virtuelle dans l'interface Web iDRAC6, effectuez les étapes suivantes :

1. Cliquez sur **Système→ Console/Média→ Configuration** pour configurer les paramètres de la console virtuelle iDRAC6.
2. Configurez les propriétés de la console virtuelle.Le Tableau 9-2 décrit les paramètres de la console virtuelle.
3. Une fois l'opération terminée, cliquez sur **Appliquer** pour enregistrer les nouveaux paramètres.

**Tableau 9-2. Propriétés de configuration de la console virtuelle**

| Propriété | Description |
|---|---|
| **Enabled (Activé)** | Cliquez pour activer ou désactiver la console virtuelle. Si cette option est cochée, cela signifie que la console virtuelle est activée. L'option par défaut est **Activé**.<br>**REMARQUE :** le fait de cocher ou de décocher l'option **Activé** une fois que la console virtuelle est lancée risque de déconnecter toutes vos sessions Console virtuelle existantes. |
| **Nombre maximal de sessions** | Sélectionnez le nombre maximal de sessions Console virtuelle autorisées, entre 1 et 4. La valeur par défaut est **2**. |

**Tableau 9-2. Propriétés de configuration de la console virtuelle *(suite)***

| Propriété | Description |
|---|---|
| **Sessions actives** | Affiche le nombre de sessions de consoles actives. Ce champ est en lecture seule. |
| **Port de présence à distance** | Numéro de port réseau utilisé en vue de la connexion à l'option clavier/souris de la console virtuelle. Ce trafic est toujours crypté. Vous devez peut-être changer ce numéro si un autre programme utilise le port par défaut. Le port par défaut est **5900**.<br>**REMARQUE :** le fait de modifier la valeur **Port de présence à distance** une fois que la console virtuelle est lancée risque de déconnecter toutes vos sessions Console virtuelle existantes. |
| **Cryptage vidéo activé** | **Coché** indique que le cryptage vidéo est activé. Tout le trafic à destination du port vidéo est crypté.<br>**Décoché** indique que le cryptage vidéo est désactivé. Le trafic à destination du port vidéo n'est pas crypté.<br>La valeur par défaut est **Crypté**. La désactivation du cryptage peut améliorer les performances sur les réseaux plus lents.<br>**REMARQUE :** le fait d'activer ou de désactiver l'option **Cryptage vidéo activé** une fois que la console virtuelle est lancée risque de déconnecter toutes vos sessions Console virtuelle existantes. |
| **Vidéo locale du serveur activée** | Coché indique que la sortie vers le moniteur Console virtuelle iDRAC6 est désactivée lors de l'utilisation de la console virtuelle. Ceci assure que les tâches que vous effectuez avec la **console virtuelle** ne sont pas visibles sur le moniteur local du serveur géré. |
| **Type de plug-in** | Type de plug-in à configurer.<br>• **Natif** (ActiveX pour Windows et le plug-in Java pour Linux) : le visualiseur ActiveX fonctionne uniquement sur Internet Explorer.<br>• **Java** : un visualiseur Java est lancé. |

**REMARQUE :** pour obtenir des informations sur l'utilisation du média virtuel avec la console virtuelle, voir « Configuration et utilisation du média virtuel », à la page 279.

## Ouverture d'une session Console virtuelle

Lorsque vous ouvrez une session Console virtuelle, l'application du visualiseur de la console virtuelle de Dell démarre et le bureau du système distant apparaît dans le visualiseur. Grâce à l'application du visualiseur de la console virtuelle, vous pouvez contrôler les fonctions de souris et de clavier du système distant à partir de votre station de gestion locale.

**REMARQUE :** le lancement de la console virtuelle à partir d'une station de gestion Windows Vista peut générer des messages de redémarrage de la console virtuelle. Pour éviter ce problème, définissez les valeurs du délai d'expiration appropriées aux emplacements suivants : **Panneau de configuration→ Options d'alimentation→ Economiseur d'énergie→ Paramètres avancés→ Disque dur→ Eteindre le disque dur après <délai_d'expiration>** et dans le **Panneau de configuration→ Options d'alimentation→ Haute performance→ Paramètres avancés→ Disque dur→ Eteindre le disque dur après <délai_d'expiration>**.

Pour ouvrir une session Console virtuelle dans l'interface Web, effectuez les étapes suivantes :

1. Cliquez sur **Système→ Console/Média→ Console virtuelle et média virtuel**.
2. Servez-vous des informations du Tableau 9-3 pour vérifier qu'une session Console virtuelle est disponible.

   Pour reconfigurer les valeurs des propriétés affichées, consultez « Configuration de la console virtuelle dans l'interface Web iDRAC6 », à la page 225.

**Tableau 9-3. Console virtuelle**

| Propriété | Description |
|---|---|
| **Console virtuelle activée** | Oui/Non (cochée\non cochée) |
| **Cryptage vidéo activé** | Oui/Non (cochée\non cochée) |
| **Nombre maximal de sessions** | Affiche le nombre maximal de sessions Console virtuelle prises en charge. |
| **Sessions actives** | Affiche le nombre actuel de sessions Console virtuelle actives. |

**Tableau 9-3. Console virtuelle *(suite)***

| Propriété | Description |
|---|---|
| Vidéo locale du serveur activée | Oui = Activé ; non = Désactivé. |
| Port de présence à distance | Numéro de port réseau utilisé en vue de la connexion à l'option clavier/souris de la console virtuelle. Ce trafic est toujours crypté. Vous devez peut-être changer ce numéro si un autre programme utilise le port par défaut. L'adresse par défaut est 5900. |
| Type de plug-in | Affiche le type de plug-in que vous avez sélectionné à la page **Configuration**.<br>**REMARQUE :** pour les plateformes Windows 64 bits, le plug-in Active–X d'authentification iDRAC6 ne s'installe pas correctement si une version 64 bits du progiciel redistribuable Microsoft Visual C++ 2005 est déployée. Pour installer et exécuter le plug-in Active–X correctement, déployez la version 32 bits du progiciel redistribuable Microsoft Visual C++ 2005 SP1 (x86). Ce progiciel est requis pour lancer la session Console virtuelle sur un navigateur Internet Explorer. |

**REMARQUE :** pour obtenir des informations sur l'utilisation du média virtuel avec la console virtuelle, voir « Configuration et utilisation du média virtuel », à la page 279.

3 Si une session de console virtuelle est disponible, cliquez sur **Lancer la console virtuelle** sur la page **Console virtuelle et média virtuel**.

**REMARQUE :** plusieurs boîtes de message peuvent apparaître après le lancement de l'application. Afin d'empêcher l'accès non autorisé à l'application, naviguez au sein de ces boîtes de message dans les trois minutes. Sinon, vous êtes invité à relancer l'application.

**REMARQUE :** si une ou plusieurs fenêtres **Alerte de sécurité** apparaissent au cours des étapes suivantes, lisez les informations qu'elles contiennent et cliquez sur **Oui** pour continuer.

La station de gestion se connecte à iDRAC6 et le bureau du système distant apparaît dans l'application du visualiseur de la console virtuelle iDRAC6.

4 Deux pointeurs de souris apparaissent dans la fenêtre du visualiseur : un pour le système distant et l'autre pour votre système local. Vous pouvez les remplacer par un curseur unique en sélectionnant l'option **Curseur unique** sous **Outils** dans le menu Console virtuelle iDRAC6.

## Aperçu de la console virtuelle

Avant de lancer la console virtuelle, vous pouvez afficher un aperçu de l'état de celle-ci sur la page **Système→ Propriétés→ Résumé du système**. La section **Aperçu de la console virtuelle** affiche une image montrant l'état de la console virtuelle. L'image est automatiquement actualisée toutes les 30 secondes.

**REMARQUE :** l'image Console virtuelle est disponible uniquement si vous avez activé la console virtuelle et si la carte iDRAC6 Enterprise est présente.

Le Tableau 9-4 fournit des informations sur les options disponibles.

**Tableau 9-4. Options de l'aperçu de la console virtuelle**

| Option | Description |
|---|---|
| **Lancer** | Cliquez sur ce lien pour lancer la console virtuelle.<br>Si seul le média virtuel est activé, le fait de cliquer sur ce lien lance directement le média virtuel.<br>Ce lien ne s'affiche pas si vous ne disposez pas des privilèges Console virtuelle ou si la console virtuelle et le média virtuel sont désactivés. |
| **Paramètres** | Cliquez sur ce lien pour afficher ou modifier les paramètres de configuration de la console virtuelle sur la page **Configuration de la console/du média**.<br>**REMARQUE :** vous devez disposer des privilèges de configuration iDRAC pour pouvoir modifier les paramètres de configuration de la console virtuelle. |
| **Actualiser** | Cliquez sur ce lien pour actualiser l'image Console virtuelle qui s'affiche. |

# Utilisation de la console virtuelle iDRAC6 (Video Viewer)

La console virtuelle iDRAC6 (Video Viewer) fournit une interface utilisateur entre la station de gestion et le serveur géré, vous permettant ainsi de visualiser le bureau du serveur géré et de contrôler ses fonctions clavier et souris à partir de votre station de gestion. Lorsque vous vous connectez au système distant, la console virtuelle iDRAC6 démarre dans une fenêtre séparée.

**REMARQUE :** vous devez disposez des droits d'administrateur pour pouvoir lancer une console virtuelle iDRAC6 (Video Viewer).

**REMARQUE :** si le serveur distant est éteint, le message **Aucun signal** s'affiche.

**REMARQUE :** la barre de titre Console virtuelle affiche le nom DNS ou l'adresse IP de l'iDRAC auquel vous êtes connecté à partir de la station de gestion. Si l'iDRAC ne possède pas de nom DNS, l'adresse IP s'affiche alors. Le format est le suivant : `<nom DNS / adresse IPv6 / adresse IPv4>, <Modèle>, Utilisateur : <nom d'utilisateur>, <fps>`

La console virtuelle iDRAC6 fournit divers réglages de commandes tels que la synchronisation de la souris, les instantanés, les macros de clavier et l'accès au média virtuel. Pour plus d'informations sur ces fonctions, cliquez sur **Système→ Console/Média** puis sur **Aide** sur la page d'IUG **Console virtuelle et média virtuel**.

Lorsque vous démarrez une session Console virtuelle et que la console virtuelle iDRAC6 apparaît, il est possible que vous ayez à synchroniser les pointeurs de souris.

Le Tableau 9-5 décrit les options de menu disponibles dans le visualiseur.

**Tableau 9-5. Sélections sur la barre de menus du visualiseur**

| Élément de menu | Élément | Description |
|---|---|---|
| Icône « broche » | S/O | Cliquez sur l'icône « broche » pour verrouiller la barre de menus Console virtuelle iDRAC6. Cela empêche le masquage automatique de la barre d'outils.<br>**REMARQUE :** cette opération s'applique uniquement au visualiseur Active-X, et non au plug-in Java. |

**Tableau 9-5. Sélections sur la barre de menus du visualiseur *(suite)***

| Élément de menu | Élément | Description |
|---|---|---|
| Média virtuel | Lancer le média virtuel | La **session de média virtuel** s'affiche et répertorie les périphériques disponibles en vue du mappage dans la fenêtre principale. Pour virtualiser une image ISO ou IMG, cliquez sur **Ajouter** et sélectionnez le fichier image. Le fichier image sélectionné s'affiche, ainsi que la liste des périphériques disponibles en vue du mappage, dans la fenêtre principale. Pour virtualiser un périphérique ou une image, cochez l'option dans la colonne **Mappé** du tableau. Le périphérique ou l'image sera mappé au serveur à ce stade. Pour démapper, décochez la case.<br><br>Cliquez sur **Détails** pour afficher un volet répertoriant les images et périphériques virtuels. Celui-ci affiche également l'activité de lecture/écriture inhérente à chaque périphérique ou image. |
| Fichier | Saisir dans un fichier | Saisit l'écran du système distant actuel dans un fichier **.bmp** sous Windows ou dans un fichier **.png** sous Linux. Une boîte de dialogue s'affiche pour que vous puissiez enregistrer le fichier dans un emplacement spécifié.<br><br>**REMARQUE :** le format de fichier **.bmp** sous Windows ou **.png** sous Linux s'appliquent uniquement au plug-in natif. Le plug-in Java prend uniquement en charge les formats de fichier **.jpg** et **.jpeg**. |
| | Quitter | Lorsque vous n'avez plus besoin d'utiliser la console et que vous avez fermé la session (en suivant la procédure de fermeture de session du système distant), sélectionnez **Quitter** dans le menu **Fichier** pour fermer la fenêtre **Console virtuelle iDRAC6**. |

**Tableau 9-5. Sélections sur la barre de menus du visualiseur *(suite)***

| Élément de menu | Élément | Description |
|---|---|---|
| Afficher | Actualiser | Actualise l'affichage de la console virtuelle vidéo. La console virtuelle sollicite une trame vidéo de référence auprès du serveur. |
| | Plein écran/En fenêtre | Affichez la console virtuelle vidéo en mode Plein écran. Pour quitter le mode Plein écran, cliquez sur **En fenêtre**. |
| | Ajuster | Redimensionne la fenêtre Console virtuelle vidéo à la taille minimale requise pour afficher la vidéo du serveur. Cet élément de menu n'est pas disponible en mode Plein écran. |

**Tableau 9-5. Sélections sur la barre de menus du visualiseur *(suite)***

| Élément de menu | Élément | Description |
|---|---|---|
| Macros | • Alt+Ctrl+Suppr<br>• Alt+Tab<br>• Alt+Échap<br>• Ctrl+Échap<br>• Alt+Espace<br>• Alt+Entrée<br>• Alt+Tiret<br>• Alt+F4<br>• ImprÉcran<br>• Alt+Impr. écran<br>• F1<br>• Pause (Suspension)<br>• Tab<br>• Ctrl+Entrée<br>• Syst<br>• Alt+Maj gauche+Maj droit+Échap<br>• Ctrl+Alt+Retour arrière<br>• Alt+F? (Où F? représente les touches F1 à F12)<br>• Ctrl+Alt+F? (Où F? représente les touches F1 à F12) | Lorsque vous sélectionnez une macro ou saisissez son raccourci clavier, l'action s'exécute sur le système distant. |

**Tableau 9-5. Sélections sur la barre de menus du visualiseur *(suite)***

| Élément de menu | Élément | Description |
|---|---|---|
| Outils | **Options de session** | La fenêtre Options de sessions fournit des réglages de commandes Session Viewer supplémentaires. Cette fenêtre comporte les onglets **Général** et **Souris**.<br>Vous pouvez contrôler le **Mode de transmission au clavier** depuis l'onglet Général. Sélectionnez **Transmettre toutes les séquences de touches à la cible** pour transmettre les séquences de touches de votre station de gestion au système distant.<br>L'onglet Souris contient deux sections : **Curseur unique** et **Accélération de la souris**. La fonctionnalité **Curseur unique** est fournie afin de permettre un décalage des problèmes d'alignement de la souris sur certains systèmes d'exploitation distants. Dès que le visualiseur entre en mode **Curseur unique**, le pointeur de la souris est piégé dans la fenêtre du visualiseur. Appuyez sur la touche d'arrêt pour quitter ce mode. Utilisez cette commande pour sélectionner la touche qui sortira du mode Curseur unique.<br>La fonctionnalité **Accélération de la souris** optimise les performances de la souris selon le système d'exploitation que vous utilisez. |
| | **Curseur unique** | Active le mode curseur unique dans le visualiseur. Dans ce mode, le curseur client est masqué si bien que seul le curseur du serveur est visible. Le curseur client est également piégé dans le cadre du visualiseur. L'utilisateur ne peut pas utiliser le curseur hors de la fenêtre du visualiseur tant qu'il n'a pas appuyé sur la **touche d'arrêt** spécifiée dans la fenêtre **Options de session**, onglet **Souris**. |
| | **Statistiques** | Cette option de menu lance une boîte de dialogue qui affiche les statistiques de performances du visualiseur. Les valeurs affichées sont les suivantes :<br>• Fréquence des trames<br>• Bande passante<br>• Compression<br>• Fréquence des paquets |

**Tableau 9-5. Sélections sur la barre de menus du visualiseur *(suite)***

| Élément de menu | Élément | Description |
|---|---|---|
| Alimentation | Allumer le système | Met le système sous tension. |
| | Arrêter le système | Arrête le système. |
| | Arrêt normal | Arrête le système.<br>**REMARQUE :** assurez-vous que l'option d'arrêt est configurée pour le système d'exploitation avant d'effectuer un arrêt normal à l'aide de cette option. Si vous utilisez cette option sans la configurer sur le système d'exploitation, le système géré redémarre et le système ne s'arrête pas. |
| | Réinitialiser le système (démarrage à chaud) | Réinitialise le système sans le mettre hors tension. |
| | Exécuter un cycle d'alimentation du système (démarrage à froid) | Met le système hors tension, puis le redémarre. |
| Aide | Contenu et index | Fournit des instructions sur la façon d'afficher l'aide en ligne. |
| | À propos de la console virtuelle iDRAC6 | Affiche la version de la **console virtuelle iDRAC6**. |

## Désactivation ou activation de la vidéo locale du serveur

Vous pouvez configurer iDRAC6 pour interdire les connexions Console virtuelle iDRAC6 via l'interface Web iDRAC6.

Si vous souhaitez vous assurer que vous disposez d'un accès exclusif à la console de serveur géré, vous devez désactiver la console locale *et* reconfigurer le **nombre maximal de sessions** sur `1` sur la page **Configuration de la console virtuelle**.

**REMARQUE :** si vous désactivez (éteignez) la vidéo locale sur le serveur, le moniteur, le clavier et la souris connectés à la console virtuelle iDRAC6 sont toujours activés.

Pour désactiver ou activer la console locale, procédez comme suit :

1. Sur votre station de gestion, ouvrez un navigateur Web pris en charge et ouvrez une session sur iDRAC6.
2. Cliquez sur **Système→ Console/Média→ Configuration**.
3. Pour désactiver (éteindre) la vidéo locale sur le serveur, décochez la case **Vidéo locale du serveur activée** de la page **Configuration**, puis cliquez sur **Appliquer**. La valeur par défaut est Désactivé.

   **REMARQUE :** si la vidéo locale du serveur est activée, comptez 15 secondes pour qu'il se désactive.
4. Pour activer (allumer) la vidéo locale sur le serveur, cochez la case **Vidéo locale du serveur activée** de la page **Configuration,** puis cliquez sur **Appliquer**.

# Lancement de la console virtuelle et du média virtuel à distance

Vous pouvez lancer la console virtuelle/le média virtuel en saisissant une URL unique dans un navigateur pris en charge au lieu de le/la lancer depuis l'IUG Web iDRAC6. Selon la configuration de votre système, vous passerez par le processus d'authentification manuelle (page d'ouverture de session) ou vous serez dirigé vers le visualiseur Console virtuelle/média virtuel automatiquement.

Si SSO est déjà configuré sur le système, vous ne pouvez pas utiliser le format pour lancer la console virtuelle/média virtuel.

Vous pouvez lancer la console virtuelle avec un compte utilisateur créé localement dans iDRAC6, LDAP et Active Directory.

**REMARQUE :** Internet Explorer prend en charge les ouvertures de session locales, Active Directory (AD), par carte à puce (SC) et par connexion directe (SSO). Firefox prend uniquement en charge les ouvertures de session locales, AD et par connexion directe (SSO) sur le système d'exploitation Windows. Il ne prend pas en charge l'ouverture de session par carte à puce (SC).

### Lancement de la console avec le format URL

Si vous saisissez le `lien<IP>/console` dans un navigateur, vous pouvez ensuite ouvrir une session à l'aide de la procédure d'ouverture de session normale manuelle selon sa configuration. Si l'ouverture de session réussit, la vue Console virtuelle/Média virtuel est lancée. Sinon, vous êtes redirigé vers la page d'accueil de l'interface utilisateur iDRAC6.

La session de l'interface utilisateur Web iDRAC s'affiche sur la page vKVM en arrière-plan.

Vous ne pouvez lancer qu'une session à la fois sur la console virtuelle.

Si vous disposez de privilèges Lecture seule uniquement, utilisez le format URL pour lancer la page de la console virtuelle uniquement et non la page du média virtuel.

Si la console virtuelle est désactivée dans iDRAC6, l'utilisateur ou l'administrateur peut toujours lancer le média virtuel, s'ils disposent des privilèges adéquats. Pour des informations supplémentaires sur les privilèges adéquats, voir « Lancement de la console virtuelle et du média virtuel à distance », à la page 236.

### Scénarios d'erreurs généraux

Le Tableau 9-6 répertorie les scénarios d'erreurs généraux, les raisons de ces erreurs et le comportement d'iDRAC6.

**Tableau 9-6. Scénarios d'erreurs**

| Scénarios d'erreurs | Raison | Comportement |
|---|---|---|
| L'ouverture de session a échoué | Vous avez saisi un nom d'utilisateur non valide ou un mot de passe incorrect. | Comportement identique lorsque *https://<IP>* est spécifié et l'ouverture de session échoue. |
| Carte iDRAC6 Enterprise non présente | La carte iDRAC6 Enterprise n'est pas présente. Par conséquent, la fonctionnalité Console virtuelle/média virtuel n'est pas disponible. | Le visualiseur Console virtuelle iDRAC6 n'est pas lancé. Vous redirige vers la page d'accueil de l'IUG iDRAC6. |

**Tableau 9-6. Scénarios d'erreurs *(suite)***

| Scénarios d'erreurs | Raison | Comportement |
|---|---|---|
| Privilèges insuffisants | Vous ne disposez pas des privilèges Console virtuelle et Média virtuel. | Le visualiseur Console virtuelle iDRAC6 n'est pas lancé et vous êtes redirigé vers la page d'IUG de configuration de la console/du média. |
| Console virtuelle désactivée | La console virtuelle est désactivée sur votre système. | Le visualiseur Console virtuelle iDRAC6 n'est pas lancé et vous êtes redirigé vers la page d'IUG de configuration de la console/ du média. |
| Paramètres d'URL inconnus détectés | L'URL que vous avez saisie contient des paramètres non définis. | Le message Page introuvable (404) s'affiche. |

# Questions les plus fréquentes concernant la console virtuelle

Le Tableau 9-7 répertorie les questions les plus fréquentes et les réponses correspondantes.

**Tableau 9-7. Utilisation de la console virtuelle : Questions les plus fréquentes**

| Question | Réponse |
|---|---|
| La console virtuelle ne se déconnecte pas lors de la fermeture de la session de l'IUG Web hors bande. | Les sessions Console virtuelle et Média virtuel restent actives même si la session Web a été fermée. Fermez les applications du visualiseur du média virtuel et de la console virtuelle afin de vous déconnecter de la session correspondante. |
| Est-ce qu'une nouvelle session vidéo de la console distante peut être démarrée lorsque la vidéo locale sur le serveur est désactivée ? | Oui. |

**Tableau 9-7. Utilisation de la console virtuelle : Questions les plus fréquentes *(suite)***

| Question | Réponse |
|---|---|
| Pourquoi la vidéo locale sur le serveur prend-elle 15 secondes pour être désactivée après une requête pour la désactiver ? | Ceci permet à l'utilisateur local d'agir avant que la vidéo ne soit désactivée. |
| Est-ce qu'il y a un délai quand la vidéo locale est activée ? | Non, une fois la requête d'**activation** de la vidéo locale reçue par iDRAC6, la vidéo est activée instantanément. |
| Est-ce que l'utilisateur local peut également désactiver la vidéo ? | Lorsque la console locale est désactivée, l'utilisateur local ne peut pas désactiver la vidéo. |
| Est-ce que l'utilisateur local peut également activer la vidéo ? | Lorsque la console locale est désactivée, l'utilisateur local ne peut pas activer la vidéo. |
| La désactivation de la vidéo locale désactive-t-elle aussi le clavier et la souris locaux ? | Non |
| La désactivation de la console locale désactive-t-elle la vidéo sur la session de la console distante ? | Non, l'activation ou la désactivation de la vidéo locale est indépendante de la session de la console distante. |
| Quels sont les privilèges nécessaires à un utilisateur iDRAC6 pour activer ou désactiver la vidéo locale du serveur ? | Tout utilisateur disposant de privilèges de configuration iDRAC6 peut activer ou désactiver la console locale. |
| Comment connaître la condition actuelle de la vidéo locale du serveur ? | La condition est affichée sur la page **Configuration de la console virtuelle** de l'interface Web iDRAC6.<br>La commande CLI RACADM `racadm getconfig -g cfgRacTuning` affiche la condition dans l'objet **cfgRacTuneLocalServerVideo**. |
| Je n'arrive pas à voir le bas de l'écran système à partir de la fenêtre Console virtuelle. | Assurez-vous que la résolution du moniteur de la station de gestion est définie sur 1280 x 1024. Essayez également d'utiliser les barres de défilement du client Console virtuelle iDRAC6. |

**Tableau 9-7. Utilisation de la console virtuelle : Questions les plus fréquentes *(suite)***

| Question | Réponse |
|---|---|
| La fenêtre de la console est tronquée. | Le visualiseur de console sous Linux requiert un jeu de caractères UTF-8. Vérifiez vos paramètres régionaux et réinitialisez le jeu de caractères si nécessaire. |
| Pourquoi la souris ne se synchronise-t-elle pas sous la console de texte Linux dans Dell Unified Server Configurator (USC), Dell Lifecycle Controller ou Dell Unified Server Configurator Lifecycle Controller Enabled (USC-LCE) ? | La console virtuelle requiert le pilote de souris USB, mais le pilote de souris USB est disponible uniquement sous le système d'exploitation X-Window. |
| J'ai toujours des problèmes avec la synchronisation de la souris. | Assurez-vous que la souris appropriée est sélectionnée pour votre système d'exploitation avant de démarrer une session Console virtuelle.<br><br>Vérifiez que l'option **Curseur unique sous Outils** dans le menu Console virtuelle iDRAC6 est sélectionnée sur le client Console virtuelle iDRAC6. Le mode à deux curseurs est défini par défaut. |
| Je ne peux pas utiliser de clavier ou de souris lorsque j'installe un système d'exploitation Microsoft à distance à l'aide de la console virtuelle iDRAC6. Pourquoi ? | Lorsque vous installez à distance un système d'exploitation Microsoft pris en charge sur un système sur lequel la console virtuelle est activée dans le BIOS, vous recevez un message de connexion EMS qui vous demande de sélectionner **OK** pour pouvoir continuer. Vous ne pouvez pas utiliser la souris pour sélectionner **OK** à distance. Vous devez sélectionner **OK** sur le système local ou redémarrer le serveur géré à distance, réinstaller puis désactiver la console virtuelle dans le BIOS.<br><br>Ce message est généré par Microsoft pour avertir l'utilisateur que la console virtuelle est activée. Pour que ce message n'apparaisse pas, désactivez toujours la console virtuelle dans le BIOS avant d'installer un système d'exploitation à distance. |

**Tableau 9-7. Utilisation de la console virtuelle : Questions les plus fréquentes *(suite)***

| Question | Réponse |
|---|---|
| Pourquoi l'indicateur Verr Num sur ma station de gestion ne reflète-t-il pas la condition Verr Num sur le serveur distant ? | Lors d'un accès via iDRAC6, l'indicateur Verr Num sur la station de gestion ne correspond pas nécessairement à l'état Verr Num sur le serveur distant. L'état Verr Num dépend du paramètre sur le serveur distant lorsque la session à distance est ouverte et ne tient pas compte de l'état Verr Num sur la station de gestion. |
| Pourquoi plusieurs fenêtres Session Viewer apparaissent-elles lorsque j'établis une session Console virtuelle à partir de l'hôte local ? | Vous configurez une session Console virtuelle à partir du système local. Cette opération n'est pas prise en charge. |
| Si j'exécute une session Console virtuelle et qu'un utilisateur local accède au serveur géré, est-ce que je reçois un message d'avertissement ? | Non Si un utilisateur local accède au système, vous contrôlez tous deux le système. |
| Quelle est la bande passante nécessaire pour exécuter une session Console virtuelle ? | Il est recommandé de recourir à une connexion de 5 Mo/s. pour des performances optimales. Une connexion de 1 Mo/s suffit pour une performance minimale. |
| Quelle est la configuration système minimale requise pour que ma station de gestion puisse exécuter la console virtuelle ? | La station de gestion nécessite un processeur Intel Pentium III 500 MHz avec au moins 256 Mo de mémoire RAM. |
| Pourquoi est-ce qu'un message **Aucun signal** s'affiche dans Video Viewer Console virtuelle iDRAC6 ? | Ce message peut s'afficher lorsque le plug-in Console virtuelle iDRAC6 ne reçoit pas la vidéo du bureau du serveur distant. En règle générale, cette situation a lieu lorsque le serveur distant est éteint. Parfois, le message peut s'afficher en raison de problèmes de réception de la vidéo du bureau du serveur distant. |

**Tableau 9-7. Utilisation de la console virtuelle : Questions les plus fréquentes *(suite)***

| Question | Réponse |
|---|---|
| Pourquoi est-ce qu'un message **Hors plage** s'affiche dans le Video Viewer Console virtuelle iDRAC6 ? | Ce message peut s'afficher si un paramètre nécessaire à la capture de la vidéo se situe au-delà de la plage dans laquelle iDRAC6 peut capturer la vidéo. Des paramètres tels que la résolution de l'affichage ou un taux de rafraîchissement trop élevés peuvent entraîner une condition hors plage. En règle générale, la plage maximale des paramètres est définie par des limitations physiques telles que la taille de la mémoire vidéo ou la bande passante. |

# 10

# Utilisation de l'interface WS-MAN

Web Services for Management (WS–MAN) est un protocole SOAP (Simple Object Access Protocol - Protocole simple d'accès aux objets) utilisé à des fins de gestion de systèmes. WS–MAN fournit un protocole interopérable permettant aux périphériques de partager et d'échanger des données sur des réseaux. iDRAC6 utilise WS–MAN pour transmettre des informations de gestion basées sur le modèle CIM (modèle commun d'informations) de DMTF (Distributed Management Task Force) ; les informations CIM définissent les sémantiques et les types d'informations qui peuvent être manipulées au sein d'un système géré. Les interfaces de gestion de plateformes de serveurs intégrées Dell sont articulées autour de profils, chacun définissant les interfaces spécifiques pour un domaine de gestion ou de fonctionnalité donné. Dell a, par ailleurs, défini un certain nombre d'extensions de modèles et de profils qui fournissent des interfaces pour des fonctions supplémentaires.

Les données disponibles par le biais de WS-MAN sont fournies par l'interface d'instrumentation iDRAC6 mappée sur les profils DMTF et profils d'extension Dell suivants :

## Profils CIM pris en charge

**Tableau 10-1. DMTF standard**

| DMTF standard |
|---|
| **1** Serveur de base<br>Définit les classes CIM pour la représentation du serveur hôte. |
| **2** Processeur de service :<br>Contient la définition des classes CIM pour la représentation d'iDRAC6. |
| **3** Bien physique :<br>Définit les classes CIM pour la représentation de l'aspect physique des éléments gérés. iDRAC6 utilise ce profil pour représenter les informations FRU du serveur hôte. |

**Tableau 10-1. DMTF standard *(suite)***

| DMTF standard |
|---|
| **4** Domaine d'administration SM-CLP<br>Définit les classes CIM pour la représentation de la configuration de CLP. iDRAC6 utilise ce profil pour sa propre implémentation de CLP. |
| **5** Gestion de l'état de l'alimentation<br>Définit les classes CIM?pour les opérations de contrôle de l'alimentation. iDRAC6 utilise ce profil pour les opérations de contrôle de l'alimentation du serveur hôte. |
| **6** Bloc d'alimentation (version 1.1)<br>Définit les classes CIM pour la représentation des blocs d'alimentation. iDRAC6 utilise ce profil pour représenter les blocs d'alimentation du serveur hôte afin de décrire la consommation énergétique, par exemple les filigranes de consommation énergétique élevée ou basse. |
| **7** Service CLP<br>Définit les classes CIM pour la représentation de la configuration de CLP. iDRAC6 utilise ce profil pour sa propre implémentation de CLP. |
| **8** Interface IP |
| **9** Client DHCP |
| **10** Client DNS |
| **11** Port Ethernet<br>Les profils ci-dessus définissent les classes CIM pour la représentation des piles réseau. iDRAC6 utilise ces profils pour représenter la configuration du NIC d'iDRAC6. |
| **12** Journal des enregistrements<br>Définit les classes CIM pour la représentation de différents types de journal. iDRAC6 utilise ce profil pour représenter le journal des événements système (SEL) et le journal du RAC iDRAC6. |
| **13** Inventaire des logiciels<br>Définit les classes CIM pour faire l'inventaire des logiciels installés ou disponibles. iDRAC6 utilise ce profil pour faire l'inventaire des versions du micrologiciel iDRAC6 actuellement installées via le protocole TFTP. |
| **14** Autorisation basée sur les rôles<br>Définit les classes CIM pour la représentation des rôles. iDRAC6 utilise ce profil pour configurer les privilèges de compte iDRAC6. |

**Tableau 10-1. DMTF standard *(suite)***

| DMTF standard |
|---|
| **15** Mise à jour de logiciels<br>Définit les classes CIM pour faire l'inventaire des mises à jour de logiciels disponibles. iDRAC6 utilise ce profil pour faire l'inventaire des mises à jour du micrologiciel via le protocole TFTP. |
| **16** Recueil SMASH<br>Définit les classes CIM pour la représentation de la configuration de CLP. iDRAC6 utilise ce profil pour sa propre implémentation de CLP. |
| **17** Enregistrement des profils<br>Définit les classes CIM pour l'annonce des implémentations des profils. iDRAC6 utilise ce profil pour annoncer ses propres profils implémentés, comme l'indique ce tableau. |
| **18** Mesures de base<br>Définit les classes CIM pour la représentation des mesures. iDRAC6 utilise ce profil pour représenter les mesures du serveur hôte afin de décrire la consommation énergétique, tels que les filigranes de consommation énergétique élevée ou basse. |
| **19** Gestion simple des identités<br>Définit les classes CIM pour la représentation des identités. iDRAC6 utilise ce profil pour configurer les comptes iDRAC6. |
| **20** Redirection USB<br>Définit les classes CIM pour la représentation de la redirection à distance des ports USB locaux. iDRAC6 utilise ce profil en concomitance avec le profil de média virtuel pour configurer le média virtuel. |

**Tableau 10-1. DMTF standard *(suite)***

| Extensions Dell |
| --- |
| **1** Dell Active Directory Client version 2.0.0<br>Définit les classes d'extension CIM et Dell pour configurer le client Active Directory iDRAC6 et les privilèges locaux pour les groupes Active Directory. |
| **2** Média virtuel Dell<br>Définit les classes d'extension CIM et Dell pour la configuration du média virtuel iDRAC6. Étend le profil de redirection USB. |
| **3** Port Ethernet Dell<br>Définit les classes d'extension CIM et Dell pour la configuration de l'interface bande latérale NIC pour le NIC d'iDRAC6. Étend le profil du port Ethernet. |
| **4** Gestion de l'utilisation de l'alimentation Dell<br>Définit les classes d'extension CIM et Dell pour la représentation du bilan de puissance du serveur hôte et pour la configuration/surveillance du bilan de puissance du serveur hôte. |
| **5** Déploiement du SE Dell<br>Définit les classes d'extension CIM et Dell pour la représentation de la configuration des fonctionnalités de déploiement du SE. Il étend les capacités de gestion des profils de référencement en ajoutant la capacité de prise en charge des activités de déploiement du SE en manipulant les fonctionnalités de déploiement du SE offertes par le processeur de service. |
| **6** Contrôle de tâche Dell<br>Définit les classes d'extension CIM et Dell pour la gestion des tâches de configuration. |
| **7** Profil de gestion Dell LC<br>Définit les classes d'extension CIM et Dell pour les attributs de configuration de Dell Lifecycle Controller, comme la détection automatique. Ce profil permet également de gérer les pièces de rechange, le remplacement de la carte mère, l'exportation et l'importation du profil du système, l'amorçage depuis un partage réseau et la gestion des certificats de cryptage. |
| **8** Stockage permanent Dell<br>Définit les classes d'extension CIM et Dell pour la gestion des partitions sur la carte SD vFlash des plates-formes Dell. |
| **9** NIC simple Dell<br>Définit les classes d'extension CIM et Dell pour représenter la configuration des contrôleurs réseau de NIC. |

**Tableau 10-1. DMTF standard *(suite)***

| Extensions Dell |
| --- |
| **10** Profil de gestion du démarrage et du BIOS de Dell<br>Définit les classes d'extension CIM et Dell pour représenter les attributs du BIOS de Dell et pour configurer la séquence d'amorçage de l'hôte. |
| **11** Profil RAID Dell<br>Définit les classes d'extension CIM et Dell pour représenter la configuration du stockage RAID de l'hôte. |
| **12** Profil du bloc d'alimentation Dell<br>Définit les classes d'extension CIM et Dell pour représenter les informations d'inventaire du bloc d'alimentation de l'hôte. |
| **13** Profil de la carte iDRAC Dell<br>Définit les classes d'extension CIM et Dell pour représenter les informations d'inventaire d'iDRAC6. Ce profil permet également de représenter les attributs iDRAC et les comptes utilisateur et offre des méthodes de configuration pour ces derniers. |
| **14** Profil du ventilateur Dell<br>Définit les classes d'extension CIM et Dell pour représenter les informations d'inventaire du ventilateur de l'hôte. |
| **15** Profil de la mémoire Dell<br>Définit les classes d'extension CIM et Dell pour représenter les informations d'inventaire DIMM de l'hôte. |
| **16** Profil de l'UC Dell<br>Définit les classes d'extension CIM et Dell pour représenter les informations d'inventaire de l'UC de l'hôte. |
| **17** Profil des infos système Dell<br>Définit les classes d'extension CIM et Dell pour représenter les informations d'inventaire de la plateforme hôte. |
| **18** Profil du périphérique PCI Dell<br>Définit les classes d'extension CIM et Dell pour représenter les informations d'inventaire du périphérique PCI de l'hôte. |
| **19** Profil vidéo Dell<br>Définit les classes d'extension CIM et Dell pour représenter les informations d'inventaire de la carte vidéo de l'hôte. |

L'implémentation WS–MAN iDRAC6 utilise SSL sur le port 443 pour la sécurité du transport et prend en charge l'authentification de base et Digest. Les interfaces des services Web peuvent être utilisées en exploitant l'infrastructure client comme Windows WinRM et Powershell CLI, des utilitaires open source comme WSMANCLI, et des environnements de programmation d'applications comme Microsoft .NET.

Pour des informations supplémentaires sur les services distants du Dell Lifecycle Controller, consultez les documents suivants :

- Guide d'utilisation
- Notes de mise à jour
- Liste des messages d'erreur et des dépannages

Pour accéder à ces documents :

1. Rendez-vous sur **dell.com/support/manuals**.
2. Cliquez sur **Logiciel→ Gestion des systèmes→ Dell Unified Server Configurator et Lifecycle Controller**.
3. Cliquez sur la version pertinente pour afficher tous les documents correspondant à une version particulière.

Pour consulter des guides d'interface de services Web (Windows et Linux), des documents sur les profils, des exemples de codes, des documents techniques et accéder à d'autres informations utiles, naviguez sur **Gestion des systèmes OpenManage→ Lifecycle Controller** sur le site Web **delltechcenter.com**.

Pour plus d'informations, consultez :

- Le site Web de DMTF suivant : **dmtf.org/standards/profiles/**
- Les notes de diffusion ou le fichier « Lisez-moi » de WS–MAN.

# 11

# Utilisation de l'interface de ligne de commande SM-CLP iDRAC6

Cette section fournit des informations sur le protocole Server Management-Command Line Protocol (SM-CLP) de Distributed Management Task Force (DMTF) qui est incorporé dans iDRAC6.

**REMARQUE :** cette section suppose que vous connaissez l'initiative SMASH (Systems Management Architecture for Server Hardware) et les spécifications SM-CLP. Pour des informations supplémentaires sur ces spécifications, consultez le site Web de DMTF à l'adresse **dmtf.org**.

SM-CLP iDRAC6 est un protocole qui fournit des normes aux implémentations de la CLI de gestion de systèmes. SM-CLP est un sous-composant de l'initiative SMASH DMTF destinée à rationaliser la gestion de serveur sur des plateformes multiples. La spécification SM-CLP, conjointement à Managed Element Addressing Specification et à de nombreux profils de spécifications de mappage SM-CLP, décrit les verbes et les cibles normalisés pour les diverses exécutions de tâches de gestion.

## Prise en charge de SM-CLP iDRAC6

SM-CLP est hébergé par le micrologiciel du contrôleur iDRAC6 et prend en charge les interfaces Telnet, SSH et série. L'interface SM-CLP iDRAC6 est basée sur la spécification SM-CLP, version 1.0, fournie par l'organisation DMTF. L'interface SM-CLP iDRAC6 prend en charge tous les profils décrits dans le Tableau 10-1.

Les sections suivantes fournissent un aperçu de la fonctionnalité SM-CLP hébergée par iDRAC6.

# Fonctionnalités de SM-CLP

SM-CLP encourage la conception de verbes et de cibles pour fournir des capacités de gestion de systèmes via la CLI. Le verbe indique l'opération à effectuer et la cible détermine l'entité (ou l'objet) qui exécute l'opération.

Voir l'exemple de syntaxe de la ligne de commande SM-CLP ci-dessous.

```
<verbe> [<options>] [<cible>] [<propriétés>]
```

Pendant une session SM-CLP type, vous pouvez effectuer des opérations à l'aide des verbes énumérés dans le Tableau 11-1.

**Tableau 11-1. Verbes de la CLI pris en charge pour le système**

| Verbe | Définition |
|---|---|
| cd | Navigue dans MAP à l'aide de l'environnement |
| set | Définit une propriété sur une valeur spécifique |
| help | Affiche l'aide pour une cible spécifique |
| reset | Réinitialise la cible |
| show | Affiche les propriétés, les verbes et les sous-cibles de la cible |
| démarrage | Active une cible |
| stop | Arrête une cible |
| exit | Quitte la session d'environnement SM-CLP |
| version | Affiche les attributs de version d'une cible |
| load | Déplace une image binaire d'une URL vers une adresse cible spécifiée |

## Utilisation de SM-CLP

SSH (ou Telnet) vers iDRAC6 avec les bonnes références.

L'invite SMCLP (/admin1->) est affichée.

## Cibles SM-CLP

Le Tableau 11-2 donne une liste des cibles fournies par SM-CLP pour prendre en charge les opérations décrites dans le Tableau 11-1 ci-dessus.

**Tableau 11-2. Cibles SM-CLP**

| Cible | Définitions |
|---|---|
| admin1 | domaine admin |
| admin1/profiles1 | Profils enregistrés dans iDRAC6 |
| admin1/hdwr1 | Matériel |
| admin1/system1 | Cible du système géré |
| admin1/system1/redundancyset1 | Bloc d'alimentation |
| admin1/system1/redundancyset1/ pwrsupply* | Bloc d'alimentation du système géré |
| admin1/system1/sensors1 | Capteurs du système géré |
| admin1/system1/capabilities1 | Capacités de recueil SMASH du système géré |
| admin1/system1/capabilities1/ pwrcap1 | Capacités d'utilisation de l'alimentation du système géré |
| admin1/system1/capabilities1/ elecap1 | Capacités de cible du système géré |
| admin1/system1/logs1 | Cible des recueils du journal des enregistrements |
| admin1/system1/logs1/log1 | Entrée d'enregistrement du journal d'événements système (SEL) |
| admin1/system1/logs1/log1/ record* | Instance d'enregistrement SEL individuelle sur le système géré |
| admin1/system1/settings1 | Paramètres de recueil SMASH du système géré |
| admin1/system1/settings1/ pwrmaxsetting1 | Paramètre d'allocation de puissance maximale du système géré |
| admin1/system1/settings1/ pwrminsetting1 | Paramètre d'allocation de puissance minimale du système géré |
| admin1/system1/capacities1 | Recueil SMASH des capacités du système géré |

**Tableau 11-2. Cibles SM-CLP *(suite)***

| Cible | Définitions |
|---|---|
| admin1/system1/consoles1 | Recueil SMASH des consoles du système géré |
| admin1/system1/usbredirectsap1 | SAP de redirection USB du média virtuel |
| admin1/system1/usbredirectsap1/remotesap1 | SAP de redirection USB de destination du média virtuel |
| admin1/system1/sp1 | Processeur de service |
| admin1/system1/sp1/timesvc1 | Service de temps du processeur de service |
| admin1/system1/sp1/capabilities1 | Recueil SMASH des capacités du processeur de service |
| admin1/system1/sp1/capabilities1/clpcap1 | Capacités de service CLP |
| admin1/system1/sp1/capabilities1/pwrmgtcap1 | Capacités de service de gestion de l'état de l'alimentation sur le système |
| admin1/system1/sp1/capabilities1/ipcap1 | Capacités d'interface IP |
| admin1/system1/sp1/capabilities1/dhcpcap1 | Capacités de client DHCP |
| admin1/system1/sp1/capabilities1/NetPortCfgcap1 | Capacités de configuration de port réseau |
| admin1/system1/sp1/capabilities1/usbredirectcap1 | SAP de redirection USB des capacités de média virtuel |
| admin1/system1/sp1/capabilities1/vmsapcap1 | Capacités SAP de média virtuel |
| admin1/system1/sp1/capabilities1/swinstallsvccap1 | Capacités de service d'installation de logiciel |
| admin1/system1/sp1/capabilities1/acctmgtcap* | Capacités de service de gestion de comptes |
| admin1/system1/sp1/capabilities1/adcap1 | Capacités Active Directory |

**Tableau 11-2. Cibles SM-CLP *(suite)***

| Cible | Définitions |
|---|---|
| admin1/system1/sp1/capabilities1/rolemgtcap* | Capacités de gestion basée sur les rôles locaux |
| admin1/system1/sp1/capabilities/PwrutilmgtCap1 | Capacités de gestion de l'utilisation de l'alimentation |
| admin1/system1/sp1/capabilities/metriccap1 | Capacités de service de mesure |
| admin1/system1/sp1/capabilities1/elecap1 | Capacités d'authentification multifacteurs |
| admin1/system1/sp1/capabilities1/lanendptcap1 | Capacités de terminaison LAN (port Ethernet) |
| admin1/system1/sp1/logs1 | Recueil des journaux du processeur de service |
| admin1/system1/sp1/logs1/log1 | Journal des enregistrements système |
| admin1/system1/sp1/logs1/log1/record* | Entrée du journal système |
| admin1/system1/sp1/settings1 | Recueil des paramètres du processeur de service |
| admin1/system1/sp1/settings1/clpsetting1 | Données des paramètres de service CLP |
| admin1/system1/sp1/settings1/ipsettings1 | Données des paramètres d'affectation d'interface IP (statique) |
| admin1/system1/sp1/settings1/ipsettings1/staticipsettings1 | Données des paramètres d'affectation d'interface IP statique |
| admin1/system1/sp1/settings1/ipsettings1/dnssettings1 | Données des paramètres du client DNS |
| admin1/system1/sp1/settings1/ipsettings2 | Données des paramètres d'affectation d'interface IP (DHCP) |
| admin1/system1/sp1/settings1/ipsettings2/dhcpsettings1 | Données des paramètres du client DHCP |
| admin1/system1/sp1/clpsvc1 | Service de protocole de service CLP |

**Tableau 11-2. Cibles SM-CLP *(suite)***

| Cible | Définitions |
|---|---|
| admin1/system1/sp1/clpsvc1/ clpendpt* | Terminaison de protocole de service CLP |
| admin1/system1/sp1/clpsvc1/ tcpendpt* | Terminaison TCP de protocole de service CLP |
| admin1/system1/sp1/jobq1 | File d'attente de tâches de protocole de service CLP |
| admin1/system1/sp1/jobq1/job* | Tâche de protocole de service CLP |
| admin1/system1/sp1/pwrmgtsvc1 | Service de gestion de l'état de l'alimentation |
| admin1/system1/sp1/ipcfgsvc1 | Service de configuration d'interface IP |
| admin1/system1/sp1/ipendpt1 | Terminaison de protocole d'interface IP |
| admin1/system1/sp1/ ipendpt1/gateway1 | Passerelle d'interface IP |
| admin1/system1/sp1/ ipendpt1/dhcpendpt1 | Terminaison de protocole de client DHCP |
| admin1/system1/sp1/ ipendpt1/dnsendpt1 | Terminaison de protocole de client DNS |
| admin1/system1/sp1/ipendpt1/ dnsendpt1/dnsserver* | Serveur client DNS |
| admin1/system1/sp1/NetPortCfgsvc1 | Service de configuration de port réseau |
| admin1/system1/sp1/lanendpt1 | Terminaison LAN |
| admin1/system1/sp1/ lanendpt1/enetport1 | Port Ethernet |
| admin1/system1/sp1/VMediaSvc1 | Service de média virtuel |
| admin1/system1/sp1/ VMediaSvc1/tcpendpt1 | Terminaison de protocole TCP de média virtuel |
| admin1/system1/sp1/swid1 | Identité de logiciel |
| admin1/system1/sp1/ swinstallsvc1 | Service d'installation de logiciel |

**Tableau 11-2. Cibles SM-CLP *(suite)***

| Cible | Définitions |
|---|---|
| admin1/system1/sp1/ account1-16 | Compte d'authentification multifacteurs (MFA) |
| admin1/sysetm1/sp1/ account1-16/identity1 | Compte d'identité d'utilisateur local |
| admin1/sysetm1/sp1/ account1-16/identity2 | Compte d'identité IPMI (LAN) |
| admin1/sysetm1/sp1/ account1-16/identity3 | Compte d'identité IPMI (série) |
| admin1/sysetm1/sp1/ account1-16/identity4 | Compte d'identité CLP |
| admin1/system1/sp1/acctsvc1 | Service de gestion de compte MFA |
| admin1/system1/sp1/acctsvc2 | Service de gestion de compte IPMI |
| admin1/system1/sp1/acctsvc3 | Service de gestion de compte CLP |
| admin1/system1/sp1/group1-5 | Groupe Active Directory |
| admin1/system1/sp1/ group1-5/identity1 | Identité Active Directory |
| admin1/system1/sp1/ADSvc1 | Service Active Directory |
| admin1/system1/sp1/rolesvc1 | Service d'autorisation basée sur les rôles (RBA) locaux |
| admin1/system1/sp1/rolesvc1/ Role1-16 | Rôle local |
| admin1/system1/sp1/rolesvc1/ Role1-16/privilege1 | Privilège de rôle local |
| admin1/system1/sp1/rolesvc1/ Role17-21/ | Rôle Active Directory |
| admin1/system1/sp1/rolesvc1/ Role17-21/privilege1 | Privilège Active Directory |
| admin1/system1/sp1/rolesvc2 | Service RBA IPMI |
| admin1/system1/sp1/rolesvc2/ Role1-3 | Rôle IPMI |
| admin1/system1/sp1/rolesvc2/ Role4 | Rôle série sur LAN (SOL) IPMI |

**Tableau 11-2. Cibles SM-CLP *(suite)***

| Cible | Définitions |
|---|---|
| admin1/system1/sp1/rolesvc3 | Service RBA CLP |
| admin1/system1/sp1/rolesvc3/ Role1-3 | Rôle CLP |
| admin1/system1/sp1/rolesvc3/ Role1-3/privilege1 | Privilège de rôle CLP |
| admin1/system1/sp1/ pwrutilmgtsvc1 | Service de gestion de l'utilisation de l'alimentation |
| admin1/system1/sp1/ pwrutilmgtsvc1/pwrcurr1 | Données des paramètres d'allocation de l'alimentation actuelle du service de gestion de l'utilisation de l'alimentation |
| admin1/system1/sp1/metricsvc1 | Service de mesure |
| admin1/system1/sp1/metricsvc1/ cumbmd1 | Définition de la mesure de base cumulée |
| /admin1/system1/sp1/metricsvc1/ cumbmd1/cumbmv1 | Valeur de la mesure de base cumulée |
| /admin1/system1/sp1/metricsvc1/ cumwattamd1 | Définition de la mesure de l'agrégation de la puissance cumulée en watts |
| /admin1/system1/sp1/metricsvc1/ cumwattamd1/cumwattamv1 | Valeur de la mesure de l'agrégation de la puissance cumulée en watts |
| /admin1/system1/sp1/metricsvc1/ cumampamd1 | Définition de la mesure de l'agrégation de la puissance cumulée en ampères |
| /admin1/system1/sp1/metricsvc1/ cumampamd1/cumampamv1 | Valeur de la mesure de l'agrégation de la puissance cumulée en ampères |
| /admin1/system1/sp1/metricsvc1/ loamd1 | Définition de la mesure de l'agrégation de la consommation basse |
| /admin1/system1/sp1/metricsvc1/ loamd1/loamv* | Valeur de la mesure de l'agrégation de la consommation basse |

**Tableau 11-2. Cibles SM-CLP *(suite)***

| Cible | Définitions |
|---|---|
| /admin1/system1/sp1/metricsvc1/hiamd1 | Définition de la mesure de l'agrégation de la consommation élevée |
| /admin1/system1/sp1/metricsvc1/hiamd1/hiamv* | Valeur de la mesure de l'agrégation de la consommation élevée |
| /admin1/system1/sp1/metricsvc1/avgamd1 | Définition de la mesure de l'agrégation de la consommation moyenne |
| /admin1/system1/sp1/metricsvc1/avgamd1/avgamv* | Valeur de la mesure de l'agrégation de la consommation moyenne |

# 12

# Déploiement de votre système d'exploitation en utilisant VMCLI

L'utilitaire VMCLI (Virtual Media Command Line Interface) est une interface de ligne de commande qui fournit les fonctionnalités de média virtuel de la station de gestion à iDRAC6 dans le système distant. À l'aide de VMCLI et de méthodes avec script, vous pouvez déployer votre système d'exploitation sur plusieurs systèmes distants au sein de votre réseau.

Cette section fournit des informations sur l'intégration de l'utilitaire VMCLI dans votre réseau d'entreprise.

## Avant de commencer

Avant d'utiliser l'utilitaire VMCLI, assurez-vous que vos systèmes distants cibles et votre réseau d'entreprise répondent aux exigences mentionnées dans les sections suivantes.

### Exigences du système distant

iDRAC6 est configuré dans chaque système distant.

### Configuration réseau requise

Un partage réseau doit comprendre les composants suivants :

- Fichiers de système d'exploitation
- Pilotes requis
- Fichier(s) image de démarrage du système d'exploitation

  Le fichier image doit être une image de CD de système d'exploitation ou une image ISO de CD/DVD avec un format de démarrage standard.

# Création d'un fichier image de démarrage

Avant de déployer votre fichier image sur les systèmes distants, assurez-vous qu'un système pris en charge peut être démarré à partir du fichier. Pour tester le fichier image, transférez-le vers un système test à l'aide de l'interface utilisateur Web iDRAC6, puis redémarrez le système.

Les sections suivantes fournissent des informations spécifiques pour créer des fichiers image pour les systèmes Linux et Microsoft Windows.

### Création d'un fichier image pour les systèmes Linux

Utilisez l'utilitaire de duplicateur de données (dd) pour créer un fichier image d'amorçage pour votre système Linux.

Pour exécuter l'utilitaire, ouvrez une invite de commande et tapez les commandes suivantes :

```
dd if=<périphérique_d'entrée> of=<fichier_de_sortie>
```

Par exemple :

```
dd if=/dev/sdc0 of=mycd.img
```

### Création d'un fichier image pour les systèmes Windows

Lorsque vous choisissez un utilitaire de réplicateur de données pour les fichiers image Windows, sélectionnez un utilitaire qui copie le fichier image et les secteurs de démarrage de CD/DVD.

# Préparation au déploiement

### Configuration des systèmes distants

1. Créez un partage réseau qui puisse être accessible par la station de gestion.
2. Copiez les fichiers de système d'exploitation sur le partage réseau.
3. Si vous avez un fichier image de déploiement de démarrage préconfiguré pour déployer le système d'exploitation sur les systèmes distants, ignorez cette étape.

   Si vous n'avez pas de fichier image de déploiement de démarrage préconfiguré, créez-le. Incluez les programmes et/ou les scripts utilisés pour les procédures de déploiement de système d'exploitation.

Par exemple, pour déployer un système d'exploitation Windows, le fichier image peut inclure des programmes qui sont semblables aux méthodes de déploiement utilisées par Microsoft Systems Management Server (SMS).

Pour créer le fichier image, procédez comme suit :

- Suivez les procédures d'installation réseau standard
- Marquez l'image de déploiement en *lecture seule* pour garantir que chaque système cible démarre et exécute la même procédure de déploiement

4 Effectuez l'une des procédures suivantes :

- Intégrez **IPMItool** et VMCLI dans votre application de déploiement de système d'exploitation existante. Utilisez l'exemple de script **vm6deploy** comme guide d'utilisation de l'utilitaire.
- Utilisez le script **vm6deploy** existant pour déployer votre système d'exploitation.

# Déploiement du système d'exploitation

Utilisez l'utilitaire VMCLI et le script **vm6deploy** inclus avec l'utilitaire pour déployer le système d'exploitation sur vos systèmes distants.

Avant de commencer, vérifiez l'exemple de script **vm6deploy** inclus avec l'utilitaire VMCLI. Le script affiche les étapes détaillées requises pour déployer le système d'exploitation sur les systèmes distants de votre réseau.

La procédure suivante fournit un aperçu de haut niveau du déploiement du système d'exploitation sur les systèmes distants ciblés.

1 Répertoriez les adresses IPv4 ou IPv6 iDRAC6 des systèmes distants qui seront déployées dans le fichier texte **ip.txt**, en indiquant une seule adresse IPv4 ou IPv6 par ligne.

2 Insérez un CD ou un DVD de système d'exploitation de démarrage dans le lecteur de média client.

3 Exécutez **vm6deploy** à la ligne de commande.

Pour exécuter le script **vm6deploy**, entrez la commande suivante à l'invite de commande :

```
vm6deploy -r ip.txt -u <utilisateur_idrac> -p
<mot_de_passe_utilisateur_idrac> -c {<image-iso9660>
| <chemin>} -f {<lecteur_de_disquette> ou
<image_de_disquette>}
```

où :

- <*utilisateur_idrac*> est le nom d'utilisateur iDRAC6, par exemple **root**
- <*mot_de_passe_utilisateur_idrac*> est le mot de passe de l'utilisateur iDRAC6, par exemple **calvin**
- <*image-iso9660*> est le chemin d'une image ISO9660 du CD ou du DVD d'installation du système d'exploitation
- -f {<*lecteur_de_disquette*>} est le chemin du périphérique contenant le CD, le DVD ou la disquette d'installation du système d'exploitation
- <*image_de_disquette*> est le chemin d'une image de disquette valide

Le script **vm6deploy** transmet ses options de ligne de commande à l'utilitaire **VMCLI**. Consultez « Options de ligne de commande » pour obtenir des détails sur ces options. Le script traite l'option **-r** de manière légèrement différente de l'option **vmcli -r**. Si l'argument de l'option **-r** est le nom d'un fichier existant, le script lit les adresses IPv4 ou IPv6 iDRAC6 du fichier spécifié et exécute l'utilitaire **VMCLI** une fois pour chaque ligne. Si l'argument de l'option **-r** n'est pas un nom de fichier, il doit correspondre à l'adresse d'un iDRAC6 unique. Dans ce cas, l'option **-r** fonctionne comme décrit pour l'utilitaire **VMCLI**.

# Utilisation de l'utilitaire VMCLI

L'utilitaire VMCLI est une interface de ligne de commande scriptable qui fournit les fonctionnalités de média virtuel de la station de gestion à iDRAC6.

L'utilitaire VMCLI fournit les fonctionnalités suivantes :

**REMARQUE :** Lors de la virtualisation de fichiers image en lecture seule, plusieurs sessions peuvent partager le même média image. Lors de la virtualisation de lecteurs physiques, une seule session peut accéder à un lecteur physique donné à la fois.

- Les périphériques de média amovibles ou les fichiers image qui sont en accord avec les plug-in du média virtuel.
- L'arrêt automatique lorsque l'option démarrer une seule fois du micrologiciel iDRAC6 est activée
- Les communications sécurisées avec iDRAC6 à l'aide du protocole Secure Sockets Layer (SSL)

Avant d'exécuter l'utilitaire, assurez-vous que vous disposez des privilèges utilisateur de média virtuel pour iDRAC6.

**PRÉCAUTION : il est recommandé d'utiliser l'option « -i » d'indicateur interactif au démarrage de l'utilitaire de la ligne de commande VMCLI. Ceci permet de garantir une sécurité plus poussée en préservant la confidentialité du nom d'utilisateur et du mot de passe, car sur de nombreux systèmes d'exploitation Windows et Linux, le nom d'utilisateur et le mot de passe sont visibles lorsque les processus sont examinés par d'autres utilisateurs.**

Si votre système d'exploitation prend en charge des privilèges Administrateur ou un privilège spécifique au système d'exploitation ou une appartenance au groupe, les privilèges Administrateur sont également requis pour exécuter la commande VMCLI.

L'administrateur du système client contrôle les groupes et les privilèges d'utilisateurs, contrôlant ainsi les utilisateurs qui peuvent exécuter l'utilitaire.

Pour les systèmes Windows, vous devez disposer des privilèges Utilisateur privilégié pour pouvoir exécuter l'utilitaire VMCLI.

Pour les systèmes Linux, vous pouvez accéder à l'utilitaire VMCLI sans privilèges Administrateur en utilisant la commande **sudo**. Cette commande offre un moyen centralisé de fournir un accès non-administrateur et permet de journaliser toutes les commandes d'utilisateur. Pour ajouter ou modifier des utilisateurs dans le groupe VMCLI, l'administrateur utilise la commande **visudo**. Les utilisateurs sans privilèges Administrateur peuvent ajouter la commande **sudo** comme préfixe à la ligne de commande VMCLI (ou au script VMCLI) afin d'accéder à iDRAC6 dans le système distant et d'exécuter l'utilitaire.

## Installation de l'utilitaire VMCLI

L'utilitaire VMCLI se trouve sur le DVD *Dell Systems Management Tools and Documentation* qui est inclus avec votre kit logiciel Dell OpenManage System Management. Pour installer l'utilitaire, insérez le DVD *Dell Systems Management Tools and Documentation* dans le lecteur de DVD de votre système et suivez les instructions qui s'affichent à l'écran.

Le DVD *Dell Systems Management Tools and Documentation* contient les derniers produits Systems Management Software, notamment la gestion du stockage, le service d'accès à distance et l'utilitaire IPMItool. Ce DVD contient également des fichiers « Lisez-moi », qui fournissent les dernières informations sur les produits Systems Management Software.

Le DVD *Dell Systems Management Tools and Documentation* inclut **vm6deploy**, un exemple de script qui illustre l'utilisation des utilitaires VMCLI et IPMItool pour déployer le logiciel sur plusieurs systèmes distants.

**REMARQUE :** le script vm6deploy dépend des autres fichiers présents dans son répertoire lors de son installation. Si vous souhaitez utiliser le script à partir d'un autre répertoire, vous devez copier tous les fichiers avec ce script. Si l'utilitaire IPMItool n'est pas installé, l'utilitaire doit être copié en plus des autres fichiers.

## Options de ligne de commande

L'interface VMCLI est identique sur les systèmes Windows et Linux.

Le format d'une commande VMCLI est comme suit :

`VMCLI[paramètre] [options_ d'environnement_ de_système_d'exploitation]`

La syntaxe de ligne de commande est sensible à la casse. Pour en savoir plus, voir « Paramètres VMCLI », à la page 265.

Si le système distant accepte les commandes et si iDRAC6 autorise la connexion, la commande continue de s'exécuter jusqu'à ce qu'un des événements suivants se produise :

- La connexion VMCLI est interrompue pour une raison quelconque.
- Le processus est manuellement interrompu à l'aide d'une commande de système d'exploitation. Par exemple, sous Windows, vous pouvez utiliser le gestionnaire des tâches pour interrompre le processus.

## Paramètres VMCLI

### Adresse IP iDRAC6

`-r <adresse_IP_iDRAC[:port_SSL_iDRAC]>`

Ce paramètre fournit l'adresse IPv4 ou IPv6 iDRAC6 et le port SSL, dont l'utilitaire a besoin pour établir une connexion de média virtuel avec l'iDRAC6 cible. Si vous saisissez une adresse IPv4 ou IPv6 ou un nom DDNS non valide, un message d'erreur s'affiche et la commande se termine.

*<adresse_IP_iDRAC>* est une adresse IPv4 ou IPv6 unique valide ou le nom DDNS (Dynamic Domain Naming System) iDRAC6 (s'il est pris en charge). Si *<port_SSL_iDRAC>* est omis, le port 443 (port par défaut) est utilisé. Le port SSL optionnel n'est obligatoire que si vous modifiez le port SSL par défaut iDRAC6.

### Nom d'utilisateur iDRAC6

`-u <utilisateur_iDRAC>`

Ce paramètre fournit le nom d'utilisateur iDRAC6 qui exécutera le média virtuel.

*<utilisateur_iDRAC>* doit avoir les attributs suivants :

- Nom d'utilisateur valide
- Droit Utilisateur de média virtuel iDRAC6

Si l'authentification iDRAC6 échoue, un message d'erreur s'affiche et la commande se termine.

### Mot de passe d'utilisateur iDRAC6

`-p <mot_de-passe_d'utilisateur_iDRAC>`

Ce paramètre fournit le mot de passe de l'utilisateur iDRAC6 spécifié.

Si l'authentification iDRAC6 échoue, un message d'erreur s'affiche et la commande se termine.

**Périphérique de disquette/disque ou fichier image**

`-f {<périphérique_de_disquette> ou <image_de_disquette>}` et/ou

`-c {<périphérique_CD_DVD> ou <image_de_CD-DVD>}`

où `<`périphérique-de-disquette`>` ou `<périphérique_de_CD-DVD>` est une lettre de lecteur valide (pour les systèmes Windows) ou un nom de fichier de périphérique valide (pour les systèmes Linux), et `<image_de_disquette> ou <image_de_CD-DVD>` est le nom de fichier et le chemin d'un fichier image valide.

**REMARQUE :** les points de montage ne sont pas pris en charge pour l'utilitaire VMCLI.

Ce paramètre spécifie le périphérique ou le fichier qui fournit le média de disquette/disque virtuel.

Par exemple, un fichier image est spécifié comme :

`-f c:\temp\myfloppy.img` (système Windows)

`-f/tmp/myfloppy.img` (système Linux)

Si le fichier n'est pas protégé contre l'écriture, le média virtuel peut écrire sur le fichier image. Configurez le système d'exploitation pour protéger contre l'écriture un fichier image de disquette qui ne doit pas être écrasé.

Par exemple, un périphérique est spécifié comme :

`-f a:\` (système Windows)

`-f /dev/sdb4 # 4ème partition sur le périphérique /dev/sdb` (système Linux)

**REMARQUE :** Red Hat Enterprise Linux version 4 ne prend pas en charge les LUN multiples. Toutefois, le noyau prend en charge cette fonctionnalité. Permettez à Red Hat Enterprise Linux version 4 de reconnaître un périphérique SCSI doté de LUN multiples en procédant comme suit :

1. Modifiez **/etc/modprobe.conf** et ajoutez la ligne suivante :
   `options scsi_mod max_luns=8`
   (Vous pouvez spécifier 8 LUN ou n'importe quel nombre supérieur à 1.)
2. Récupérez le nom de l'image de noyau en tapant la commande suivante à la ligne de commande :

   `uname -r`

3 Allez dans le répertoire **/boot** et supprimez le fichier image de noyau dont vous avez déterminé le nom à l'étape 2 :

```
mkinitrd /boot/initrd-'uname -r'.img 'uname -r'
```

4 Redémarrez le serveur.

5 Exécutez la commande suivante pour confirmer que la prise en charge de LUN multiples a été ajoutée pour le nombre de LUN spécifié à l'étape 1 :

```
cat /sys/modules/scsi_mod/max_luns
```

Si le périphérique fournit une capacité de protection contre l'écriture, utilisez-la pour garantir que le média virtuel n'écrit pas sur le média.

Omettez ce paramètre de la ligne de commande si vous ne virtualisez pas le média de disquette. Si une valeur non valide est détectée, un message d'erreur s'affiche et la commande se termine.

#### Périphérique ou fichier image de CD/DVD

`-c {<nom_de_périphérique> | <fichier_image>}`

où <*nom_de_périphérique*> est une lettre de lecteur de CD/DVD valide (systèmes Windows) ou un nom de fichier de périphérique de CD/DVD valide (systèmes Linux), et <*fichier_image*> est le nom de fichier et le chemin d'un fichier image ISO-9660 valide.

Ce paramètre spécifie le périphérique ou le fichier qui fournit le média de CD/DVD-ROM virtuel :

Par exemple, un fichier image est spécifié comme :

`-c c:\temp\mydvd.img` (systèmes Windows)

`-c/tmp/mydvd.img` (systèmes Linux)

Par exemple, un périphérique est spécifié comme :

`-c d:\` (systèmes Microsoft Windows)

`-c/dev/cdrom` (systèmes Linux)

Omettez ce paramètre de la ligne de commande si vous ne virtualisez pas le média de CD/DVD. Si une valeur non valide est détectée, un message d'erreur s'affiche et la commande se termine.

Spécifiez au moins un type de média (lecteur de disquette ou de CD/DVD) avec la commande, à moins que seules des options de commutateur ne soient fournies. Sinon, un message d'erreur s'affiche et la commande se termine en générant une erreur.

#### Affichage de la version

`-v`

Ce paramètre est utilisé pour afficher la version de l'utilitaire VMCLI. Si aucune autre option de non-commutateur n'est fournie, la commande est interrompue sans message d'erreur.

#### Affichage de l'aide

`-h`

Ce paramètre permet d'afficher un résumé des paramètres de l'utilitaire VMCLI. Si aucune autre option de non-commutateur n'est fournie, la commande est interrompue sans erreur.

#### Données cryptées

`-e`

Lorsque ce paramètre est inclus dans la ligne de commande, VMCLI utilise un *canal crypté SSL* pour transférer des données entre la station de gestion et iDRAC6 dans le système distant. Si ce paramètre n'est pas inclus dans la ligne de commande, le transfert de données n'est pas crypté.

**REMARQUE :** l'utilisation de cette option ne modifie pas l'état affiché du cryptage de média virtuel sur *activé* dans les autres interfaces de configuration iDRAC6 comme RACADM ou l'interface Web.

### Options d'environnement de système d'exploitation VMCLI

Les fonctionnalités de système d'exploitation suivantes peuvent être utilisées sur la ligne de commande VMCLI :

- stderr/stdout redirection : redirige la sortie imprimée de l'utilitaire vers un fichier.

  Par exemple, le caractère plus grand que (>), suivi par un nom de fichier, écrase le fichier indiqué avec la sortie imprimée de l'utilitaire VMCLI.

  **REMARQUE :** l'utilitaire VMCLI ne lit pas à partir d'une entrée standard (**stdin**). Par conséquent, la redirection **stdin** n'est pas exigée.

- Exécution en arrière-plan : par défaut, l'utilitaire VMCLI s'exécute en avant-plan. Utilisez les fonctionnalités d'environnement de la commande du système d'exploitation pour exécuter l'utilitaire en arrière-plan. Par exemple, dans un système d'exploitation Linux, le caractère d'esperluette (&) qui suit la commande fait que le programme est engendré comme un nouveau processus en arrière-plan.

La dernière technique est utile dans les programmes de script, car elle permet au script de se poursuivre après le démarrage d'un nouveau processus pour la commande VMCLI (sinon, le script reste bloqué jusqu'à ce que le programme VMCLI soit terminé). Lorsque plusieurs instances VMCLI sont démarrées de cette manière et qu'une ou plusieurs instances de commande doivent être terminées manuellement, utilisez les fonctionnalités spécifiques au système d'exploitation pour répertorier et terminer les processus.

#### Codes de retour VMCLI

Les messages de texte en anglais seulement sont émis vers la sortie d'erreur standard chaque fois que des erreurs sont rencontrées.

# 13

# Configuration de l'interface de gestion de plateforme intelligente

Cette section fournit des informations sur la configuration et l'utilisation de l'interface IPMI iDRAC6. L'interface comprend :

- IPMI sur le LAN
- IPMI sur série
- Série sur LAN

iDRAC6 est compatible IPMI 2.0. Vous pouvez configurer IPMI iDRAC6 en utilisant :

- l'interface GUI iDRAC6 depuis votre navigateur,
- un utilitaire Open Source comme *IPMItool*,
- l'environnement IPMI de Dell OpenManage, *ipmish*,
- RACADM.

Pour plus d'informations sur l'utilisation de l'environnement IPMI, ipmish, voir le Guide d'utilisation de *Dell OpenManage Baseboard Management Controller Utilities* à l'adresse **support.dell.com\manuals**.

Pour plus d'informations sur l'utilisation de RACADM, voir « Utilisation de la RACADM à distance », à la page 117.

## Configuration d'IPMI via l'interface Web

Pour des informations détaillées, voir « Configuration IPMI via l'interface Web », à la page 64.

# Configuration d'IPMI à l'aide de la CLI RACADM

1 Ouvrez une session sur le système distant à l'aide d'une des interfaces RACADM. Voir « Utilisation de la RACADM à distance », à la page 117.

2 Configurez IPMI sur LAN.

Ouvrez une invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

```
racadm config -g cfgIpmiLan -o cfgIpmiLanEnable 1
```

**REMARQUE :** ce paramètre détermine les commandes IPMI qui peuvent être exécutées à partir de l'interface IPMI sur LAN. Pour plus d'informations, consultez les spécifications d'IPMI 2.0.

**a** Mettez à jour les privilèges du canal IPMI.

À l'invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

```
racadm config -g cfgIpmiLan -o
cfgIpmiLanPrivilegeLimit <niveau>
```

où *<niveau>* correspond à :

- 2 (utilisateur)
- 3 (opérateur)
- 4 (administrateur)

Par exemple, pour définir le privilège Canal LAN IPMI sur 2 (utilisateur), tapez la commande suivante :

```
racadm config -g cfgIpmiLan -o
cfgIpmiLanPrivilegeLimit 2
```

**b** Définissez la clé de cryptage du canal LAN IPMI, si nécessaire.

**REMARQUE :** IPMI iDRAC6 prend en charge le protocole RMCP+. Pour plus d'informations, voir les spécifications d'IPMI 2.0.

À l'invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

```
racadm config -g cfgIpmiLan -o
cfgIpmiEncryptionKey <clé>
```

où *<clé>* est une clé de cryptage de 20 caractères au format hexadécimal valide.

**3** Configurez Communications série IPMI sur le LAN (SOL).

À l'invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

```
racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1
```

**a** Mettez à jour le niveau de privilège minimal d'IPMI SOL.

**REMARQUE :** le niveau de privilège minimum d'IPMI SOL détermine le privilège minimal requis pour activer IPMI SOL. Pour plus d'informations, consultez la spécification d'IPMI 2.0.

À l'invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolMinPrivilege <niveau>
```

où *<niveau>* correspond à :

- 2 (utilisateur)
- 3 (opérateur)
- 4 (administrateur)

Par exemple, pour configurer les privilèges IPMI sur 2 (utilisateur), tapez la commande suivante :

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolMinPrivilege 2
```

**b** Mettez à jour le débit en bauds d'IPMI SOL.

**REMARQUE :** pour rediriger la console série sur LAN, assurez-vous que le débit en bauds de SOL est identique au débit en bauds de votre système géré.

À l'invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolBaudRate <débit_en_bauds>
```

où *<débit_en_bauds>* est égal à 9 600, 19 200, 57 600 ou 115 200 b/s.

Par exemple :

```
racadm config -g cfgIpmiSol -o
cfgIpmiSolBaudRate 57600
```

**c** Activez SOL pour un utilisateur individuel.

**REMARQUE :** SOL peut être activé ou désactivé pour chaque utilisateur individuel.

À l'invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

```
racadm config -g cfgUserAdmin -o
cfgUserAdminSolEnable -i <référence> 2
```

où *<référence>* est la référence unique de l'utilisateur.

**4** Configurez les communications IPMI série.

**a** Remplacez le mode de connexion des communications IPMI série par le paramètre approprié.

À l'invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

```
racadm config -g cfgSerial -o
cfgSerialConsoleEnable 0
```

**b** Configurez le débit en bauds des communications IPMI série.

Ouvrez une invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialBaudRate <débit_en_bauds>
```

où *<débit_en_bauds>* est égal à 9 600, 19 200, 57 600 ou 115 200 b/s.

Par exemple :

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialBaudRate 57600
```

**c** Activez le contrôle du débit matériel des communications IPMI série.

À l'invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialFlowControl 1
```

**d** Configurez le niveau de privilège minimal de canal des communications IPMI série.

À l'invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialChanPrivLimit <niveau>
```

où *<niveau>* correspond à :

- `2` (utilisateur)
- `3` (opérateur)
- `4` (administrateur)

Par exemple, pour définir les privilèges de canal des communications IPMI série sur 2 (utilisateur), tapez la commande suivante :

```
racadm config -g cfgIpmiSerial -o
cfgIpmiSerialChanPrivLimit 2
```

**e** Assurez-vous que MUX série est correctement configuré dans le programme de configuration du BIOS.

- Redémarrez le système.
- Pendant le POST, appuyez sur <F2> pour accéder au programme de configuration du BIOS.
- Cliquez sur **Communication série**.
- Dans le menu **Connexion série**, assurez-vous que **Connecteur série externe** est défini sur **Périphérique d'accès à distance**.
- Enregistrez et quittez le programme de configuration du BIOS.
- Redémarrez le système.

La configuration IPMI est terminée.

Si les communications IPMI série sont en mode terminal, vous pouvez configurer les paramètres supplémentaires suivants à l'aide des commandes **racadm config cfgIpmiSerial :**

- Contrôle de la suppression
- Contrôle d'écho
- Modification de ligne

- Nouvelles séquences linéaires
- Saisie de nouvelles séquences linéaires

Pour plus d'informations sur ces propriétés, voir la spécification d'IPMI 2.0.

# Utilisation de l'interface série d'accès à distance IPMI

Dans l'interface des communications IPMI série, les modes suivants sont disponibles :

- **Mode terminal IPMI :** prend en charge les commandes ASCII qui sont envoyées à partir d'un terminal série. Le jeu de commandes a un nombre limité de commandes (notamment le contrôle de l'alimentation) et prend en charge les commandes IPMI brutes qui sont saisies sous forme de caractères ASCII hexadécimaux.
- **Mode de base IPMI :** prend en charge une interface binaire pour l'accès au programme, comme l'environnement IPMI (IPMISH) qui est inclus avec l'utilitaire de gestion de la carte mère (BMU).

Pour configurer le mode IPMI à l'aide de la RACADM :

1. Désactivez l'interface série du RAC.

   À l'invite de commande, entrez :

   ```
   racadm config -g cfgSerial -o
   cfgSerialConsoleEnable 0
   ```

2. Activez le mode IPMI approprié.

   Par exemple, à l'invite de commande, tapez :

   ```
   racadm config -g cfgIpmiSerial -o
   cfgIpmiSerialConnectionMode <0 ou 1>
   ```

Pour des informations supplémentaires, voir la section Groupe de base de données de propriété iDRAC6 et les définitions d'objets du *Guide de référence de la ligne de commande RACADM pour iDRAC6 et CMC* disponible sur le site Web de support Dell à l'adresse **dell.com/support/manuals**.

# Configuration des communications série sur LAN au moyen de l'interface Web

Pour des informations détaillées, voir « Configuration IPMI via l'interface Web », à la page 64.

**REMARQUE :** vous pouvez utiliser les communications série sur LAN avec les outils Dell OpenManage suivants : SOLProxy et IPMItool. Pour plus d'informations, voir le Guide d'utilisation de *Dell OpenManage Baseboard Management Controller Utilities* à l'adresse **support.dell.com\manuals**.

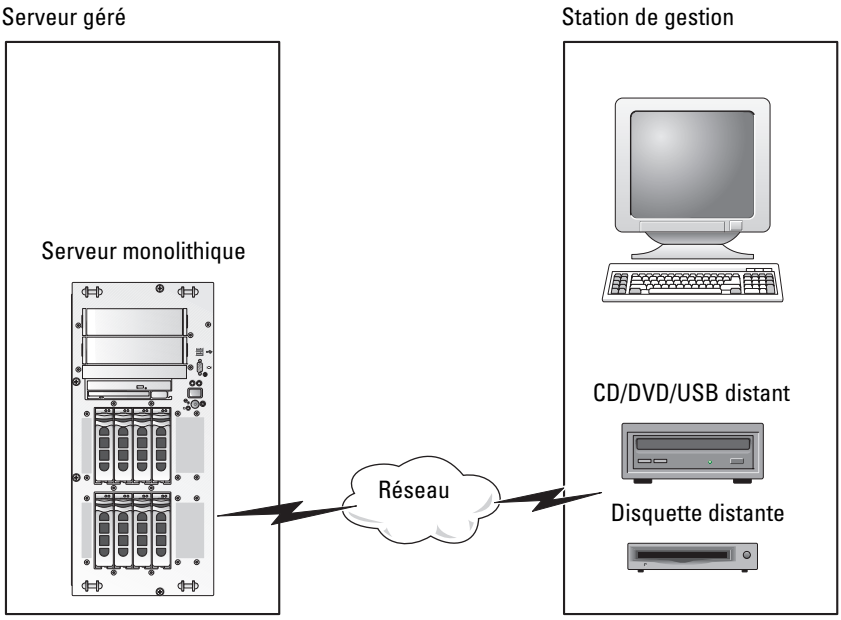
# 14

# Configuration et utilisation du média virtuel

## Présentation

La fonctionnalité **Média virtuel**, accessible via le visualiseur Console virtuelle, permet au serveur géré d'accéder au média connecté à un système distant sur le réseau.La Figure 14-1 illustre l'architecture globale d'un **média virtuel**.

**Figure 14-1. Architecture globale d'un média virtuel**



Grâce au **média virtuel**, les administrateurs peuvent démarrer à distance leurs serveurs gérés, installer des applications, mettre à jour des pilotes ou même installer de nouveaux systèmes d'exploitation à distance à partir de lecteurs de CD/DVD et de disquettes virtuels.

**REMARQUE :** le média virtuel exige une bande passante réseau disponible d'au moins 128 Kb/s.

Le **média virtuel** définit deux périphériques pour le système d'exploitation et le BIOS du serveur géré : un périphérique de disquette et un périphérique de disque optique.

La station de gestion fournit le média physique ou le fichier image sur le réseau. Lorsque le **média virtuel** est connecté ou autoconnecté, toutes les requêtes d'accès au lecteur de CD/disquette virtuel provenant du serveur géré sont dirigées vers la station de gestion par le réseau. La connexion du **média virtuel** revient à insérer le média dans des périphériques physiques sur le système géré. Lorsque le **média virtuel** se trouve dans l'état de connexion, les périphériques virtuels du système géré se présentent sous la forme de deux lecteurs sur lesquels le média n'est pas installé.

Le Tableau 14-1 répertorie les connexions de lecteur prises en charge pour les lecteurs de disquette virtuels et les lecteurs optiques virtuels.

**REMARQUE :** le changement de **média virtuel** en cours de connexion est susceptible d'interrompre la séquence de démarrage du système.

**Tableau 14-1. Connexions de lecteur prises en charge**

| Connexions de lecteur de disquette virtuel prises en charge | Connexions de lecteur optique virtuel prises en charge |
|---|---|
| Lecteur de disquette 1.44 hérité avec disquette 1.44 | Lecteur de CD-ROM, de DVD, CD-RW, mixte avec média de CD-ROM |
| Lecteur de disquette USB avec disquette 1.44 | Fichier image de CD-ROM/DVD au format ISO9660 |
| Image de disquette 1.44 | Lecteur de CD-ROM USB avec média de CD-ROM |
| Disque amovible USB | |

### Station de gestion Windows

Pour exécuter la fonctionnalité **Média virtuel** sur une station de gestion fonctionnant sous un système d'exploitation Microsoft Windows, installez une version prise en charge d'Internet Explorer ou de Firefox avec un environnement d'exécution Java (JRE).

### Station de gestion Linux

Pour exécuter la fonctionnalité Média virtuel sur une station de gestion fonctionnant sous un système d'exploitation Linux, installez une version prise en charge de Firefox.

Un environnement d'exécution Java (JRE) 32 bits est requis pour exécuter le plug-in de la console virtuelle. Vous pouvez télécharger un JRE à l'adresse **java.sun.com**.

**PRÉCAUTION : pour réussir à lancer le média virtuel, vérifiez que vous avez bien installé une version JRE 32 bits ou 64 bits sur un système d'exploitation 64 bits, ou une version JRE 32 bits sur un système d'exploitation 32 bits. iDRAC6 ne prend *pas* en charge les versions ActiveX 64 bits. En outre, assurez-vous que, pour Linux, le progiciel connexe « compat-libstdc++-33-3.2.3-61 » est installé pour pouvoir lancer le média virtuel. Sous Windows, il se peut que le progiciel soit inclus dans le progiciel d'infrastructure .NET.**

# Configuration du média virtuel

1. Ouvrez une session sur l'interface Web iDRAC6.
2. Sélectionnez **Système**→ onglet **Console/Média**→ **Configuration**→ **Média virtuel** pour configurer les paramètres du média virtuel.

   Le Tableau 14-2 décrit les valeurs de configuration du **média virtuel**.
3. Une fois les paramètres configurés, cliquez sur **Appliquer**.

**Tableau 14-2. Propriétés de configuration du média virtuel**

| Attribut | Valeur |
|---|---|
| État | **Connecter :** connecte immédiatement le **média virtuel** au serveur.<br>**Déconnecter :** déconnecte immédiatement le **média virtuel** du serveur.<br>**Autoconnecter** : connecte le **média virtuel** au serveur uniquement quand une session de média virtuel est démarrée. |
| Nombre maximal de sessions | Affiche le nombre maximal de sessions de **média virtuel** autorisées qui est toujours fixé à 1. |
| Sessions actives | Affiche le nombre actuel de sessions de média virtuel. |
| Cryptage de média virtuel activé | Sélectionnez ou désélectionnez la case à cocher pour activer ou désactiver le cryptage des connexions du **média virtuel**. La sélection active le cryptage, la désélection désactive le cryptage. |
| Émulation de disquette | Indique si le **média virtuel** apparaît au serveur comme un lecteur de disquette ou comme une clé USB. Si l'option **Émulation de disquette** est cochée, le périphérique de **média virtuel** apparaît comme un périphérique de disquette sur le serveur. Si elle désélectionnée, le média virtuel apparaît comme un lecteur de clé USB.<br>**REMARQUE :** dans certains environnements Windows Vista et Red Hat, il se peut que vous ne puissiez pas virtualiser une clé USB si l'option **Émulation de disquette** est activée. |
| État de la connexion | **Connecté :** une session de média virtuel est en cours.<br>**Pas connecté :** aucune session de média virtuel n'est en cours. |
| Activer Démarrer une seule fois | Cochez cette case pour activer l'option **Démarrer une seule fois**. Utilisez cet attribut pour démarrer à partir du média virtuel. Au prochain démarrage, sélectionnez le périphérique de démarrage dans le menu de démarrage du BIOS. Cette option déconnecte automatiquement les périphériques de **média virtuel** après le démarrage unique du système. |

# Exécution du média virtuel

**PRÉCAUTION : n'émettez pas une commande racreset lorsque vous exécutez une session de média virtuel. Sinon, des résultats indésirables peuvent se produire, y compris une perte de données.**

**REMARQUE :** l'application de la fenêtre Visualiseur de console doit rester active lorsque vous accédez au média virtuel.

**REMARQUE :** suivez les étapes ci-dessous pour activer Red Hat Enterprise Linux (version 4) afin de reconnaître un périphérique SCSI avec plusieurs unités logiques (LUN) :

1. Ajoutez la ligne suivante à **/ect/modprobe** :

   ```
   options scsi_mod max_luns=256

   cd /boot

   mkinitrd -f initrd-2.6.9.78ELsmp.img 2.6.3.78ELsmp
   ```

2. Redémarrez le serveur.
3. Exécutez les commandes suivantes pour afficher le CD/DVD virtuel et/ou la disquette virtuelle :

   ```
   cat /proc/scsi/scsi
   ```

**REMARQUE :** avec le média virtuel, vous ne pouvez virtualiser qu'une seule disquette/lecteur USB/image/clé et un seul lecteur optique à partir de votre station de gestion pour une mise à disposition comme lecteur (virtuel) sur le serveur géré.

## Configurations de média virtuel prises en charge

Vous pouvez activer le média virtuel pour un seul lecteur de disquette et un seul lecteur optique. Un seul lecteur pour chaque type de média peut être virtualisé à la fois.

Les lecteurs de disquette pris en charge incluent une image de disquette ou un seul lecteur de disquette disponible. Les lecteurs optiques pris en charge incluent un seul lecteur optique disponible ou un seul fichier image ISO maximum.

### Connexion du média virtuel

Effectuez les étapes suivantes pour exécuter le média virtuel :

1. Ouvrez un navigateur Web pris en charge sur votre station de gestion.

2 Démarrez l'interface Web iDRAC6. Reportez-vous à la section « Accès à l'interface Web », à la page 48 pour en savoir plus.

3 Sélectionnez **Système→ Console/Média→ Console virtuelle et média virtuel.**

4 La page **Console virtuelle et média virtuel** s'affiche. Si vous souhaitez modifier les valeurs des attributs affichés, voir « Configuration du média virtuel », à la page 281.

**REMARQUE :** le **Fichier image de disquette** dans **Lecteur de disquette** (si applicable) peut apparaître, car ce périphérique peut être virtualisé comme une disquette virtuelle. Vous pouvez sélectionner simultanément un seul lecteur optique et un seul lecteur flash de disquette/USB à virtualiser.

**REMARQUE :** les lettres des lecteurs de périphériques virtuels sur le serveur géré ne coïncident pas avec celles des lecteurs physiques sur la station de gestion.

**REMARQUE :** le **média virtuel** peut ne pas fonctionner correctement sur les clients de système d'exploitation Windows qui sont configurés avec l'option de sécurité avancée d'Internet Explorer. Pour résoudre ce problème, voir la documentation de votre système d'exploitation Microsoft ou contactez votre administrateur système.

5 Cliquez sur **Lancer la console virtuelle**.

**REMARQUE :** sous Linux, le fichier **jviewer.jnlp** est téléchargé sur votre bureau et une boîte de dialogue vous demande ce que vous souhaitez faire avec le fichier. Choisissez l'option **Ouvrir avec le programme**, puis sélectionnez l'application **javaws** qui se trouve dans le sous-répertoire **bin** de votre répertoire d'installation JRE.

L'application **Console virtuelle iDRAC6** se lance dans une fenêtre distincte.

6 Cliquez sur **Média virtuel→ Lancer le média virtuel**.

L'assistant **Session de média virtuel** s'affiche.

**REMARQUE :** ne fermez pas cet assistant, sauf si vous désirez mettre fin à la session de média virtuel.

7 Si le média est connecté, vous devez le déconnecter avant de connecter une source de média différente. Décochez la case en regard du média que vous souhaitez déconnecter.

8 Sélectionnez les types de média que vous souhaitez connecter.

Si vous souhaitez connecter une image de disquette ou une image ISO, saisissez le chemin (sur votre ordinateur local) de l'image ou cliquez sur le bouton **Ajouter image...** et recherchez l'image.

Le média est connecté et la fenêtre **Condition** est mise à jour.

#### Déconnexion du média virtuel

1 Cliquez sur **Outils→ Lancer le média virtuel**.

2 Décochez la case en regard du média que vous souhaitez déconnecter.

Le média est déconnecté et la fenêtre **Condition** est mise à jour.

3 Cliquez sur **Quitter** pour mettre fin à l'assistant **Session de média virtuel**.

**REMARQUE :** à chaque fois qu'une session Média virtuel est lancée ou qu'un disque vFlash est connecté, un lecteur supplémentaire intitulé « LCDRIVE » s'affiche sur le système d'exploitation hôte et sur le BIOS. Le lecteur supplémentaire disparaît lorsque le disque vFlash ou la session Média virtuel est déconnecté.

### Démarrage à partir d'un média virtuel

Le BIOS système vous permet de démarrer à partir de lecteurs optiques virtuels ou de lecteurs de disquette virtuels. Pendant le POST, accédez à la fenêtre Configuration du BIOS et vérifiez que les lecteurs virtuels sont activés et répertoriés dans le bon ordre.

Pour modifier le paramètre du BIOS, effectuez les étapes suivantes :

1 Démarrez le serveur géré.

2 Appuyez sur <F2> pour accéder à la fenêtre Configuration du BIOS.

3 Faites défiler jusqu'à la séquence de démarrage et appuyez sur <Entrée>.

Dans la fenêtre contextuelle, les lecteurs optiques virtuels et les lecteurs de disquette virtuels sont répertoriés avec les périphériques de démarrage standard.

4 Assurez-vous que le lecteur virtuel est activé et répertorié comme étant le premier périphérique avec un média d'amorçage. Si nécessaire, suivez les instructions affichées à l'écran pour modifier l'ordre de démarrage.

5 Enregistrez les modifications et quittez.

Le serveur géré redémarre.

Le serveur géré tente de démarrer à partir d'un périphérique d'amorçage en suivant l'ordre de démarrage. Si le périphérique virtuel est connecté et qu'un média d'amorçage est présent, le système démarre sur le périphérique virtuel. Autrement, le système ignore le périphérique, tout comme un périphérique physique sans média d'amorçage.

### Installation de systèmes d'exploitation avec un média virtuel

Cette section décrit une méthode manuelle interactive d'installation du système d'exploitation sur votre station de gestion qui peut prendre plusieurs heures. Une procédure d'installation avec script du système d'exploitation utilisant le **média virtuel** peut prendre moins de 15 minutes. Pour en savoir plus, voir « Déploiement du système d'exploitation », à la page 261.

1 Vérifiez les points suivants :

- Le CD d'installation du système d'exploitation est inséré dans le lecteur de CD de la station de gestion.
- Le lecteur de CD local est sélectionné.
- Vous êtes connecté aux lecteurs virtuels.

2 Suivez les étapes de démarrage à partir du média virtuel de la section « « Démarrage à partir d'un média virtuel », à la page 285 » afin de garantir que le BIOS est défini pour démarrer à partir du lecteur de CD à partir duquel vous effectuez l'installation.

3 Suivez les instructions à l'écran pour terminer l'installation.

Pour une installation multi-disques, il est essentiel de suivre les étapes suivantes :

1 Démappez le CD/DVD virtualisé (redirigé) de la console du média virtuel.

2 Insérez le CD/DVD suivant dans le lecteur optique distant.

3 Mappez (redirigez) ce CD/DVD depuis la console du média virtuel.

L'insertion d'un nouveau CD/DVD dans le lecteur optique distant sans remappage peut se solder par un échec.

#### Fonctionnalité Démarrer une seule fois

La fonctionnalité Démarrer une seule foisvous aide à modifier temporairement l'ordre de démarrage afin de démarrer à partir d'un périphérique de média virtuel. Cette fonctionnalité est utilisée conjointement avec le média virtuel, en règle générale lors de l'installation de systèmes d'exploitation.

**REMARQUE :** vous devez disposer de privilèges **Configuration iDRAC6** pour utiliser cette fonctionnalité.

**REMARQUE :** les périphériques distants doivent être redirigés à l'aide du média virtuel pour utiliser cette fonctionnalité.

Pour utiliser la fonctionnalité Démarrer une seule fois, procédez comme suit :

1. Ouvrez une session sur iDRAC6 par le biais de l'interface Web et cliquez sur **Système→ Console/Média→ Configuration**.
2. Cochez l'option **Activer Démarrer une seule fois** sous **Média virtuel**.
3. Allumez le serveur et accédez au gestionnaire de démarrage du BIOS.
4. Modifiez la séquence de démarrage afin de démarrer à partir du périphérique de média virtuel distant.
5. Effectuez un cycle d'alimentation sur le serveur.

   Le serveur démarre à partir du périphérique de média virtuel distant. Au prochain redémarrage du serveur, la connexion au média virtuel distant est interrompue.

   **REMARQUE :** le média virtuel doit être en état **connecté** pour que les lecteurs virtuels apparaissent dans la séquence de démarrage. Assurez-vous que le média de démarrage est présent dans le lecteur virtualisé pour activer **Démarrer une seule fois**.

### Utilisation d'un média virtuel lors de l'exécution du système d'exploitation du serveur

#### Systèmes Windows

Sur les systèmes Windows, les lecteurs de média virtuel sont montés automatiquement s'ils sont connectés et configurés avec une lettre de lecteur.

L'utilisation de lecteurs virtuels à partir de Windows est semblable à l'utilisation de vos lecteurs physiques. Lorsque vous vous connectez au média via l'Assistant Média virtuel, le média est disponible sur le système en cliquant sur le lecteur et en parcourant son contenu.

#### Systèmes Linux

Selon la configuration du logiciel installé sur votre système, les lecteurs de média virtuel ne peuvent pas être montés automatiquement. Si vos lecteurs ne sont pas montés automatiquement, montez-les manuellement à l'aide de la commande **mount** Linux.

## Questions les plus fréquentes concernant le média virtuel

Le Tableau 14-3 répertorie les questions les plus fréquentes et les réponses correspondantes.

**Tableau 14-3. Utilisation d'un média virtuel : Questions les plus fréquentes**

| Question | Réponse |
|---|---|
| Je remarque parfois que ma connexion de client au média virtuel est interrompue. Pourquoi ? | Si le délai d'attente du réseau expire, le micrologiciel iDRAC6 interrompt la connexion en déconnectant la liaison entre le serveur et le lecteur virtuel.<br><br>Si les paramètres de configuration du média virtuel sont modifiés dans l'interface Web iDRAC6 ou via les commandes de la RACADM locale, tout média connecté est déconnecté lorsque les modifications de la configuration sont appliquées.<br><br>Pour rétablir la connexion au lecteur virtuel, utilisez l'Assistant Média virtuel. |
| Quels sont les systèmes d'exploitation pris en charge par iDRAC6 ? | Voir « Systèmes d'exploitation pris en charge », à la page 27 pour obtenir la liste des systèmes d'exploitation pris en charge. |
| Quels sont les navigateurs Web qui prennent en charge iDRAC6 ? | Pour obtenir la liste des navigateurs Web pris en charge, voir « Navigateurs Web pris en charge », à la page 28. |

**Tableau 14-3. Utilisation d'un média virtuel : Questions les plus fréquentes *(suite)***

| Question | Réponse |
|---|---|
| Pourquoi m'arrive-t-il parfois de perdre ma connexion client ? | • Vous pouvez parfois perdre votre connexion client si le réseau est lent ou si vous changez le CD dans le lecteur de CD du système client. Par exemple, si vous changez le CD dans le lecteur de CD du système client, le nouveau CD peut avoir une fonctionnalité Autodémarrage. Si c'est le cas, le micrologiciel peut arriver au bout du délai d'attente et la connexion peut être perdue si le système client prend trop longtemps avant d'être prêt pour lire le CD. Si une connexion est perdue, reconnectez-vous à partir de l'IUG et continuez l'opération précédente.<br>• Si le délai d'attente du réseau expire, le micrologiciel iDRAC6 interrompt la connexion en déconnectant la liaison entre le serveur et le lecteur virtuel. En outre, il se peut que quelqu'un ait modifié les paramètres de configuration du média virtuel dans l'interface Web ou en ayant saisi des commandes RACADM. Pour rétablir la connexion au lecteur virtuel, utilisez la fonctionnalité **Média virtuel**. |
| Une installation du système d'exploitation Windows via le média virtuel semble prendre trop longtemps. Pourquoi ? | Si vous installez le système d'exploitation Windows à l'aide du DVD *Dell Systems Management Tools and Documentation* et que la connexion réseau est lente, la procédure d'installation peut nécessiter beaucoup plus de temps pour accéder à l'interface Web iDRAC6 en raison de la latence du réseau. Même si la fenêtre d'installation n'indique pas la progression de l'installation, la procédure d'installation est en cours. |

**Tableau 14-3. Utilisation d'un média virtuel : Questions les plus fréquentes *(suite)***

| Question | Réponse |
|---|---|
| Comment puis-je configurer mon périphérique virtuel comme périphérique d'amorçage ? | Sur le serveur géré, accédez à la configuration du BIOS et cliquez sur le menu de démarrage. Recherchez le CD virtuel, la disquette virtuelle ou le disque Flash virtuel et changez la séquence d'amorçage des périphériques, si nécessaire. En outre, faites du périphérique virtuel un périphérique de démarrage en appuyant sur la touche « Barre d'espace » dans la séquence de démarrage de l'installation CMOS. Par exemple, pour démarrer à partir d'un lecteur de CD, définissez-le en tant que premier lecteur dans l'ordre de démarrage. |
| À partir de quels types de média puis-je démarrer ? | iDRAC6 vous permet de démarrer à partir des médias de démarrage suivants :<br>• Média de données de CD-ROM/DVD<br>• Image ISO 9660<br>• Disquette 1.44 ou image de disquette<br>• Clé USB qui est reconnue par le système d'exploitation comme disque amovible<br>• Image de clé USB |
| Comment faire pour faire de ma clé USB une clé d'amorçage ? | Recherchez sur le site **support.dell.com** l'utilitaire de démarrage Dell, un programme Windows que vous pouvez utiliser pour faire de votre clé USB Dell une clé d'amorçage.<br>Vous pouvez également démarrer à l'aide d'un disque de démarrage de Windows 98 et copier les fichiers système du disque de démarrage sur votre clé USB. Par exemple, à l'invite du DOS, tapez la commande suivante :<br>`sys a: x: /s`<br>où *x*: est la clé USB que vous voulez utiliser comme clé d'amorçage. |

**Tableau 14-3. Utilisation d'un média virtuel : Questions les plus fréquentes *(suite)***

| Question | Réponse |
|---|---|
| Je n'arrive pas à trouver mon périphérique de disquette virtuel/CD virtuel sur un système exécutant le système d'exploitation Red Hat Enterprise Linux ou SUSE Linux. Mon média virtuel est connecté et je suis connecté à ma disquette distante. Que dois-je faire ? | Certaines versions de Linux ne montent pas automatiquement le lecteur de disquette virtuel et le lecteur de CD virtuel de la même manière. Pour monter le lecteur de disquette virtuel, recherchez le nœud de périphérique que Linux attribue au lecteur de disquette virtuel. Procédez comme suit pour rechercher et monter correctement le lecteur de disquette virtuel :<br>**1** Ouvrez une invite de commande Linux et exécutez la commande suivante :<br>`grep "Virtual Floppy" /var/log/messages`<br>**2** Recherchez la dernière entrée de ce message et notez l'heure.<br>**3** À l'invite de Linux, exécutez la commande suivante :<br>`grep "hh:mm:ss" /var/log/messages` où :<br>*`hh:mm:ss`* correspond à l'horodatage du message retourné par grep à l'étape 1.<br>**4** À l'étape 3, lisez le résultat de la commande grep et recherchez le nom du périphérique attribué à la disquette virtuelle Dell.<br>**5** Assurez-vous que vous êtes relié et connecté au lecteur de disquette virtuel.<br>**6** À l'invite de Linux, exécutez la commande suivante :<br>mount */dev/sdx* /mnt/floppy<br>où :<br>*`/dev/sdx`* est le nom du périphérique trouvé à l'étape 4<br>`/mnt/floppy` est le point de montage. |

**Tableau 14-3. Utilisation d'un média virtuel : Questions les plus fréquentes *(suite)***

| Question | Réponse |
|---|---|
| Je n'arrive pas à trouver mon périphérique de disquette virtuel/CD virtuel sur un système exécutant le système d'exploitation Red Hat Enterprise Linux ou SUSE Linux. Mon média virtuel est connecté et je suis connecté à ma disquette distante. Que dois-je faire ? | *(suite de la réponse)*<br>Pour monter le lecteur de CD virtuel, recherchez le nœud de périphérique que Linux attribue au lecteur de CD virtuel. Suivez ces étapes pour trouver et monter le lecteur de CD virtuel :<br>**1** Ouvrez une invite de commande Linux et exécutez la commande suivante :<br>`grep "Virtual CD" /var/log/messages`<br>**2** Recherchez la dernière entrée de ce message et notez l'heure.<br>**3** À l'invite de Linux, exécutez la commande suivante :<br>`grep "hh:mm:ss" /var/log/messages`<br>où<br>`hh:mm:ss` correspond à l'horodatage du message renvoyé par `grep` à l'étape 1.<br>**4** À l'étape 3, lisez le résultat de la commande grep et recherchez le nom du périphérique qui est donné au *CD Dell Virtual*.<br>**5** Assurez-vous que vous êtes relié et connecté au lecteur de CD virtuel.<br>**6** À l'invite de Linux, exécutez la commande suivante :<br>`mount /dev/sdx /mnt/CD`<br>où :<br>`/dev/sdx` est le nom du périphérique trouvé à l'étape 4<br>`/mnt/floppy` est le point de montage. |

**Tableau 14-3. Utilisation d'un média virtuel : Questions les plus fréquentes *(suite)***

| Question | Réponse |
|---|---|
| Lorsque j'ai effectué une mise à jour de micrologiciel à distance via l'interface Web iDRAC6, mes lecteurs virtuels présents sur le serveur ont été supprimés. Pourquoi ? | Les mises à jour de micrologiciel entraînent la réinitialisation d'iDRAC6, une interruption de la connexion à distance et le démontage des lecteurs virtuels. |
| Pourquoi tous mes périphériques USB sont-ils déconnectés après que j'ai connecté un périphérique USB ? | Les périphériques de média virtuel et les périphériques vFlash sont connectés au BUS USB hôte en tant que périphérique USB composite et ils partagent un port USB commun. À chaque fois qu'un périphérique USB de média virtuel ou vFlash est connecté au BUS USB hôte ou déconnecté de ce dernier, tous les périphériques de média virtuel et vFlash sont momentanément déconnectés du bus hôte USB et seront reconnectés par la suite. Si un périphérique de média virtuel est utilisé par le système d'exploitation hôte, vous devez éviter de connecter ou déconnecter un ou plusieurs périphériques de média virtuel ou vFlash. Il est recommandé de connecter d'abord tous les périphériques USB nécessaires avant de les utiliser. |
| Que fait le bouton **Réinitialisation USB** ? | Il réinitialise les périphériques USB distants et locaux connectés au serveur. |

**Tableau 14-3. Utilisation d'un média virtuel : Questions les plus fréquentes *(suite)***

| Question | Réponse |
|---|---|
| Comment puis-je obtenir les performances maximales du média virtuel ? | Pour obtenir les performances maximales du média virtuel, lancez le média virtuel en veillant à ce que la console virtuelle soit désactivée ou effectuez l'une des opérations suivantes :<br>• Réduisez la résolution vidéo et l'intensité de couleur de l'écran Console virtuelle afin de les définir sur les valeurs minimales autorisées.<br>• Désactivez le cryptage du média virtuel et de la console virtuelle.<br>**REMARQUE :** dans ce cas, le transfert des données entre le serveur géré et l'iDRAC pour le média virtuel et la console virtuelle n'est pas sécurisé.<br>• Si vous utilisez un système d'exploitation Windows Server, arrêtez le service Windows intitulé Windows Event Collector. Pour ce faire, allez dans **Démarrer > Outils d'administration > Services**. Cliquez-droite sur **Windows Event Collector** et cliquez sur **Arrêter**. |

# 15

# Configuration de la carte SD vFlash et gestion des partitions vFlash

La carte SD vFlash est une carte numérique sécurisée (SD/Secure Digital) qui se connecte dans un logement de carte iDRAC6 Enterprise en option à l'arrière du système. Elle offre un espace de stockage et se comporte comme une clé de mémoire flash USB courante. Elle fait office d'emplacement de stockage pour les partitions définies par l'utilisateur pouvant être configurées à des fins d'exposition au système en tant que périphérique USB et servant également à créer un périphérique USB d'amorçage. Selon le mode d'émulation sélectionné, les partitions sont exposées au système en tant que lecteur de disquette et disque dur, ou en tant que lecteur de CD/DVD. Vous pouvez définir l'un d'entre eux en tant que périphérique d'amorçage.

Pour plus d'informations sur l'installation et le retrait de la carte de votre système, consultez le *Manuel du propriétaire du matériel* à l'adresse **dell.com/support/manuals**.

Les cartes SD vFlash et SD standard sont prises en charge. Une *carte SD vFlash* est la carte qui prend en charge les nouvelles fonctionnalités vFlash améliorées. Une carte *SD standard* est une carte SD normale prête à être utilisée prenant en charge uniquement des fonctionnalités vFlash limitées.

Grâce à la carte SD vFlash, vous pouvez créer jusqu'à 16 partitions. Vous pouvez spécifier un nom d'étiquette pour la partition au moment de sa création et effectuer un éventail de tâches pour gérer et utiliser les partitions. Une carte SD vFlash peut être de toute taille sans toutefois excéder 8 Go. Chaque taille de partition peut atteindre 4 Go.

Une carte SD standard peut être de toute taille, mais prend en charge une seule partition. La taille de la partition est limitée à 256 Mo. Par défaut, le nom d'étiquette de la partition est VFLASH.

**REMARQUE :** veillez à insérer uniquement une carte SD vFlash ou une carte SD standard dans le logement de carte iDRAC6 Enterprise. Si vous insérez une carte d'un autre format (par exemple, Multi-Media Card [MMC]), le message d'erreur suivant s'affiche lorsque vous initialisez la carte : *Une erreur s'est produite lors de l'initialisation de la carte SD.*

Si vous êtes un administrateur, vous pouvez effectuer toutes les tâches sur les partitions vFlash. Dans le cas contraire, vous devez disposer du privilège Accès au média virtuel pour créer, supprimer, formater, attacher, détacher ou copier le content de la partition.

## Configuration de la carte SD vFlash ou standard via l'interface Web iDRAC6

Après avoir installé la carte SD vFlash ou standard, vous pouvez afficher ses propriétés, activer ou désactiver vFlash, et initialiser la carte. La fonctionnalité vFlash doit être activée pour pouvoir gérer la partition. Lorsque la carte est désactivée, vous pouvez uniquement afficher ses propriétés. L'opération d'initialisation supprime les partitions existantes et réinitialise la carte.

**REMARQUE :** vous devez disposer de l'autorisation Configurer iDRAC pour activer ou désactiver vFlash, ou pour initialiser la carte.

Si la carte n'est pas disponible dans le logement de carte iDRAC6 Enterprise du système, le message d'erreur suivant s'affiche.

```
Carte SD non détectée. Insérez une carte SD d'une
taille supérieure ou égale à 256 Mo.
```

Pour afficher et configurer la carte SD vFlash ou standard :

1. Ouvrez une fenêtre de navigateur Web pris en charge et ouvrez une session sur l'interface Web iDRAC6.
2. Dans l'arborescence du système, sélectionnez **Système**.
3. Cliquez sur l'onglet **vFlash**. La page **Propriétés de la carte SD** s'affiche.

   Le Tableau 15-1 répertorie les propriétés affichées pour la carte SD.

**Tableau 15-1. Propriétés de la carte SD**

| Attribut | Description |
|---|---|
| **Name (Nom)** | Affiche le nom de la carte insérée dans le logement de carte iDRAC6 Enterprise du serveur. Si la carte prend en charge les nouvelles fonctionnalités vFlash améliorées, la mention *Carte SD vFlash* apparaît. Si elle prend en charge des fonctionnalités vFlash limitées, la mention *Carte SD* apparaît. |
| **Taille** | Affiche la taille de la carte en gigaoctets (Go). |

**Tableau 15-1. Propriétés de la carte SD *(suite)***

| Attribut | Description |
|---|---|
| **Espace disponible** | Affiche l'espace inutilisé sur la carte SD vFlash en Mo. Cet espace est disponible pour créer des partitions supplémentaires sur la carte SD vFlash.<br>Si la carte SD vFlash insérée n'est pas initialisée, l'espace disponible l'indique.<br>Dans le cas de la carte SD standard, l'espace disponible n'est pas affiché. |
| **Protégé contre l'écriture** | Affiche si la carte est protégée contre l'écriture, ou non. |
| **Intégrité** | Affiche l'intégrité générale de la carte SD vFlash. Ce peut être :<br>• OK<br>• Warning (Avertissement)<br>• Critique<br>Si Avertissement est affiché, réinitialisez la carte.<br>Si Critique est affiché, réinstallez et réinitialisez la carte.<br>Dans le cas de la carte SD standard, l'intégrité n'est pas affichée. |
| **vFlash activé** | Cochez la case pour effectuer une gestion de partition vFlash sur la carte. Décochez la case pour désactiver la gestion de partition vFlash. |

4 Cliquez sur **Appliquer** pour activer ou désactiver la gestion de partition vFlash sur la carte.

Si une partition vFlash est connectée, vous ne pouvez pas désactiver vFlash et un message d'erreur s'affiche.

**REMARQUE :** si vFlash est désactivée, seul le sous-onglet **Propriétés de la carte SD** s'affiche.

5 Cliquez sur **Initialiser**. Toutes les partitions existantes sont supprimées et la carte est réinitialisée. Un message de confirmation s'affiche.

6 Cliquez sur **OK**. Une fois l'opération d'initialisation terminée, un message de réussite s'affiche.

**REMARQUE :** **initialiser** est activé uniquement si vous sélectionnez l'option **vFlash activé**.

Si une partition vFlash est connectée, l'opération d'initialisation échoue et un message d'erreur s'affiche.

Si vous cliquez sur l'une des options des pages vFlash lorsqu'une application comme le fournisseur WSMAN, l'utilitaire de configuration iDRAC6 ou la RACADM utilise vFlash, ou si vous naviguez vers une autre page de l'interface utilisateur, iDRAC6 peut afficher le message suivant

`vFlash est actuellement utilisé par un autre processus. Réessayez dans quelques instants.`

# Configuration de la carte SD vFlash ou standard via la RACADM

Vous pouvez afficher et configurer la carte SD vFlash ou standard à l'aide des commandes RACADM à partir de la console locale, distante ou Telnet/SSH.

**REMARQUE :** vous devez disposer de l'autorisation Configurer iDRAC pour activer ou désactiver vFlash, et pour initialiser la carte.

## Affichage des propriétés de la carte SD vFlash ou standard

Ouvrez une console telnet/SSH/série sur le serveur, ouvrez une session et entrez la commande suivante :

```
racadm getconfig -g cfgvFlashSD
```

Les propriétés en lecture seule suivantes s'affichent :

- `cfgvFlashSDSize`
- `cfgvFlashSDLicense`
- `cfgvFlashSDAvailableSize`
- `cfgvFlashSDHealth`

## Activation ou désactivation de la carte SD vFlash ou standard

Ouvrez une console telnet/SSH/série sur le serveur, ouvrez une session et entrez les commandes suivantes :

- Pour activer la carte SD vFlash ou standard :

  ```
  racadm config -g cfgvFlashsd -o cfgvflashSDEnable 1
  ```

- Pour désactiver la carte SD vFlash ou standard :

  ```
  racadm config -g cfgvFlashsd -o cfgvflashSDEnable 0
  ```

**REMARQUE :** la commande RACADM fonctionne uniquement si une carte SD vFlash ou standard est présente. Si aucune carte n'est présente, le message suivant s'affiche : *ERREUR : Carte SD non présente*.

### Initialisation de la carte SD vFlash ou standard

Ouvrez une console telnet/SSH/série sur le serveur, ouvrez une session et entrez la commande suivante pour initialiser la carte :

```
racadm vflashsd initialize
```

Toutes les partitions existantes sont supprimées et la carte est réinitialisée.

### Obtention de la dernière condition sur la carte SD vFlash ou standard

Ouvrez une console telnet/SSH/série sur le serveur, ouvrez une session et entrez la commande suivante pour obtenir la condition de la dernière commande d'initialisation envoyée à la carte SD vFlash ou standard :

```
racadm vFlashsd status
```

**REMARQUE :** cette commande affiche uniquement la condition des commandes envoyées à la carte SD. Pour obtenir la condition des commandes envoyées aux partitions individuelles de la carte SD, utilisez la commande suivante : `racadm vflashpartition status`

### Réinitialisation de la carte SD vFlash ou standard

Ouvrez une console telnet/SSH/série sur le serveur, ouvrez une session et entrez :

```
racadm vflashsd initialize
```

Pour des informations supplémentaires sur la commande `vflashsd`, voir le *Guide de référence de la ligne de commande RACADM pour iDRAC6 et CMC* sur le site Web de support Dell à l'adresse **support.dell.com/manuals**.

**REMARQUE :** la prise en charge de la commande `racadm vmkey reset` a été éliminée à partir de la version 1.5. La fonctionnalité de cette commande est désormais prise en charge par `vflashsd initialize`. Même si l'exécution de la commande `vmkey reset` réussit, il est recommandé d'utiliser la commande `vflashsd initialize`. Pour plus d'informations, voir « Initialisation de la carte SD vFlash ou standard », à la page 299.

# Gestion des partitions vFlash via l'interface Web iDRAC6

Vous pouvez réaliser les tâches suivantes :

- Créer une partition vide
- Créer une partition à l'aide d'un fichier image
- Formater une partition
- Afficher les partitions disponibles
- Modifier une partition
- Connecter/Déconnecter une partition
- Supprimer des partitions existantes
- Télécharger le contenu d'une partition
- Démarrer à partir d'une partition

## Création d'une partition vide

Une partition vide est similaire à une clé USB vide. Vous pouvez créer des partitions vides sur une carte SD vFlash ou standard. Vous pouvez choisir de créer une partition de type *Disquette* ou *Disque dur*. Le type de partition CD n'est pas pris en charge dans le cadre de la création de partitions vides.

**REMARQUE :** vous devez disposer du privilège Accès au média virtuel pour pouvoir créer des partitions vides.

Avant de créer une partition vide, veillez à ce que :

- La carte soit initialisée.
- La carte ne soit pas protégée contre l'écriture.
- Une opération d'initialisation ne soit pas déjà en cours d'exécution sur la carte.

Pour créer une partition vFlash vide :

1. Dans l'interface Web iDRAC6, sélectionnez **Système**→ onglet **vFlash**→ sous-onglet **Créer une partition vide**. La page **Créer une partition vide** s'affiche.
2. Entrez les informations mentionnées dans Tableau 15-2.

3 Cliquez sur **Appliquer**. Une nouvelle partition est créée. Une page indiquant le pourcentage de progression s'affiche.

Un message d'erreur s'affiche si :

- La carte est protégée contre l'écriture.
- Le nom d'étiquette correspond à l'étiquette d'une partition existante.
- Une valeur autre qu'un entier est entrée pour la taille de partition, la valeur dépasse l'espace disponible sur la carte ou la taille de partition est supérieure à 4 Go.
- Une opération d'initialisation est déjà en cours d'exécution sur la carte.

**REMARQUE :** la nouvelle partition est non formatée (BRUTE).

**Tableau 15-2. Options de la page Créer une partition vide**

| Champ | Description |
|---|---|
| **Index** | Sélectionnez un index de partition. Seuls les index inutilisés s'affichent dans la liste déroulante. L'index disponible le plus faible est sélectionné par défaut. Vous pouvez le remplacer par toute autre valeur d'index issue de la liste déroulante.<br>**REMARQUE :** dans le cas de la carte SD standard, seul l'index 1 est disponible. |
| **Étiquette** | Entrez une étiquette unique pour la nouvelle partition. Le nom d'étiquette peut contenir jusqu'à six caractères alphanumériques. N'incluez pas d'espace dans le nom d'étiquette. Les caractères s'affichent en majuscules.<br>**REMARQUE :** dans le cas de la carte SD standard, le nom d'étiquette est VFLASH par défaut et vous ne pouvez pas le modifier. |
| **Type d'émulation** | Sélectionnez le type d'émulation de la partition dans la liste déroulante. Les options disponibles sont **Disquette** et **Disque dur**. |
| **Taille** | Entrez la taille de partition en mégaoctets (Mo). La taille de partition maximale est de 4 Go, ou inférieure ou égale à l'espace disponible sur la carte SD vFlash.<br>**REMARQUE :** dans le cas de la carte SD standard, la taille de partition est de 256 Mo et ne peut pas être modifiée. |

### Création d'une partition à l'aide d'un fichier image

Vous pouvez créer une nouvelle partition sur la carte SD vFlash ou standard à l'aide d'un fichier image (disponible au format **.img** ou **.iso**). Vous pouvez créer une partition de type Disquette, Disque dur ou CD.

**REMARQUE :** vous devez disposer des privilèges Accès au média virtuel pour pouvoir créer des partitions.

Si un fichier image **.iso** (pour CD) est utilisé, une partition en lecture seule est créée. Si un fichier image **.img** (pour disquette et disque dur) est utilisé, une partition en lecture-écriture est créée.

La taille de la partition qui vient d'être créée est identique à la taille du fichier image. La taille du fichier image doit être :

- Inférieure ou égale à l'espace disponible sur la carte.
- Inférieure ou égale à 4 Go. La taille de partition maximale est de 4 Go.

Lorsque l'interface Web est utilisée, la taille de l'image pouvant être téléversée sur la carte SD vFlash est limitée à un maximum de 2 Go sur les navigateurs 32 bits et 64 bits (Internet Explorer et FireFox).

Lorsque l'interface RACADM et WSMAN est utilisée, la taille de l'image pouvant être téléversée sur une carte SD vFlash est de 4 Go au maximum.

Dans le cas de la carte SD standard, la taille de l'image doit être inférieure ou égale à 256 Mo.

Avant de créer une partition à partir d'un fichier image, veillez à ce que :

- La carte soit initialisée.
- La carte ne soit pas protégée contre l'écriture.
- Une opération d'initialisation ne soit pas déjà en cours d'exécution sur la carte.

**REMARQUE :** lorsque vous créez une partition à partir d'un fichier image, assurez-vous que le type d'image et le type d'émulation correspondent. iDRAC émule l'image en tenant compte du type d'image spécifié. Des problèmes peuvent survenir lorsque l'image téléversée et le type d'émulation ne correspondent pas. Par exemple, si la partition est créée à l'aide d'une image ISO et si le type d'émulation spécifié est Disque dur, le BIOS n'est pas en mesure de démarrer à partir de cette image.

Pour créer une partition vFlash à l'aide d'un fichier image :

1. Dans l'interface Web iDRAC6, sélectionnez **Système**→ onglet **vFlash**→ sous-onglet **Créer à partir de l'image**. La page **Créer une partition à partir d'un fichier image** s'affiche.

2 Entrez les informations mentionnées dans Tableau 15-3.

3 Cliquez sur **Appliquer**. Une nouvelle partition est créée.

Un message d'erreur s'affiche si :

- La carte est protégée contre l'écriture.
- Le nom d'étiquette correspond à l'étiquette d'une partition existante.
- La taille du fichier image est supérieure à 4 Go ou excède l'espace disponible sur la carte.
- Le fichier image n'existe pas ou son extension n'est ni **.img** ni **.iso**.
- Une opération d'initialisation est déjà en cours d'exécution sur la carte.

**Tableau 15-3. Options de la page Créer une partition à partir d'un fichier image**

| Champ | Description |
|---|---|
| **Index** | Sélectionnez un index de partition. Seuls les index inutilisés s'affichent dans la liste déroulante. L'index disponible le plus faible est sélectionné par défaut. Vous pouvez le remplacer par toute autre valeur d'index issue de la liste déroulante.<br>**REMARQUE :** dans le cas de la carte SD standard, seul l'index 1 est disponible. |
| **Étiquette** | Entrez une étiquette unique pour la nouvelle partition. Celle-ci peut contenir jusqu'à six caractères alphanumériques. N'incluez pas d'espaces dans le nom d'étiquette. Les caractères s'affichent en majuscules.<br>**REMARQUE :** dans le cas de la carte SD standard, le nom d'étiquette est VFLASH et ne peut pas être modifié. |
| **Type d'émulation** | Sélectionnez le type d'émulation de la partition dans la liste déroulante. Les options disponibles sont **Disquette**, **Disque dur** et **CD**. |
| **Emplacement d'image** | Cliquez sur **Parcourir** et spécifiez l'emplacement du fichier image. Seuls les types de fichier **.img** ou **.iso** sont pris en charge. |

### Formatage d'une partition

Vous pouvez formater une partition existante sur la carte SD vFlash en fonction du type de système de fichiers. Les types de système de fichiers pris en charge sont EXT2, EXT3, FAT16 et FAT32. La carte SD standard aux fonctionnalités vFlash limitées prend uniquement en charge le format FAT32.

Vous pouvez uniquement formater les partitions de type Disque dur ou Disquette. Le formatage de la partition de type CD n'est pas pris en charge. Vous ne pouvez pas formater les partitions en lecture seule.

**REMARQUE :** vous devez disposer des privilèges Accès au média virtuel pour pouvoir formater des partitions.

Avant de formater la partition, veillez à ce que :

- La carte soit activée.
- La partition ne soit pas connectée.
- La carte ne soit pas protégée contre l'écriture.
- Une opération d'initialisation ne soit pas déjà en cours d'exécution sur la carte.

Pour formater la partition vFlash :

1. Dans l'interface Web iDRAC6, sélectionnez **Système**→ onglet **vFlash**→ sous-onglet **Formater**. La page **Formater la partition** s'affiche.
2. Entrez les informations mentionnées dans Tableau 15-4.
3. Cliquez sur **Appliquer**. Un message d'avertissement indiquant que toutes les données de la partition seront effacées s'affiche. Cliquez sur **OK**. La partition sélectionnée est formatée en fonction du type de système de fichiers spécifié.

   Un message d'erreur s'affiche si :

   - La carte est protégée contre l'écriture.
   - Une opération d'initialisation est déjà en cours d'exécution sur la carte.

**Tableau 15-4. Options de la page Formater la partition**

| Champ | Description |
|---|---|
| **Étiquette** | Sélectionnez le nom de la partition que vous souhaitez formater. La première partition disponible est sélectionnée par défaut.<br>Toutes les partitions existantes de type Disquette ou Disque dur sont disponibles dans la liste déroulante. Les partitions connectées ou en lecture seule ne sont pas disponibles dans la liste déroulante. |
| **Type de format** | Sélectionnez le type de système de fichiers que vous souhaitez utiliser pour formater la partition. Les options disponibles sont EXT2, EXT3, FAT16 et FAT32. |

## Affichage des partitions disponibles

Assurez-vous que la carte SD vFlash ou standard est activée pour afficher la liste des partitions disponibles.

Pour afficher les partitions disponibles sur la carte :

1. Dans l'interface Web iDRAC6, sélectionnez **Système→ vFlash→** sous-onglet **Gérer**. La page **Gérer les partitions** répertorie les partitions disponibles.
2. Pour chaque partition, vous pouvez afficher les informations mentionnées dans Tableau 15-5.

**Tableau 15-5. Affichage des partitions disponibles**

| Champ | Description |
|---|---|
| **Index** | Les partitions sont indexées de 1 à 16. L'index de partition est unique à une partition particulière. Elle est spécifiée lors de la création de la partition. |
| **Étiquette** | Identifie la partition. Elle est spécifiée lors de la création de la partition. |
| **Taille** | Taille de la partition en mégaoctets (Mo). |

**Tableau 15-5. Affichage des partitions disponibles *(suite)***

| Champ | Description |
|---|---|
| Lecture seule | État d'accès en lecture-écriture de la partition.<br>• Coché = partition en lecture seule.<br>• Décoché = partition en lecture-écriture<br>**REMARQUE :** dans le cas de la carte SD standard, la partition est en lecture-écriture, et cette colonne n'est pas affichée. |
| Connecté | Indique si la partition est visible au système d'exploitation en tant que périphérique USB. Pour connecter ou déconnecter des partitions, consultez la section « Connexion et déconnexion d'une partition », à la page 307. |
| Type | Affiche si le type de partition est Disquette, Disque dur ou CD. |
| État | Condition d'une opération en cours ou de la dernière opération effectuée sur la partition, avec le pourcentage de progression. Les valeurs de condition sont les suivantes :<br>• Inactivité : aucune opération n'est effectuée.<br>• Formatage : la partition est en cours de formatage.<br>• Création : la partition est en cours de création. |

## Modification d'une partition

Assurez-vous que la carte est activée pour modifier la partition.

Vous pouvez remplacer une partition en lecture seule par une partition en lecture-écriture ou inversement. Pour ce faire :

1. Dans l'interface Web iDRAC6, sélectionnez **Système**→ onglet v**Flas**h→ sous-onglet **Gérer**. La page **Gérer les partitions** s'affiche.
2. Dans la colonne **Lecture seule**, cochez la case correspondant à la partition, ou aux partitions, que vous souhaitez définir sur Lecture seule, ou décochez la case de celle(s) que vous souhaitez définir sur lecture-écriture.

**REMARQUE :** si la partition est de type CD, l'état est lecture seule et la case est cochée par défaut. Vous ne pouvez pas modifier l'état pour le définir sur lecture-écriture.
Si la partition est connectée, la case à cocher est grisée.
Dans le cas de la carte SD standard, la partition est en lecture-écriture et la colonne **Lecture seule** n'est pas affichée.

3 Cliquez sur **Appliquer**. Les partitions passent en lecture seule ou en lecture-écriture selon les sélections effectuées.

### Connexion et déconnexion d'une partition

Vous pouvez connecter une ou plusieurs partitions en tant que périphérique de stockage de masse USB virtuel de manière à ce qu'elles soient visibles au système d'exploitation et au BIOS en tant que périphériques de stockage de masse. Lorsque plusieurs partitions sont connectées simultanément, elles sont présentées dans l'ordre croissant au système d'exploitation hôte en fonction de l'index. L'attribution de la lettre de lecteur correspondante est contrôlée par le système d'exploitation.

Si vous déconnectez une partition, celle-ci n'est plus vue en tant que périphérique de stockage de masse USB virtuel dans le système d'exploitation hôte et est supprimée du menu de séquence d'amorçage du BIOS.

Si vous connectez ou déconnectez une partition, le bus USB du système est réinitialisé. Ceci peut avoir une incidence sur les applications (par exemple, le système d'exploitation) qui utilisent vFlash et déconnectera les sessions Média virtuel d'iDRAC.

**REMARQUE :** vous devez disposer des privilèges Accès au média virtuel pour connecter ou déconnecter une partition.

Avant de connecter ou de déconnecter une partition, veillez à ce que :

- La carte soit activée.
- Une opération d'initialisation ne soit pas déjà en cours d'exécution sur la carte.

Pour connecter ou déconnecter des partitions :

1 Dans l'interface Web iDRAC6, sélectionnez **Système**→ onglet **vFlash**→ sous-onglet **Gérer**. La page **Gérer les partitions** s'affiche.

2 Dans la colonne **Connecté**, cochez la case correspondant à la/aux partitions que vous souhaitez connecter ou décochez la case correspondant à celle(s) que vous souhaitez déconnecter.

**REMARQUE :** les partitions déconnectées ne s'affichent pas dans la séquence d'amorçage.

3 Cliquez sur **Appliquer**. Les partitions sont connectées ou déconnectées en fonction des sélections effectuées.

#### Comportement du système d'exploitation pour les partitions connectées

Lorsque les partitions sont connectées et que le système d'exploitation hôte est Windows, les lettres de lecteur attribuées aux partitions connectées sont contrôlées par le système d'exploitation.

Si une partition est en lecture seule, elle le demeure comme dans le système d'exploitation hôte.

Si le système d'exploitation hôte ne prend pas en charge le système de fichiers d'une partition connectée, vous ne pouvez pas lire ni modifier le contenu de la partition à partir du système d'exploitation hôte. Par exemple, une partition de type EXT2 ne peut pas être lue à partir d'un système d'exploitation Windows.

Lorsque vous modifiez le nom d'étiquette d'une partition connectée à partir du système d'exploitation hôte, cette opération n'a aucune incidence sur le nom d'étiquette stocké par iDRAC pour cette partition.

### Suppression de partitions existantes

**REMARQUE :** vous pouvez supprimer des partitions existantes de la carte SD vFlash ou standard.

Avant de supprimer des partitions existantes, assurez-vous que :

- La carte soit activée.
- La carte ne soit pas protégée contre l'écriture.
- La partition ne soit pas connectée.
- Une opération d'initialisation ne soit pas déjà en cours d'exécution sur la carte.

Pour supprimer une ou des partition(s) existante(s) :

1 Dans l'interface Web iDRAC6, sélectionnez **Système**→ onglet **vFlash**→ sous-onglet **Gérer**. La page **Gérer les partitions** s'affiche.

2 Dans la colonne **Supprimer**, cliquez sur l'icône de suppression correspondant à la partition, ou aux partitions, que vous souhaitez supprimer et cliquez sur **Appliquer**. Les partitions sont supprimées.

### Téléchargement du contenu d'une partition

Vous pouvez télécharger le contenu d'une partition vFlash sur un emplacement local ou distant en tant que fichier image, au format **.img** ou **.iso**. L'emplacement local se trouve sur le système de gestion à partir duquel l'interface Web iDRAC6 Web s'exécute. L'emplacement distant est un emplacement réseau mappé sur la station de gestion.

**REMARQUE :** vous devez disposer des privilèges Accès au média virtuel pour pouvoir télécharger des partitions.

Avant de télécharger le contenu sur un emplacement local ou distant, veillez à ce que :

- La carte soit activée.
- Une opération d'initialisation ne soit pas déjà en cours d'exécution sur la carte.
- Dans le cas d'une partition en lecture-écriture, elle ne doit pas être connectée.

Pour télécharger le contenu de la partition vFlash sur un emplacement de votre système :

1. Dans l'interface Web iDRAC6, sélectionnez **Système**→ onglet v**Flash**→ sous-onglet **Télécharger**. La page **Télécharger la partition** s'affiche.
2. Dans le menu déroulant **Nom**, sélectionnez la partition que vous souhaitez télécharger. Toutes les partitions existantes s'affichent dans la liste, à l'exception de celles qui sont connectées. La première partition est sélectionnée par défaut.
3. Cliquez sur **Télécharger**.
4. Spécifiez l'emplacement d'enregistrement du fichier.

   Si seul l'emplacement du dossier est spécifié, le nom de la partition est alors utilisé en tant que nom de fichier, ainsi que l'extension **.iso** pour les partitions de type CD, et **.img** pour les partitions de type Disquette et Disque dur.
5. Cliquez sur **Save** (Enregistrer). Le contenu de la partition sélectionnée est téléchargé vers l'emplacement spécifié.

### Démarrage à partir d'une partition

Vous pouvez définir une partition vFlash connectée en tant que périphérique de démarrage de la prochaine opération de démarrage. La partition vFlash doit contenir une image d'amorçage (au format **.img** ou **.iso**) pour la définir en tant que périphérique de démarrage. Assurez-vous que la carte est activée pour définir une partition en tant que périphérique de démarrage et pour effectuer l'opération de démarrage.

**REMARQUE :** vous devez disposer des privilèges Accès au média virtuel pour pouvoir définir une partition en tant que périphérique de démarrage.

Vous pouvez effectuer l'opération de démarrage de la carte SD vFlash ou standard. Pour connaître les étapes à suivre, consultez la section « Périphérique de démarrage initial », à la page 84.

**REMARQUE :** si le BIOS système ne prend pas en charge vFlash en tant que périphérique de démarrage initial, il se peut alors que la ou les partition(s) vFlash connectée(s) ne soi(en)t pas répertoriée(s) dans le menu déroulant **Périphérique de démarrage initial**. Par conséquent, veillez à mettre à jour le BIOS vers la dernière version qui permet de définir la partition vFlash en tant que périphérique de démarrage initial. Si le BIOS correspond à la dernière version, le redémarrage du serveur indique alors au BIOS d'informer iDRAC qu'il prend en charge vFlash en tant que périphérique de démarrage initial, et iDRAC répertorie la partition vFlash dans le menu déroulant **Périphérique de démarrage initial**.

## Gestion de partitions vFlash via la RACADM

Vous pouvez utiliser la sous-commande `vFlashPartition` pour créer, supprimer, répertorier ou afficher la condition des partitions sur une carte SD vFlash ou standard déjà initialisée. Le format est le suivant :

```
racadm vflashpartition <créer | supprimer | condition |
répertorier> <options>
```

**REMARQUE :** vous devez disposer des privilèges Accès au média virtuel pour pouvoir procéder à la gestion de la partition vFlash.

Options valides :

| | |
|---|---|
| -i <index> | Index de la partition pour laquelle cette commande s'applique.<br><index> doit être un entier compris entre 1 et 16.<br>**REMARQUE :** dans le cas de la carte SD standard, la valeur d'index est limitée à 1 car seule une partition d'une taille de 256 Mo est prise en charge. |

Options valides uniquement avec l'action de création :

| | |
|---|---|
| -o <nom> | Nom qui s'affiche lorsque la partition est montée sur le système d'exploitation.<br><nom> doit être une chaîne incluant jusqu'à six caractères alphanumériques et ne doit pas contenir d'espaces. |
| -e <type> | Type d'émulation de la partition. <type> doit être Disquette, CD-DVD ou Disque dur. |
| -t <type> | Créez une partition de type <type>. <type> doit être :<br>• vide - Créez une partition vide.<br>  • -s <taille> - Taille de partition en Mo.<br>  • -f <type>- Type de format de la partition en fonction du type de système de fichiers. Les options valides sont RAW, FAT16, FAT32, EXT2 ou EXT3.<br>• image - Créez une partition à l'aide d'une image relative à l'iDRAC. Les options suivantes sont valides avec le type d'image :<br>  • -l <chemin> - Spécifie le chemin distant relatif à l'iDRAC. Le chemin peut se trouver sur un lecteur monté :<br>  Chemin SMB : //<ip ou domaine>/<nom_partage> /<chemin_vers_image><br>  Chemin NFS : <adresse_ip>:/<chemin_vers_image><br>  • -u <utilisateur> - Nom d'utilisateur en vue de l'accès à l'image distante.<br>  • -p <mot de passe> - Mot de passe en vue de l'accès à l'image distante. |

Options valides uniquement avec l'action de condition :

| | |
|---|---|
| -a | Affiche la condition des opérations sur toutes les partitions existantes. |

### Création d'une partition

- Pour créer une partition vide de 20 Mo :

  ```
  racadm vflashpartition create -i 1 -o drive1 -t
  empty -e HDD -f fat16 -s 20
  ```

- Pour créer une partition à l'aide d'un fichier image sur un système distant :

  ```
  racadm vflashpartition create –i 1 –o drive1 –e
  HDD –t image –l //myserver/sharedfolder/foo.iso –u
  root –p mypassword
  ```

  **REMARQUE :** cette commande est sensible à la casse pour l'extension du nom de fichier de l'image. Si l'extension du nom de fichier est en majuscule, par exemple FOO.ISO au lieu de FOO.iso, la commande redevient alors une erreur de syntaxe.

**REMARQUE :** la création d'une partition à l'aide d'un fichier image n'est pas prise en charge par la RACADM locale.

### Suppression d'une partition

- Pour supprimer une partition :

  ```
  racadm vflashpartition delete -i 1
  ```

- Pour supprimer toutes les partitions, réinitialisez la carte SD vFlash. Pour plus d'informations, voir « Initialisation de la carte SD vFlash ou standard », à la page 299.

### Obtention de la condition d'une partition

- Pour obtenir la condition de l'opération sur la partition 1 :

  ```
  racadm vflashpartition status -i 1
  ```

- Pour obtenir la condition de toutes les partitions existantes :

  ```
  racadm vflashpartition status -a
  ```

### Affichage des informations relatives à la partition

Pour répertorier toutes les partitions existantes et leurs propriétés :

```
racadm vflashpartition list
```

### Démarrage à partir d'une partition

- Pour répertorier les périphériques disponibles dans la liste de démarrage :

  ```
  racadm getconfig -g cfgServerInfo -o
  cfgServerFirstBootDevice
  ```

  S'il s'agit d'une carte SD vFlash, les noms d'étiquette des partitions connectées figurent dans la liste de démarrage. S'il s'agit d'une carte SD standard et si la partition est connectée, VFLASH apparaît alors dans la liste de démarrage.

- Pour définir une partition vFlash en tant que périphérique de démarrage :

  ```
  racadm config -g cfgServerInfo -o
  cfgServerFirstBootDevice " <nom de la partition
  vFlash> "
  ```

  où <nom de la partition vFlash> correspond au nom d'étiquette de la carte SD vFlash et VFLASH à celui de la carte SD standard.

  **REMARQUE :** lorsque vous exécutez cette commande, le nom de la partition vFlash est automatiquement défini pour démarrer une seule fois, autrement dit **cfgserverBootOnce** est défini sur 1. Démarrer une seule fois permet de démarrer le périphérique sur la partition à une seule reprise et ne le maintient pas de manière permanente en première position dans la séquence d'amorçage.

### Connexion ou déconnexion d'une partition

- Pour connecter une partition :

  ```
  racadm config -g cfgvflashpartition  -i 1 -o
  cfgvflashPartitionAttachState 1
  ```

- Pour déconnecter une partition :

  ```
  racadm config -g cfgvflashpartition  -i 1 -o
  cfgvflashPartitionAttachState 0
  ```

### Modification d'une partition

- Pour remplacer une partition en lecture seule par une partition en lecture-écriture :

  ```
  racadm config -g cfgvflashpartition  -i 1 -o
  cfgvflashPartitionAccessType 1
  ```

- Pour remplacer une partition en lecture-écriture par une partition en lecture seule :

  ```
  racadm config -g cfgvflashpartition  -i 1 -o
  cfgvflashPartitionAccessType 0
  ```

Pour des informations supplémentaires sur les sous-commandes RACADM et les définitions d'objet et de groupe de bases de données des propriétés d'iDRAC6, consultez le *Guide de référence de la ligne de commande RACADM pour iDRAC6 et CMC* disponible sur le site Web du support de Dell à l'adresse **support.dell.com/manuals**.

# Questions les plus fréquentes

### À quel moment la carte SD vFlash ou standard est-elle verrouillée ?

Le média flash virtuel est verrouillé par le contrôleur iDRAC lorsque l'opération qu'il exécute requiert un accès exclusif au média. Par exemple, lors d'une opération d'initialisation.

# 16

# Contrôle et gestion de l'alimentation

Les systèmes Dell PowerEdge intègrent de nombreuses nouvelles fonctionnalités améliorées de gestion de l'alimentation. La plateforme entière, du matériel au micrologiciel au logiciel de gestion de systèmes, a été conçue dans l'optique de réduire, de contrôler et de gérer l'alimentation.

La conception du matériel de base a été optimisée selon la perspective de l'alimentation :

- Des blocs d'alimentation haute performance et des régulateurs de tension ont été incorporés dans la conception.
- Le cas échéant, des composants dotés d'une consommation inférieure ont été sélectionnés.
- La conception du châssis optimise l'écoulement de l'air à travers le système pour réduire la puissance de ventilation.

Les systèmes PowerEdge comportent de nombreuses fonctionnalités de contrôle et de gestion de l'alimentation.

- **Inventaire énergétique et bilan de puissance :** au démarrage, un inventaire système permet de calculer un bilan de puissance système de la configuration actuelle.
- **Plafonnement de l'alimentation :** les systèmes peuvent comporter un limiteur pour maintenir un plafond d'alimentation spécifié.
- **Contrôle de l'alimentation :** iDRAC6 interroge les blocs d'alimentation pour recueillir des mesures d'alimentation. iDRAC6 recueille un historique des mesures d'alimentation et calcule les moyennes d'exploitation et les crêtes. À l'aide de l'interface Web iDRAC6, vous pouvez consulter les informations affichées dans l'écran **Contrôle de l'alimentation**.

## Inventaire énergétique, bilan de puissance et plafonnement

Sur le plan de l'utilisation, vous pouvez ne disposer que d'un refroidissement limité au niveau du rack. Avec un plafond d'alimentation défini par l'utilisateur, vous pouvez allouer l'alimentation conformément aux besoins pour obtenir les performances requises.

iDRAC6 surveille la consommation énergétique et limite dynamiquement les processeurs en fonction du plafond d'alimentation que vous avez défini afin d'optimiser les performances tout en répondant à vos exigences en matière d'alimentation.

## Power Monitoring (Surveillance de l'alimentation)

iDRAC6 surveille continuellement la consommation énergétique dans les serveurs PowerEdge. iDRAC6 calcule les valeurs d'alimentation suivantes et fournit les informations via son interface Web ou la CLI RACADM :

- Consommation énergétique cumulée
- Consommation d'alimentation moyenne, minimale et maximale
- Valeurs de hauteur d'alimentation
- Consommation énergétique (également affichée sous forme de graphiques dans l'interface Web)

## Configuration et gestion de l'alimentation

Vous pouvez utiliser l'interface Web iDRAC6 et l'interface de ligne de commande (CLI) de la RACADM pour gérer et configurer les commandes d'alimentation du système PowerEdge. Vous pouvez notamment :

- afficher l'état de l'alimentation du serveur,
- exécuter des opérations de contrôle de l'alimentation sur le serveur (par exemple, mise sous tension, mise hors tension, réinitialisation du système, cycle d'alimentation),

- afficher les informations du bilan de puissance du serveur et des blocs d'alimentation installés, notamment la consommation énergétique potentielle minimale et maximale,
- afficher et configurer le seuil du bilan de puissance du serveur,

# Affichage de la condition d'intégrité des blocs d'alimentation.

La page **Blocs d'alimentation** indique la condition et la puissance des blocs d'alimentation installés dans le serveur.

### Utilisation de l'interface Web

Pour afficher la condition d'intégrité des blocs d'alimentation :

1. Ouvrez une session sur l'interface Web iDRAC6.
2. Sélectionnez **Blocs d'alimentation** dans l'arborescence du système. La page **Blocs d'alimentation** affiche les informations suivantes :
   - **Condition de la redondance des blocs d'alimentation** : les valeurs possibles sont les suivantes :
   - **Intégrale** : les blocs d'alimentation installés au sein du système sont du même type et fonctionnent correctement.
   - **Perdue** : dans les systèmes dotés de deux unités d'alimentation, les blocs d'alimentation installés au sein du système sont de types différents, ou l'un d'entre eux ne fonctionne pas correctement ou a été retiré. Dans les systèmes dotés de quatre unités d'alimentation, les blocs d'alimentation installés au sein du système sont de types différents, ou deux ou trois d'entre eux ne fonctionnent pas correctement ou ont été retirés.
   - **Désactivée** : un seul des blocs d'alimentation est disponible. Aucune redondance n'existe.
   - **Dégradée** (concerne uniquement les systèmes dotés de quatre unités d'alimentation) : quatre unités d'alimentation sont installées au sein du système, mais l'une d'entre elles ne fonctionne pas correctement ou a été retirée.

- **Éléments des blocs d'alimentation individuels** : les valeurs possibles sont les suivantes :

– **Condition** indique :
  - **OK** signifie que le bloc d'alimentation est présent et communique avec le serveur.
  - **Avertissement** signifie que seules des alertes d'avertissement ont été émises et qu'une action corrective doit être prise par l'administrateur. 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 émise. Une condition de panne indique une panne d'alimentation sur le serveur et la nécessité d'actions correctives immédiates.

– **Emplacement** indique le nom du bloc d'alimentation : PS-n, n étant le numéro du bloc d'alimentation.

– **Type** indique le type de bloc d'alimentation, tel que CA ou CC (conversion de tension CA-CC ou CC-CC).

– **Puissance d'entrée** indique la puissance d'entrée du bloc d'alimentation, c'est-à-dire la charge d'alimentation CA maximale que le système peut faire supporter au centre de données.

– **Puissance maximale** indique la puissance maximale du bloc d'alimentation, c'est-à-dire la puissance CC disponible pour le système. Cette valeur permet de confirmer qu'une capacité de bloc d'alimentation suffisante est disponible pour la configuration du système.

– **Condition en ligne** indique l'état des blocs d'alimentation : présent et OK, entrée perdue, absent ou panne prévisible.

– **Version ML** indique la version de micrologiciel du bloc d'alimentation.

**REMARQUE :** la **puissance maximale** diffère de la **puissance d'entrée** selon l'efficacité du bloc d'alimentation. Par exemple, si l'efficacité du bloc d'alimentation est de 89 % et la **puissance maximale** de 717 W, la **puissance d'entrée** est évaluée à 797 W.

### Utilisation de la RACADM

Ouvrez une console texte Telnet/SSH sur iDRAC, ouvrez une session et tapez :

```
racadm getconfig -g cfgServerPower
```

# Affichage du bilan de puissance

Le serveur fournit des aperçus de la condition du bilan de puissance du sous-système d'alimentation sur la page **Informations du bilan de puissance**.

## Utilisation de l'interface Web

**REMARQUE :** vous devez disposer du privilège **Administrateur** pour effectuer des tâches de gestion de l'alimentation.

1. Ouvrez une session sur l'interface Web iDRAC6.
2. Cliquez sur l'onglet **Alimentation**.
3. Sélectionnez l'option **Bilan de puissance**.
4. La page **Informations du bilan de puissance** s'affiche.

Le premier tableau indique les limites minimale et maximale des seuils d'alimentation définis par l'utilisateur pour la configuration système en cours. Elles représentent la plage des consommations énergétiques CA que vous pouvez définir comme plafond système. Une fois sélectionné, ce plafond constitue la charge d'alimentation CA maximale que le système peut faire supporter au centre de données.

**Consommation énergétique minimale du système** affiche la valeur du seuil énergétique le plus bas par défaut.

**Consommation énergétique maximale du système** affiche la valeur du seuil énergétique le plus haut par défaut. Cette valeur correspond également à la consommation énergétique maximale absolue de la configuration système actuelle.

## Utilisation de la RACADM

Ouvrez une console texte Telnet/SSH sur iDRAC, ouvrez une session et tapez :

```
racadm getconfig -g cfgServerPower
```

**REMARQUE :** pour des informations supplémentaires sur la commande cfgServerPower, y compris les détails de sortie, voir cfgServerPower dans le Guide de référence de la ligne de *commande RACADM pour iDRAC6 et CMC* sur le site de support Dell à l'adresse **dell.com/support/manuals**.

# Seuil du bilan de puissance

Le seuil du bilan de puissance, s'il est activé, permet de définir une limite de plafonnement de l'alimentation pour le système. Les performances du système sont dynamiquement ajustées afin de maintenir la consommation énergétique à proximité du seuil spécifié. La consommation énergétique réelle peut être inférieure pour les faibles charges de travail et peut momentanément excéder le seuil jusqu'à ce que les ajustements de performances soient terminés.

Si vous cochez **Activé** pour Seuil du bilan de puissance, le système applique le seuil spécifié par l'utilisateur. Si vous laissez la valeur Seuil du bilan de puissance **non cochée**, le système n'est pas plafonné en alimentation.
Par exemple, pour une configuration système donnée, la consommation énergétique potentielle maximale est de 700 W et la consommation énergétique potentielle minimale est de 500 W. Vous pouvez spécifier et activer un seuil du bilan de puissance pour ramener la consommation actuelle de 650 W à 525 W. Par la suite, les performances du système seront dynamiquement ajustées afin que la consommation énergétique ne dépasse pas le seuil de 525 W spécifié par l'utilisateur.

### Utilisation de l'interface Web

1. Ouvrez une session sur l'interface Web iDRAC6.
2. Cliquez sur l'onglet **Alimentation**.
3. Sélectionnez l'option **Bilan de puissance**. La page **Informations du bilan de puissance** s'affiche.
4. Entrez une valeur en watts, BTU/h ou pourcentage dans le tableau **Bilan de puissance**. La valeur spécifiée en watts ou BTU/h est la valeur limite du seuil du bilan de puissance. Si vous spécifiez une valeur en pourcentage, il s'agit d'un pourcentage de l'intervalle de la consommation énergétique potentielle minimale-maximale. Par exemple, un seuil de 100 % signifie une consommation énergétique potentielle maximale tandis que 0 % signifie une consommation énergétique potentielle minimale.

   **REMARQUE :** le seuil du bilan de puissance ne peut pas être supérieur à la consommation énergétique potentielle maximale, ni inférieur à la consommation énergétique potentielle minimale.

5 Sélectionnez **Activé** pour activer le seuil. Le système applique le seuil défini par l'utilisateur. Si vous décochez la case, aucun seuil énergétique n'est appliqué au système.

6 Cliquez sur **Appliquer les modifications**.

### Utilisation de la RACADM

```
racadm config -g cfgServerPower -o
cfgServerPowerCapWatts <valeur du plafond
d'alimentation en watts>

racadm config -g cfgServerPower -o
cfgServerPowerCapBTUhr <valeur du plafond
d'alimentation en BTU/h>

racadm config -g cfgServerPower -o
cfgServerPowerCapPercent <valeur du plafond
d'alimentation en % >

racadm config -g cfgServerPower -o
cfgServerPowerCapEnable <1 pour activer, 0 pour
désactiver>
```

**REMARQUE :** lors de la définition du seuil du bilan de puissance en BTU/h, la conversion en watts est arrondie à la valeur entière la plus proche. Lors de la relecture du seuil du bilan de puissance, la conversion de watts en BTU/h est de nouveau arrondie de cette manière. En conséquence, la valeur inscrite peut être nominalement différente de la valeur lue ; par exemple, un seuil défini sur 600 BTU/h sera relu avec la valeur 601 BTU/h.

## Affichage du contrôle de l'alimentation

### Utilisation de l'interface Web

Pour afficher les données de contrôle de l'alimentation :

1 Ouvrez une session sur l'interface Web iDRAC6.

2 Sélectionnez **Contrôle de l'alimentation** dans l'arborescence du système. La page **Contrôle de l'alimentation** s'affiche.

La section suivante décrit les informations se trouvant sur la page **Contrôle de l'alimentation** :

#### Power Monitoring (Surveillance de l'alimentation)

- **Condition : OK** indique que les blocs d'alimentation sont présents et communiquent avec le serveur, **Avertissement** indique qu'une alerte d'avertissement a été émise et **Grave** indique qu'une alerte de panne a été émise.
- **Nom du capteur :** niveau du système de la carte système. Cette description indique que le capteur est surveillé par son emplacement dans le système.
- **Lecture :** la consommation énergétique actuelle en watts/BTU/h.
- **Seuil d'avertissement** : affiche la consommation de puissance acceptable (en watts et en BTU/h) recommandée pour le fonctionnement du système. Une consommation énergétique qui excèderait cette valeur entraînerait des événements d'avertissement.
- **Seuil de panne** : affiche la consommation de puissance la plus élevée acceptable (en watts et en BTU/h) requise pour le fonctionnement du système. Une consommation énergétique qui excèderait cette valeur entraînerait des événements critiques/de panne.

#### Intensité du courant

- **Emplacement :** indique le nom du bloc d'alimentation : PS-n, n étant le numéro du bloc d'alimentation.
- **Lecture :** la consommation énergétique actuelle en ampères

#### Statistiques de consommation de puissance

- **Consommation énergétique** affiche la consommation énergétique cumulée actuelle du serveur, mesurée à l'entrée des blocs d'alimentation. La valeur est indiquée en KWh et est une valeur cumulée qui représente l'énergie totale utilisée par le système. Vous pouvez réinitialiser cette valeur à l'aide du bouton **Réinitialiser**.
- **Puissance maximale du système** spécifie la moyenne de puissance maximale sur 1 minute du système depuis l'heure de début des mesures. Vous pouvez réinitialiser cette valeur à l'aide du bouton **Réinitialiser.**

- **Intensité système maximale** spécifie la valeur de puissance maximale dans l'intervalle spécifié par les heures de consommation initiale et maximale. Vous pouvez réinitialiser cette valeur à l'aide du bouton **Réinitialiser.**
- **Heure de début des mesures** affiche la date et l'heure enregistrées depuis que la dernière statistique a été effacée et qu'un nouveau cycle de mesures a débuté. Pour **Consommation énergétique**, vous pouvez réinitialiser la valeur avec le bouton **Réinitialiser**, mais elle persistera jusqu'à une opération de réinitialisation ou de basculement du système.
  Pour **Puissance système maximale** et **Intensité système maximale**, vous pouvez réinitialiser la valeur avec le bouton **Réinitialiser**, mais elle persistera également jusqu'à une opération de réinitialisation ou de basculement du système.
- **Heure de fin des mesures** affiche la date et l'heure de calcul de la consommation d'énergie du système pour l'affichage. **Heure de consommation maximale** affiche l'heure à laquelle la consommation maximale a été enregistrée.

**REMARQUE :** les statistiques de la consommation énergétique sont conservées lors des réinitialisations du système et reflètent ainsi l'ensemble des activités qui se sont produites dans l'intervalle entre les heures de début et de fin indiquées. Le bouton **Réinitialiser** permet de réinitialiser le champ respectif sur la valeur zéro. Dans le tableau suivant, les données de consommation énergétique ne sont pas conservées lors des réinitialisations du système et sont mises à zéro. Les valeurs d'alimentation affichées sont des moyennes cumulées au cours de l'intervalle de temps respectif (minute, heure, jour et semaine précédents). Comme les intervalles de temps du début à la fin peuvent ici différer de ceux des statistiques de consommation de puissance, les valeurs d'alimentation maximales (maximum en watts par rapport à la consommation énergétique maximale) peuvent différer.

#### Consommation énergétique

- Affiche la consommation énergétique moyenne, maximale et minimale du système au cours de la minute, de l'heure, du jour et de la semaine précédents.
- Consommation énergétique moyenne : moyenne de la minute précédente, heure précédente, jour précédent et semaine précédente.
- Consommation énergétique maximale et consommation énergétique minimale : les consommations énergétiques maximale et minimale observées au cours de l'intervalle de temps donné.
- Heure d'alimentation maximale et minimale : heure à laquelle les consommations énergétiques maximale et minimale ont été observées.

#### Hauteur

- **La hauteur instantanée du système** indique la différence entre l'alimentation disponible dans les blocs d'alimentation et la consommation énergétique actuelle du système.
- **La hauteur maximale du système** indique la différence entre l'alimentation disponible dans les blocs d'alimentation et la consommation énergétique maximale du système.

#### Afficher le graphique

Cliquez sur **Afficher le graphique** pour afficher les graphiques indiquant les consommations énergétique et de courant d'iDRAC6 en watts et ampères, respectivement, au cours de la dernière heure. L'utilisateur peut consulter ces statistiques pour la semaine précédente à l'aide du menu déroulant proposé au-dessus des graphiques.

**REMARQUE :** chaque point de données tracé sur les graphiques représente la moyenne des lectures sur une période de 5 minutes. Par conséquent, les graphiques peuvent ne pas refléter les brèves fluctuations d'alimentation énergétique ou de courant.

### Utilisation de la RACADM

Ouvrez une console texte Telnet/SSH sur iDRAC, ouvrez une session et tapez :

```
racadm getconfig -g cfgServerPower
```

Pour des informations supplémentaires sur la commande **cfgServerPower**, y compris les détails de sortie, voir **cfgServerPower** dans le *Guide de référence de la ligne de commande RACADM pour iDRAC6 et CMC* sur le site de support Dell à l'adresse **dell.com/support/manuals**.

## Exécution de tâches de contrôle de l'alimentation sur le serveur

**REMARQUE :** pour réaliser des tâches de gestion de l'alimentation, vous devez disposer du privilège **Administrateur de contrôle du châssis**.

iDRAC6 vous permet d'effectuer plusieurs actions de gestion de l'alimentation à distance, par exemple un arrêt méthodique.

### Utilisation de l'interface Web

1. Ouvrez une session sur l'interface Web iDRAC6.
2. Cliquez sur l'onglet **Alimentation**. La page **Contrôle de l'alimentation** s'affiche.
3. Sélectionnez l'une des **opérations de contrôle de l'alimentation** suivantes en cliquant sur le bouton radio correspondant :
   - **Mise sous tension du système** permet de mettre le serveur sous tension (équivaut à appuyer sur le bouton d'alimentation quand le serveur est hors tension). Cette option est désactivée si le système est déjà sous tension.
   - **Mise hors tension du système** permet d'éteindre le serveur. Cette option est désactivée si le système est déjà hors tension.
   - **NMI (Interruption non masquable)** génère une NMI pour arrêter le système.
   - **Arrêt normal** arrête le système.

     **REMARQUE :** assurez-vous que l'option d'arrêt est configurée pour le système d'exploitation avant d'effectuer un arrêt normal à l'aide de cette option. Si vous utilisez cette option sans la configurer sur le système d'exploitation, le système géré redémarre et le système ne s'arrête pas.
   - **Réinitialisation du système (démarrage à chaud)** réinitialise le système sans le mettre hors tension. Cette option est désactivée si le système est déjà hors tension.
   - **Exécuter un cycle d'alimentation sur le système (démarrage à froid)** arrête, puis redémarre le système. Cette option est désactivée si le système est déjà hors tension.
4. Cliquez sur **Appliquer**. Une boîte de dialogue de confirmation s'affiche.
5. Cliquez sur **OK** pour effectuer la tâche de gestion de l'alimentation sélectionnée (réinitialisation du système, par exemple).

### Utilisation de la RACADM

Ouvrez une console texte Telnet/SSH sur le serveur, ouvrez une session et tapez :

```
racadm serveraction <action>
```

où `<action>` a pour valeur powerup (mise sous tension), powerdown (mise hors tension), powercycle (cycle d'alimentation), hardreset (réinitialisation matérielle) ou powerstatus (condition de l'alimentation).

# 17

# Utilisation de l'utilitaire de configuration iDRAC6

## Présentation

L'utilitaire de configuration iDRAC6 est un environnement de configuration de prédémarrage vous permettant d'afficher et de définir les paramètres d'iDRAC6 et du serveur géré. Vous pouvez notamment :

- afficher les numéros de révision du micrologiciel pour le micrologiciel iDRAC6 et le micrologiciel de fond de panier principal,
- activer ou désactiver le réseau local iDRAC6,
- activer ou désactiver IPMI sur LAN,
- configurer les paramètres LAN,
- activer ou désactiver la découverte automatique et configurer le serveur de provisionnement,
- Configurer le média virtuel
- configurer la carte à puce,
- changer le nom d'utilisateur et le mot de passe d'administration,
- réinitialiser les paramètres d'usine de la configuration iDRAC6,
- Afficher ou effacer les messages du journal des événements système (SEL)
- configurer l'écran LCD,
- configurer les services système.

Les tâches pouvant être réalisées à l'aide de l'utilitaire de configuration iDRAC6 peuvent également être exécutées avec d'autres utilitaires fournis par le logiciel iDRAC6 ou Dell OpenManage, notamment l'interface Web, l'interface de ligne de commande SM-CLP ainsi que l'interface de ligne de commande RACADM locale et distante.

# Démarrage de l'utilitaire de configuration iDRAC6

1. Mettez sous tension ou redémarrez le serveur en appuyant sur le bouton d'alimentation situé à l'avant du serveur.
2. Lorsque le message **Appuyez sur <Ctrl-E> pour configurer l'accès à distance dans 5 s...** s'affiche, appuyez immédiatement sur **<Ctrl><E>**.

**REMARQUE :** si votre système d'exploitation commence à se charger avant d'appuyer sur **<Ctrl><E>**, laissez le système terminer son démarrage, puis redémarrez votre serveur et réessayez.

La fenêtre **Utilitaire de configuration iDRAC6** s'affiche. Les deux premières lignes fournissent des informations sur les révisions du micrologiciel iDRAC6 et du micrologiciel du fond de panier principal. Les niveaux de révision peuvent être utiles afin de déterminer si une mise à niveau du micrologiciel est nécessaire.

Le micrologiciel iDRAC6 est la partie des informations relatives aux interfaces externes, telles que l'interface Web, SM-CLP et les interfaces Web. Le micrologiciel de fond de panier principal est la partie du micrologiciel qui s'interface avec l'environnement matériel du serveur et qui le surveille.

# Utilisation de l'utilitaire de configuration iDRAC6

Sous les messages de révision du micrologiciel, le reste de l'utilitaire de configuration iDRAC6 se compose d'un menu d'éléments auxquels vous pouvez accéder à l'aide de la <flèche vers le haut> et la <flèche vers le bas>.

- Si un élément de menu renvoie à un sous-menu ou à un champ de texte modifiable, appuyez sur <Entrée> pour accéder à l'élément et sur <Échap> pour le quitter, une fois sa configuration terminée.
- Si des valeurs sélectionnables telles que Oui/Non ou Activé/Désactivé sont associées à un élément, appuyez sur la <flèche vers la gauche>, la <flèche vers la droite> ou sur la <barre d'espace> pour choisir une valeur.
- Si un élément n'est pas modifiable, il apparaît en bleu. Certains éléments deviennent modifiables en fonction des autres sélections que vous effectuez.
- La dernière ligne de l'écran affiche des instructions concernant l'élément actuel. Vous pouvez appuyer sur <F1> pour afficher l'aide sur l'élément actuel.

- Lorsque vous avez fini d'utiliser l'utilitaire de configuration iDRAC6, appuyez sur <Échap> pour afficher le menu Quitter, dans lequel vous pouvez choisir d'enregistrer ou d'ignorer vos modifications, ou encore de retourner dans l'utilitaire.

Les sections suivantes décrivent les éléments de menu de l'utilitaire de configuration iDRAC6.

### LAN iDRAC6

Utilisez la <flèche vers la gauche>, la <flèche vers la droite> et la barre d'espace pour choisir entre **Activé** et **Désactivé**.

Le LAN iDRAC6 est activé dans la configuration par défaut. Le LAN doit être activé pour permettre l'utilisation des services iDRAC6, tels que l'interface Web, Telnet/SSH, la console virtuelle et le média virtuel.

Si vous choisissez de désactiver le LAN, l'avertissement suivant s'affiche :

```
L'interface hors bande iDRAC6 est désactivée si le
canal LAN est désactivé.

Appuyez sur n'importe quelle touche pour effacer le
message et continuer.
```

Le message vous informe que outre les services auxquels vous accédez en vous connectant directement aux ports iDRAC6 HTTP, HTTPS, Telnet ou SSH, le trafic réseau de gestion hors bande, tels que les messages IPMI envoyés à iDRAC6 à partir d'une station de gestion, n'est pas reçu lorsque le LAN est désactivé. L'interface RACADM locale reste disponible et peut être utilisée pour reconfigurer le LAN iDRAC6.

### IPMI Over LAN (IPMI sur LAN)

Appuyez sur la <flèche vers la gauche>, la <flèche vers la droite> et la barre d'espace pour choisir entre **Activé** et **Désactivé**. Lorsque **Désactivé** est sélectionné, iDRAC6 n'accepte pas les messages IPMI en provenance de l'interface LAN.

Si vous sélectionnez **Désactivé**, l'avertissement suivant s'affiche :

```
L'interface IPMI hors bande iDRAC6 sera désactivée si
IPMI sur LAN est désactivé.
```

Appuyez sur n'importe quelle touche pour effacer le message et continuer. Voir « LAN iDRAC6 », à la page 329 pour obtenir une explication du message.

## Paramètres LAN

Appuyez sur <Entrée> pour afficher le sous-menu Paramètres LAN. Une fois la configuration des paramètres LAN terminée, appuyez sur <Échap> pour revenir au menu précédent.

**Tableau 17-1. Paramètres LAN**

| Élément | Description |
|---|---|
| **Paramètres communs** | |
| NIC Selection (Sélection de carte réseau) | Appuyez sur la <flèche vers la droite>, la <flèche vers la gauche> et la barre d'espace pour basculer d'un mode à l'autre.<br>Les modes disponibles sont : **Dédié, Partagé**, **Partagé avec basculement LOM2** et **Partagé avec basculement tous les LOM**.<br>Ces modes permettent à iDRAC6 de se servir de l'interface correspondante pour communiquer avec l'extérieur. |
| Adresse MAC | Il s'agit de l'adresse MAC non modifiable de l'interface réseau iDRAC6. |
| Activation du VLAN | Sélectionnez **Activé** pour activer le filtrage du LAN virtuel pour iDRAC6. |
| Numéro VLAN | Si **Activation du VLAN** est défini sur **Activé**, saisissez une valeur Numéro VLAN entre 1 et 4 094. |
| Priorité du VLAN | Si **Activation du VLAN** est défini sur **Activé**, sélectionnez la priorité du VLAN entre 0 et 7. |
| Enregistrer le nom iDRAC6 | Sélectionnez **Activé** pour enregistrer le nom iDRAC6 auprès du service DNS. Sélectionnez **Désactivé** si vous ne voulez pas que les utilisateurs puissent trouver le nom iDRAC6 dans DNS. |

**Tableau 17-1. Paramètres LAN *(suite)***

| Élément | Description |
|---|---|
| Nom iDRAC6 | Si **Enregistrer le nom iDRAC** est défini sur **Activé**, appuyez sur <Entrée> pour modifier le champ de texte **Nom iDRAC DNS actuel**. Appuyez sur <Entrée> une fois la modification du nom iDRAC6 terminée. Appuyez sur <Échap> pour revenir au menu précédent. Le nom iDRAC6 doit être un nom d'hôte DNS valide. |
| Nom de domaine de DHCP | Sélectionnez **Activé** si vous souhaitez obtenir le nom de domaine auprès d'un service DHCP sur le réseau. Sélectionnez **Désactivé** si vous souhaitez spécifier le nom de domaine. |
| Nom de domaine | Si **Nom de domaine de DHCP** est défini sur **Désactivé**, appuyez sur <Entrée> pour modifier le champ de texte **Nom de domaine actuel**. Appuyez sur <Entrée> une fois la modification terminée. Appuyez sur <Échap> pour revenir au menu précédent. Le nom de domaine doit être un domaine DNS valide, par exemple `monentreprise.com`. |
| Chaîne de nom d'hôte | Appuyez sur <Entrée> pour modifier. Saisissez le nom de l'hôte pour les alertes d'interruptions d'événements sur plateforme (PET). |
| Alerte LAN activée | Sélectionnez **Activé** pour activer l'alerte LAN PET. |
| Entrée 1 de règle d'alerte | Sélectionnez **Activer** ou **Désactiver** pour activer la première destination de l'alerte. |
| Destination de l'alerte 1 | Si **Alerte LAN activée** est défini sur **Activé**, saisissez l'adresse IP à laquelle les alertes LAN PET seront transférées. |
| **Paramètres IPv4** | Activez ou désactivez la prise en charge de la connexion IPv4. |
| IPv4 | Sélectionnez **Activé** ou **Désactivé** pour la prise en charge du protocole IPv4. |
| Clé de cryptage RMCP+ | Appuyez sur <Entrée> pour modifier la valeur et sur <Échap> lorsque vous avez terminé. La clé de cryptage RMCP+ est une chaîne hexadécimale de 40 caractères (caractères 0-9, a-f et A-F). RMCP+ est une extension IPMI qui ajoute de l'authentification et du cryptage à IPMI. La valeur par défaut est une chaîne de 40 0 (zéros). |

**Tableau 17-1. Paramètres LAN *(suite)***

| Élément | Description |
|---|---|
| IP Address Source (Source d'adresse IP) | Choisissez entre **DHCP** et **Statique**. Lorsque DHCP est sélectionné, les champs **Adresse IP Ethernet**, **Masque de sous-réseau** et **Passerelle par défaut** sont obtenus auprès d'un serveur DHCP. Si aucun serveur DHCP n'est trouvé sur le réseau, les champs sont définis sur zéro.<br>Lorsque **Statique** est sélectionné, les éléments **Adresse IP Ethernet**, **Masque de sous-réseau** et **Passerelle par défaut** deviennent modifiables. |
| Adresse IP Ethernet | Si la **source d'adresse IP** est définie sur **DHCP**, ce champ affiche l'adresse IP obtenue auprès de DHCP.<br>Si la **source d'adresse IP** est définie sur **Statique**, saisissez l'adresse IP que vous souhaitez attribuer à iDRAC6.<br>L'adresse par défaut est **192.168.0.120**. |
| Masque de sous-réseau | Si la **source d'adresse IP** est définie sur **DHCP**, ce champ affiche l'adresse de masque de sous-réseau obtenue auprès de DHCP.<br>Si la **source d'adresse IP** est définie sur **Statique**, saisissez le masque de sous-réseau d'iDRAC6. L'adresse par défaut est **255.255.255.0**. |
| Passerelle par défaut | Si la **source d'adresse IP** est définie sur **DHCP**, ce champ affiche l'adresse IP de la passerelle par défaut obtenue auprès de DHCP.<br>Si la **source d'adresse IP** est définie sur **Statique**, saisissez l'adresse IP de la passerelle par défaut. L'adresse par défaut est **192.168.0.1**. |
| Serveurs DNS de DHCP | Sélectionnez **Activé** pour récupérer les adresses de serveur DNS auprès d'un service DHCP sur le réseau. Sélectionnez **Désactivé** pour spécifier les adresses de serveur DNS ci-dessous. |
| Serveur DNS 1 | Si **Serveurs DNS de DHCP** est défini sur **Désactivé**, saisissez l'adresse IP du premier serveur DNS. |
| Serveur DNS 2 | Si **Serveurs DNS de DHCP** est défini sur **Désactivé**, saisissez l'adresse IP du deuxième serveur DNS. |

**Tableau 17-1. Paramètres LAN *(suite)***

| Élément | Description |
|---|---|
| **Paramètres IPv6** | Activez ou désactivez la prise en charge de la connexion IPv6. |
| IP Address Source (Source d'adresse IP) | Choisissez entre **AutoConfig** et **Statique**. Lorsque **AutoConfig** est sélectionné, les champs **Adresse IPv6 1**, **Longueur du préfixe** et **Passerelle par défaut** sont obtenus auprès de DHCP.<br><br>Lorsque **Statique** est sélectionné, les éléments **Adresse IPv6 1**, **Longueur du préfixe** et **Passerelle par défaut** deviennent modifiables. |
| Adresse IPv6 1 | Si la **source d'adresse IP** est définie sur **AutoConfig**, ce champ affiche l'adresse IP obtenue auprès de DHCP.<br><br>Si la **source d'adresse IP** est définie sur **Statique**, saisissez l'adresse IP que vous souhaitez attribuer à iDRAC6. |
| Longueur du préfixe | Configure la longueur du préfixe de l'adresse IPv6. Il peut s'agir d'une valeur entre 1 et 128 inclus. |
| Passerelle par défaut | Si la **source d'adresse IP** est définie sur **AutoConfig**, ce champ affiche l'adresse IP de la passerelle par défaut obtenue auprès de DHCP.<br><br>Si la **source d'adresse IP** est définie sur **Statique**, saisissez l'adresse IP de la passerelle par défaut. |
| Adresse locale de la liaison IPv6 | Il s'agit de l'**adresse locale de la liaison IPv6** non modifiable de l'interface réseau iDRAC6. |
| Adresse IPv6 2 | Il s'agit de l'**adresse IPv6 2** non modifiable de l'interface réseau iDRAC6. |
| Serveurs DNS de DHCP | Sélectionnez **Activé** pour récupérer les adresses de serveur DNS auprès d'un service DHCP sur le réseau. Sélectionnez **Désactivé** pour spécifier les adresses de serveur DNS ci-dessous. |
| Serveur DNS 1 | Si **Serveurs DNS de DHCP** est défini sur **Désactivé**, saisissez l'adresse IP du premier serveur DNS. |
| Serveur DNS 2 | Si **Serveurs DNS de DHCP** est défini sur **Désactivé**, saisissez l'adresse IP du premier serveur DNS. |

**Tableau 17-1. Paramètres LAN *(suite)***

| Élément | Description |
|---|---|
| Configurations LAN avancées | |
| Négociation automatique | Si **Sélection de NIC** est défini sur **Dédié**, choisissez entre **Activé** et **Désactivé**.<br>Lorsque **Activé** est sélectionné, **Paramètre de vitesse du LAN** et **Paramètre de duplex du LAN** sont automatiquement configurés. |
| Paramètre de vitesse du LAN | Si **Négociation automatique** est défini sur **Désactivé**, choisissez entre 10 Mbits/s et 100 Mbits/s. |
| Paramètre de duplex du LAN | Si **Négociation automatique** est défini sur **Désactivé**, choisissez entre **Semi-duplex** et **Duplex intégral**. |

## Configuration des médias virtuels

### Média virtuel

Appuyez sur <Entrée> pour sélectionner **Déconnecté, Connecté** ou **Autoconnecté**. Lorsque vous sélectionnez **Connecté**, les périphériques de média virtuel sont connectés au bus USB, ce qui les rend disponibles lors des sessions de **Console virtuelle**.

Si vous sélectionnez **Déconnecté**, les utilisateurs ne peuvent pas accéder aux périphériques de média virtuel lors des sessions **Console virtuelle**.

**REMARQUE :** pour utiliser un lecteur flash USB avec la fonctionnalité **Média virtuel**, le **type d'émulation de lecteur flash USB** doit être défini sur **Disque dur** dans l'utilitaire de configuration du BIOS. L'utilitaire de configuration du BIOS est accessible en appuyant sur <F2> lors du démarrage du serveur. Si le **type d'émulation de lecteur flash USB** est défini sur **Automatique**, le lecteur flash apparaît sous forme de lecteur de disquette sur le système.

### vFlash

Appuyez sur <Entrée> pour sélectionner **Activé** ou **Désactivé**.

- **Activé** : vFlash est disponible en vue de la gestion des partitions.
- **Désactivé** : vFlash n'est pas disponible en vue de la gestion des partitions.

**PRÉCAUTION : vFlash ne peut pas être désactivé si une ou plusieurs partitions sont en cours d'utilisation ou connectées.**

#### Initialiser vFlash

Choisissez cette option pour initialiser la carte vFlash. L'opération d'initialisation efface les données existantes sur la carte SD et toutes les partitions existantes sont supprimées. Vous ne pouvez pas effectuer d'opération d'initialisation si une ou plusieurs partitions sont en cours d'utilisation ou connectées. Cette option est accessible uniquement si une carte de taille supérieure à 256 Mo est présente dans le logement de carte iDRAC Enterprise et si vFlash est activé.

Appuyez sur <Entrée> pour initialiser la carte SD vFlash.

L'opération d'initialisation peut échouer pour les raisons suivantes :

- La carte SD n'est pas actuellement présente.
- vFlash est actuellement utilisé par un autre processus.
- vFlash n'est pas activé.
- La carte SD est protégée contre l'écriture.
- Une ou plusieurs partitions sont en cours d'utilisation.
- Une ou plusieurs partitions sont actuellement connectées.

#### Propriétés vFlash

Appuyez sur <Entrée> pour afficher les propriétés suivantes de la carte SD vFlash :

- **Nom** : affiche le nom de la carte SD vFlash insérée dans le logement de carte SD vFlash du serveur. S'il s'agit d'une carte SD Dell, la mention « Carte SD vFlash » s'affiche. S'il s'agit d'une carte SD autre que Dell, la mention « Carte SD » s'affiche.
- **Taille** : affiche la taille de la carte SD vFlash en gigaoctets (Go).
- **Espace disponible** : affiche l'espace inutilisé sur la carte SD vFlash en mégaoctets (Mo). Cet espace est disponible pour créer des partitions supplémentaires sur la carte SD vFlash. Pour les cartes SD, la mention « 256 Mo » sert à spécifier l'espace disponible.

- **Protégé contre l'écriture** : affiche si la carte SD vFlash est protégée ou non protégé, contre l'écriture.
- **Intégrité** : affiche l'intégrité générale de la carte SD vFlash. Ce peut être :
  - OK
  - Warning (Avertissement)
  - Critique

Appuyez sur <Échap> pour quitter.

### ouverture d'une session par carte à puce

Appuyez sur <Entrée> pour sélectionner **Activé** ou **Désactivé**. Cette option permet de configurer la fonctionnalité Ouverture de session par carte à puce. Les options disponibles sont **Activé**, **Désactivé** et **Activé avec RACADM**.

**REMARQUE :** lorsque vous sélectionnez **Activé** ou **Activé avec RACADM**, **IPMI sur LAN** est désactivé et bloqué en vue de la modification.

## Configuration de System Services

#### System Services (Services système)

Appuyez sur <Entrée> pour sélectionner **Activé** ou **Désactivé**. Voir le *Guide d'utilisation de Dell Lifecycle Controller* disponible sur le site Web du support de Dell à l'adresse **dell.com/support/manuals** pour plus d'informations.

**REMARQUE :** la modification de cette option entraîne le redémarrage du serveur lorsque vous utilisez **Enregistrer** et **Quitter** pour appliquer les nouveaux paramètres.

**REMARQUE :** si vous choisissez de restaurer les paramètres d'usine, les paramètres de System Services restent inchangés.

#### Annuler les services système

Appuyez sur <Entrée> pour sélectionner **Non** ou **Oui**.

Lorsque vous sélectionnez **Oui**, toutes les sessions d'Unified Server Configurator sont fermées et le serveur redémarre lorsque vous utilisez **Enregistrer** et **Quitter** pour appliquer les nouveaux paramètres.

#### Recueillir l'inventaire système au redémarrage

Sélectionnez **Activé** pour permettre le recueil de l'inventaire lors du démarrage. Voir le *Guide d'utilisation de Dell Lifecycle Controller* disponible sur le site Web du support de Dell à l'adresse **dell.com/support/manuals** pour plus d'informations.

**REMARQUE :** la modification de cette option entraîne le redémarrage du serveur lorsque vous avez enregistré vos paramètres et avez quitté l'utilitaire de configuration iDRAC6.

**REMARQUE :** si vous choisissez de restaurer les paramètres d'usine, les paramètres de Collecte de l'inventaire système au redémarrage restent inchangés.

## Configuration de l'écran LCD

Appuyez sur <Entrée> pour afficher le sous-menu **Configuration de l'écran LCD**. Une fois la configuration des paramètres de l'écran LCD terminée, appuyez sur <Échap> pour revenir au menu précédent.

**Tableau 17-2. Configuration utilisateur de l'écran LCD**

| | |
|---|---|
| Ligne 1 de l'écran LCD | Appuyez sur la <flèche vers la droite>, la <flèche vers la gauche> et la barre d'espace pour basculer d'une option à l'autre.<br>Cette option définit l'affichage de l'**Écran d'accueil** sur l'écran LCD selon l'une des options suivantes :<br>**Temp ambiante, Numéro d'inventaire, Nom d'hôte, Adresse IPv4 iDRAC6, Adresse IPv6 iDRAC6, Adresse MAC iDRAC6, Numéro de modèle, Aucun, Numéro de service, Alimentation système, Chaîne définie par l'utilisateur.** |
| Chaîne définie par l'utilisateur de l'écran? LCD | Affichez ou entrez la chaîne à afficher sur l'écran LCD. La chaîne peut comporter 62 caractères au maximum. |
| Blocs d'alimentation du système LCD | Sélectionnez **Watt** ou **BTU/h** pour spécifier l'unité à afficher sur l'écran LCD. |
| Unités de temp ambiante de l'écran LCD | Sélectionnez **Celsius** ou **Fahrenheit** pour spécifier l'unité à afficher sur l'écran LCD. |

| | |
|---|---|
| Affichage des erreurs de l'écran LCD | Sélectionnez **Simple** ou **SEL** (journal des événements système).<br>Cette fonctionnalité permet l'affichage des messages d'erreur sur l'écran LCD dans l'un des deux formats :<br>Le format Simple consiste en une description, en anglais, de l'événement.<br>Le format SEL affiche une chaîne de texte du journal des événements système. |
| Indication « Console virtuelle distante » de l'écran LCD | Sélectionnez **Activé** pour afficher le texte *Console virtuelle* à chaque fois qu'une console virtuelle est active sur l'unité. |
| Accès au panneau avant de l'écran LCD | Appuyez sur la <flèche vers la droite>, la <flèche vers la gauche > et la barre d'espace pour passer d'une option à l'autre : **Désactivé**, **Afficher et modifier** et **Afficher uniquement**.<br>Ce paramètre permet de définir le niveau d'accès utilisateur pour l'écran LCD. |

### Configuration de l'utilisateur du LAN

L'utilisateur du LAN est le compte administrateur iDRAC6, soit **root** par défaut. Appuyez sur <Entrée> pour afficher le sous-menu Configuration de l'utilisateur du LAN. Une fois la configuration de l'utilisateur du LAN terminée, appuyez sur <Échap> pour revenir au menu précédent.

### Réinitialiser les paramètres par défaut

Utilisez l'élément de menu **Réinitialiser les paramètres par défaut** pour réinitialiser tous les paramètres d'usine de tous les éléments de la configuration iDRAC6. Cette opération peut être requise, par exemple, si vous avez oublié le mot de passe utilisateur d'administration ou si vous souhaitez reconfigurer iDRAC6 à partir des paramètres par défaut.

Appuyez sur <Entrée> pour sélectionner l'élément. Le message d'avertissement suivant s'affiche :

```
La réinitialisation des paramètres d'usine va
restaurer les paramètres utilisateur non volatiles à
distance. Continuer ?
```

```
< NON (Annuler) >

< OUI (Continuer) >
```

Sélectionnez **OUI** et appuyez sur <Entrée> pour réinitialiser les paramètres par défaut d'iDRAC6.

L'un des messages d'erreur suivants s'affiche si cette opération échoue :

- La commande de réinitialisation a échoué. Essayez plus tard - iDRAC est occupé.
- Impossible de restaurer les valeurs par défaut des paramètres - Délai d'expiration.
- Impossible d'envoyer la commande de réinitialisation. Essayez plus tard - iDRAC est occupé.

**Tableau 17-3. Configuration de l'utilisateur du LAN**

| Élément | Description |
|---|---|
| Découverte automatique | La fonctionnalité Découverte automatique permet la découverte automatique de systèmes sans provisionnement sur le réseau ; elle permet en outre d'établir des références initiales *de manière sécurisée* afin que ces systèmes découverts puissent être gérés. Cette fonctionnalité permet à iDRAC6 de détecter le serveur de provisionnement. iDRAC6 et le serveur du service de provisionnement s'authentifient mutuellement. Le serveur de provisionnement distant envoie les références utilisateur afin qu'iDRAC6 crée un compte utilisateur avec ces références. Une fois le compte utilisateur créé, une console distante peut établir une communication WS-MAN avec iDRAC6 à l'aide des références spécifiées au cours du processus de découverte, puis envoyer les instructions sécurisées à iDRAC6 afin qu'il déploie un système d'exploitation à distance.<br><br>Pour des informations supplémentaires sur le déploiement d'un système d'exploitation à distance, reportez-vous au Guide d'utilisation de *Dell Lifecycle Controller* disponible sur le site Web du support de Dell à l'adresse **dell.com/support/manuals**.<br><br>Exécutez les actions requises suivantes dans une session de l'**utilitaire de configuration iDRAC6** *séparée avant d'établir manuellement la découverte automatique* :<br>• Activer le NIC<br>• Activer IPv4<br>• Activation de DHCP<br>• Obtenir le nom de domaine auprès de DHCP<br>• Désactiver le compte admin (compte n° 2)<br>• Obtention de l'adresse du serveur DNS auprès de DHCP<br>• Obtention du nom de domaine DNS auprès de DHCP<br><br>Sélectionnez **Activé** pour activer la fonctionnalité Découverte automatique. Par défaut, cette option est définie sur **Désactivé**. Si vous avez commandé un système Dell doté de la fonctionnalité Découverte automatique défini sur **Activé**, iDRAC6 sur le système Dell est alors livré avec DHCP activé sans références par défaut pour l'ouverture de session à distance. |

**Tableau 17-3. Configuration de l'utilisateur du LAN *(suite)***

| Élément | Description |
|---|---|
| Découverte automatique *(suite)* | Avant l'ajout de votre système Dell au réseau et l'utilisation de la fonctionnalité Découverte automatique, assurez-vous que :<br>• Le serveur DHCP (protocole de configuration dynamique de l'hôte)/le système de noms de domaine (DNS) sont configurés.<br>• Les services Web de provisionnement sont installés, configurés et enregistrés. |
| Serveur de provisionnement | Ce champ est utilisé pour configurer le serveur de provisionnement. L'adresse du serveur de provisionnement peut être une combinaison d'adresses IPv4 ou de nom d'hôte, et ne doit pas dépasser 255 caractères. Chaque adresse doit être séparée par une virgule.<br>Si la fonctionnalité Découverte automatique est activée et une fois le processus de découverte automatique exécuté avec succès, les références utilisateur sont récupérées auprès du serveur de provisionnement configuré afin de permettre un provisionnement distant à venir.<br>Pour des informations supplémentaires, consultez le *Guide d'utilisation de Dell Lifecycle Controller* disponible sur le site Web du support de Dell à l'adresse **dell.com/support/manuals**. |
| Accès au compte | Sélectionnez **Activé** pour activer le compte administrateur. Sélectionnez **Désactivé** pour désactiver le compte administrateur ou lorsque la découverte automatique est activée. |
| Privilèges de compte | Choisissez entre **Administrateur**, **Utilisateur**, **Opérateur** et **Aucun accès**. |
| Nom d'utilisateur du compte | Appuyez sur <Entrée> pour modifier le nom d'utilisateur et appuyez sur <Échap> lorsque vous avez terminé. Le nom d'utilisateur par défaut est **root** (racine). |
| Saisir le mot de passe | Tapez le nouveau mot de passe du compte administrateur. Les caractères ne sont pas renvoyés sur l'affichage lorsque vous les tapez. |
| Confirm Password (Confirmer le mot de passe) | Retapez le nouveau mot de passe du compte administrateur. Si les caractères que vous entrez ne correspondent pas à ceux que vous avez entrés dans le champ **Saisir le mot de passe**, un message s'affiche et vous devez entrer à nouveau le mot de passe. |

### Menu Journal des événements système

Le menu **Journal des événements système** vous permet d'afficher les messages du journal des événements système (SEL) et d'effacer les messages du journal. Appuyez sur <Entrée> pour afficher le menu **Journal des événements système**. Le système compte les entrées de journal, puis affiche le nombre total d'enregistrements et le message le plus récent. Le journal SEL conserve un maximum de 512 messages.

Pour afficher les messages du journal SEL, sélectionnez **Afficher le journal des événements système** et appuyez sur <Entrée>. Utilisez la <flèche vers la gauche> pour accéder au message précédent (le plus ancien) et la <flèche vers la droite> pour accéder au message suivant (le plus récent). Saisissez un numéro d'enregistrement pour atteindre cet enregistrement. Appuyez sur <Échap> lorsque vous avez fini d'afficher les messages du journal SEL.

Pour effacer le journal SEL, sélectionnez **Effacer le journal des événements système** et appuyez sur <Entrée>

Lorsque vous avez fini d'utiliser le menu Journal SEL, appuyez sur <Échap> pour revenir au menu précédent.

### Sortie de l'utilitaire de configuration iDRAC6

Lorsque vous avez fini d'apporter des modifications à la configuration iDRAC6, appuyez sur la touche <Échap> pour afficher le menu Quitter.

- Sélectionnez **Enregistrer les modifications et quitter** et appuyez sur <Entrée> pour conserver vos modifications. Si cette opération échoue, l'un des messages suivants s'affiche :
  - Échec de communication iDRAC6 : s'affiche si l'iDRAC n'est pas accessible.
  - Certains des paramètres ne peuvent pas être appliqués : Ce message s'affiche lorsqu'un certain nombre de paramètres ne peuvent pas être appliqués.
- Sélectionnez **Ignorer les modifications et quitter** et appuyez sur <Entrée> pour ignorer les modifications que vous avez apportées.
- Sélectionnez **Retourner à la configuration** et appuyez sur <Entrée> pour retourner à l'utilitaire de configuration iDRAC6.

# 18

# Surveillance et gestion des alertes

Cette section explique comment surveiller iDRAC6 et fournit les procédures pour configurer votre système et iDRAC6 pour recevoir des alertes.

## Configuration du système géré pour la saisie de l'écran de la dernière panne

Pour qu'iDRAC6 puisse saisir l'écran du dernier plantage, vous devez configurer le système géré de la façon suivante.

1. Installez le logiciel Managed System. Pour des informations supplémentaires sur l'installation du logiciel du système géré, voir le *Guide d'utilisation de Server Administrator*.
2. Exécutez un système d'exploitation Microsoft Windows pris en charge en désélectionnant la fonctionnalité de *redémarrage automatique* de Windows dans les **paramètres de démarrage et de récupération de Windows**.
3. Activez l'écran du dernier plantage (désactivé par défaut).

   Pour activer l'écran du dernier plantage à l'aide de la RACADM locale, ouvrez une invite de commande et tapez les commandes suivantes :

   ```
   racadm config -g cfgRacTuning -o
   cfgRacTuneAsrEnable 1
   ```
4. Activez l'horloge de récupération automatique et choisissez **Réinitialiser**, **Mise hors tension** ou **Cycle d'alimentation** comme action de **récupération automatique**. Pour configurer l'horloge de **récupération automatique**, vous devez utiliser Server Administrator ou IT Assistant.

   Pour des informations sur la configuration de l'horloge de **récupération automatique**, consultez le *Guide d'utilisation de Server Administrator*. Pour que l'écran du dernier plantage puisse être saisi, l'horloge de **récupération automatique** doit être définie sur 60 secondes ou plus. Le paramètre par défaut est 480 secondes.

   L'écran du dernier plantage n'est pas disponible quand l'action de **récupération automatique** est définie sur **Arrêt** ou **Cycle d'alimentation** si le système géré est tombé en panne.

# Désactivation de l'option Redémarrage automatique de Windows

Pour que la fonctionnalité Écran du dernier plantage de l'interface Web iDRAC6 fonctionne correctement, désactivez l'option **Redémarrage automatique** sur les systèmes gérés exécutant les systèmes d'exploitation Microsoft Windows Server 2008 et Windows Server 2003.

### Désactivation de l'option Redémarrage automatique dans Windows Server 2008

1. Ouvrez le **Panneau de configuration** de Windows et double-cliquez sur l'icône **Système**.
2. Cliquez sur **Paramètres système avancés** sous **Tâches** sur la gauche.
3. Cliquez sur l'onglet **Advanced** (Avancé).
4. Sous **Démarrage et récupération**, cliquez sur **Paramètres**.
5. Désélectionnez la case à cocher **Redémarrage automatique**.
6. Cliquez sur **OK** deux fois.

### Désactivation de l'option Redémarrage automatique dans Windows Server 2003

1. Ouvrez le **Panneau de configuration** de Windows et double-cliquez sur l'icône **Système**.
2. Cliquez sur l'onglet **Advanced** (Avancé).
3. Sous **Démarrage et récupération**, cliquez sur **Paramètres**.
4. Décochez la case **Redémarrage automatique**.
5. Cliquez sur **OK** deux fois.

# Configuration des événements sur plateforme

La configuration des événements sur plateforme offre un outil de configuration du périphérique d'accès à distance pour effectuer les actions sélectionnées sur certains messages d'événements. Ces actions incluent le redémarrage, le cycle d'alimentation, la mise hors tension et le déclenchement d'une alerte (interruption des événements sur plateforme [PET] et/ou e-mail).

Les événements sur plateforme pouvant être filtrés incluent :

1. Filtre d'assertion critique du ventilateur
2. Filtre d'assertion d'avertissement concernant la batterie
3. Filtre d'assertion critique de la batterie
4. Filtre d'assertion critique de la tension
5. Filtre d'assertion d'avertissement concernant la température
6. Filtre d'assertion critique de la température
7. Filtre d'assertion critique de l'intrusion
8. Filtre de dégradation de la redondance
9. Filtre de perte de la redondance
10. Filtre d'assertion d'avertissement concernant le processeur
11. Filtre d'assertion critique du processeur
12. Filtre d'assertion critique du processeur absent
13. Filtre d'assertion d'avertissement concernant le bloc d'alimentation
14. Filtre d'assertion critique du bloc d'alimentation
15. Filtre d'assertion critique du bloc d'alimentation absent
16. Filtre d'assertion critique du journal des événements
17. Filtre d'assertion critique de la surveillance
18. Filtre d'assertion d'avertissement concernant l'alimentation système
19. Filtre d'assertion critique de l'alimentation système
20. Filtre d'assertion informative du média Flash amovible absent
21. Filtre d'assertion critique du média Flash amovible
22. Filtre d'assertion d'avertissement du média Flash amovible

Lorsqu'un événement sur plateforme se produit (par exemple, une panne de sonde de ventilateur), un événement système est généré et enregistré dans le journal des événements système (SEL). Si cet événement correspond à un filtre d'évènement sur plateforme (PEF) dans la liste des filtres d'événements sur plateforme et que vous avez configuré ce filtre pour générer une alerte (PET ou par e-mail), une alerte PET ou par e-mail est alors envoyée à une ou plusieurs destinations configurées.

Si le même filtre d'événements sur plateforme est également configuré pour effectuer une action (tel qu'un redémarrage du système), l'action est effectuée.

## Configuration des filtres d'événements sur plateforme (PEF)

Configurez vos filtres d'événements sur plateforme avant de configurer les interruptions d'événement sur plateforme ou les paramètres d'alerte par e-mail.

### Configuration de PEF à l'aide de l'interface Web

Pour des informations détaillées, voir « Configuration des filtres d'événements sur plateforme (PEF) », à la page 61.

### Configuration de PEF à l'aide de la CLI RACADM

1. Activez PEF.

   Ouvrez une invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i
   1 1
   ```

   où `1` et `1` correspondent à l'index PEF et à la sélection activer/désactiver, respectivement.

   L'index PEF peut être une valeur de 1 à 22. La sélection activer/désactiver peut être définie sur 1 (Activé) ou 0 (Désactivé).

   Par exemple, pour activer PEF avec l'index 5, tapez la commande suivante :

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefEnable -i
   5 1
   ```

2. Configurez vos actions PEF.

   À l'invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

   ```
   racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i
   1 <action>
   ```

   où les bits des valeurs <*action*> sont les suivants :

   - 0 = aucune action d'alerte
   - 1 = mise hors tension du serveur
   - 2 = redémarrage du serveur
   - 3 = cycle d'alimentation du serveur

Par exemple, pour permettre à PEF de redémarrer le serveur, tapez la commande suivante :

```
racadm config -g cfgIpmiPef -o cfgIpmiPefAction -i
1 2
```

où `1` est l'index PEF et 2 est l'action PEF pour le redémarrage.

## Configuration du PET

### Configuration de PET à l'aide de l'interface utilisateur Web

Pour des informations détaillées, voir « Configuration des interruptions d'événement sur plateforme (PET) », à la page 62.

### Configuration de PET à l'aide de la CLI RACADM

1. Activez vos alertes globales.

   Ouvrez une invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

   ```
   racadm config -g cfgIpmiLan -o
   cfgIpmiLanAlertEnable 1
   ```

2. Activez PET.

   À l'invite de commande, tapez les commandes suivantes et appuyez sur <Entrée> après chaque commande :

   ```
   IPv4:racadm config -g cfgIpmiPet -o
   cfgIpmiPetAlertEnable -i 1 1
   ```

   ```
   IPv6:racadm config -g cfgIpmiPetIpv6 -o
   cfgIpmiPetIpv6PetAlertEnable -i 1 1
   ```

   où `1` et `1` correspondent à l'index de destination PET et à la sélection activer/désactiver, respectivement.

   L'index de destination PET peut être une valeur de 1 à 4. La sélection activer/désactiver peut être définie sur 1 (Activé) ou 0 (Désactivé).

Par exemple, pour activer PET avec l'index 4, tapez la commande suivante :

```
iPv4:racadm config -g cfgIpmiPet -o
cfgIpmiPetAlertEnable -i 4 1
```

```
iPv6:racadm config -g cfgIpmiPetIpv6 -o
cfgIpmiPetIpv6PetAlertEnable -i 4 1
```

**3** Configurez votre règle PET.

À l'invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

```
iPv4:racadm config -g cfgIpmiPet -o
cfgIpmiPetAlertDestIPAddr -i 1 <adresse_IPv4>
```

```
iPv6:racadm config -g cfgIpmiPetIpv6 -o
cfgIpmiPetIPv6AlertDestIPAddr -i 1 <adresse_IPv6>
```

où `1` est l'index de destination PET et *<adresse_IPv4>* et *<adresse_IPv6>* sont les adresses IP de destination du système qui reçoit les alertes d'événement sur plateforme.

**4** Configurez la chaîne Nom de communauté.

À l'invite de commande, entrez :

```
racadm config -g cfgIpmiLan -o
cfgIpmiPetCommunityName <Nom>
```

## Configuration des alertes par e-mail

### Configuration des alertes par e-mail à l'aide de l'interface utilisateur Web

Pour des informations détaillées, voir « Configuration des alertes par e-mail », à la page 63.

### Configuration des alertes par e-mail à l'aide de la CLI RACADM

**1** Activez vos alertes globales.

Ouvrez une invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

```
racadm config -g cfgIpmiLan -o
cfgIpmiLanAlertEnable 1
```

2 Activez les alertes par e-mail.

À l'invite de commande, tapez les commandes suivantes et appuyez sur <Entrée> après chaque commande :

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertEnable -i 1 1
```

où 1 et 1 correspondent à l'index de destination d'e-mail et à la sélection activer/désactiver, respectivement.

L'index de destination d'e-mail peut être une valeur de 1 à 4. La sélection activer/désactiver peut être définie sur 1 (Activé) ou 0 (Désactivé).

Par exemple, pour activer l'e-mail avec l'index 4, tapez la commande suivante :

```
racadm config -g cfgEmailAlert -o
cfgEmailAlertEnable -i 4 1
```

3 Configurez vos paramètres d'e-mail.

À l'invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 *<adresse_e-mail>*

où 1 est l'index de destination d'e-mail et *<adresse_e-mail>* l'adresse e-mail de destination qui reçoit les alertes d'événement sur plateforme.

Pour configurer un message personnalisé, à l'invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 *<message_personnalisé>*

où 1 est l'index de destination d'e-mail et *<message_personnalisé>* est le message affiché dans l'alerte par e-mail.

### Test des alertes par e-mail

La fonctionnalité Alertes par e-mail du RAC permet aux utilisateurs de recevoir des alertes par e-mail lorsqu'un événement critique se produit sur le système géré. L'exemple suivant montre comment tester la fonctionnalité Alertes par e-mail pour garantir que le RAC peut correctement envoyer des alertes par e-mail sur le réseau.

```
racadm testemail -i 2
```

**REMARQUE :** assurez-vous que les paramètres SMTP et Alerte par e-mail sont configurés avant de tester la fonctionnalité Alertes par e-mail. Pour en savoir plus, voir « Configuration des alertes par e-mail », à la page 348.

### Test de la fonctionnalité Alerte par interruption SNMP du RAC

La fonctionnalité Alerte par interruption SNMP du RAC permet aux configurations de l'écouteur d'interruptions SNMP de recevoir des interruptions pour les événements système qui se produisent sur le système géré.

L'exemple suivant montre comment un utilisateur peut tester la fonctionnalité Alerte par interruption SNMP du RAC.

```
racadm testtrap -i 2
```

Avant de tester la fonctionnalité Alertes par interruption SNMP du RAC, assurez-vous que les paramètres SNMP et d'interruption sont configurés correctement. Pour configurer ces paramètres, voir les descriptions des sous-commandes testtrap et testemail dans le *Guide de référence de la ligne de commande RACADM pour iDRAC6 et CMC* disponible sur le site Web de support Dell à l'adresse **dell.com/support/manuals**.

# Questions les plus fréquentes concernant l'authentification SNMP

**Explication de l'affichage du message suivant :**

```
Accès distant : échec de l'authentification SNMP
```

Pendant la découverte, IT Assistant essaie 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 iDRAC6 est **public**. Lorsqu'IT Assistant envoie une requête set, l'agent iDRAC6 génère une erreur d'authentification SNMP, car il accepte uniquement les requêtes de la **communauté = public**.

**REMARQUE :** ceci est le nom de communauté de l'agent SNMP.

Vous pouvez changer le nom de communauté iDRAC6 à l'aide de RACADM.

Pour afficher le nom de communauté iDRAC6, utilisez la commande suivante :

```
racadm getconfig -g cfgOobSnmp
```

Pour définir le nom de communauté iDRAC6, utilisez la commande suivante :

```
racadm config -g cfgOobSnmp -o
cfgOobSnmpAgentCommunity <nom de communauté>
```

Pour accéder à/configurer le nom de communauté de l'agent SNMP iDRAC6 à l'aide de l'interface Web, accédez à **Paramètres iDRAC→ Réseau/Sécurité→ Services**, puis cliquez sur **Agent SNMP**.

Pour éviter de générer des erreurs d'authentification SNMP, vous devez saisir des noms de communauté qui seront acceptés par l'agent. Comme iDRAC6 n'accepte qu'un seul nom de communauté, vous devez utiliser le même nom de communauté **get** et **set** pour configurer la découverte sous IT Assistant.

# 19

# Récupération et dépannage du système géré

Cette section explique comment utiliser l'interface Web iDRAC6 pour effectuer les tâches de récupération et de dépannage d'un système distant en panne.

- « Premières étapes de dépannage d'un système distant », à la page 353.
- « Gestion de l'alimentation d'un système distant », à la page 354.
- « Utilisation des journaux de démarrage POST », à la page 364.
- « Affichage de l'écran du dernier plantage système », à la page 365.

## 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 ?

Pour les systèmes en panne, voir l'écran du dernier plantage (voir « Affichage de l'écran du dernier plantage système », à la page 365) et utilisez la console virtuelle et la gestion de l'alimentation à distance (voir « Gestion de l'alimentation d'un système distant », à la page 354) pour redémarrer le système et observer le processus de redémarrage.

# Gestion de l'alimentation d'un système distant

iDRAC6 vous permet d'effectuer à distance plusieurs actions de gestion de l'alimentation sur le système géré de manière à récupérer le système après une panne système ou un autre événement système.

### Sélection d'actions de contrôle de l'alimentation à partir de l'interface Web iDRAC6

Pour effectuer des actions de gestion de l'alimentation à l'aide de l'interface Web, voir « Exécution de tâches de contrôle de l'alimentation sur le serveur », à la page 324.

### Sélection d'actions de contrôle de l'alimentation depuis la CLI iDRAC6

Utilisez la commande `racadm serveraction` pour effectuer des opérations de gestion de l'alimentation sur le système hôte.

`racadm serveraction <action>`

Les options de la chaîne <*action*> sont :

- **powerdown :** met le système géré hors tension.
- **powerup :** met le système géré sous tension.
- **powercycle :** lance une opération de cycle d'alimentation sur le système géré. Cette action est équivalente à l'enfoncement du bouton d'alimentation situé sur le panneau avant du système pour la mise hors puis sous tension du système.
- **powerstatus :** affiche l'état actuel de l'alimentation du serveur (« ACTIVÉ » ou « DÉSACTIVÉ »).
- **hardreset :** effectue une opération de réinitialisation (redémarrage) sur le système géré.

# Affichage des informations système

La page **Résumé du système** vous permet d'afficher des informations relatives à l'intégrité de votre système et d'autres informations iDRAC6 de base en un coup d'œil et vous fournit des liens permettant d'accéder aux pages d'informations et d'intégrité du système. En outre, vous avez la possibilité de lancer rapidement des tâches courantes à partir de cette page et d'afficher les événements récents consignés dans le journal des événements système (SEL).

Pour accéder à la page **Résumé du système**, cliquez sur **Système**→ Onglet **Propriétés**→ **Résumé du système**. Pour plus d'informations, voir l'*aide en ligne d'iDRAC6*.

La page **Détails du système** affiche des informations sur les composants système suivants :

- Châssis principal du système
- Remote Access Controller

Pour accéder à la page **Détails du système**, développez l'arborescence du **système** et cliquez sur **Propriétés**→ onglet **Détails du système**.

## Châssis principal du système

**REMARQUE :** pour recevoir les informations sur le **nom d'hôte** et le **nom du SE**, les services iDRAC6 doivent être installés sur le système géré.

**Tableau 19-1. Informations système**

| Champ | Description |
|---|---|
| **Description** | Description du système. |
| **Version du BIOS** | Version du BIOS du système. |
| **Service Tag (Numéro de service)** | Numéro de service du système. |
| **Code de service express:** | Code de service du système. |
| **Host Name (Nom d'hôte)** | Nom du système hôte. |
| **Nom du système d'exploitation** | Système d'exploitation s'exécutant sur le système. |
| **OS Version (Version de SE)** | Version du système d'exploitation s'exécutant sur le système. |
| **Révision du système** | Numéro de révision du système. |
| **Micrologiciel du Lifecycle Controller** | Version du micrologiciel du Lifecycle Controller. |

**Tableau 19-2. Récupération automatique**

| Champ | Description |
|---|---|
| **Action de restauration** | Lorsqu'un *blocage système* est détecté, le contrôleur iDRAC6 peut être configuré pour effectuer l'une des actions suivantes : Pas d'action, Réinitialisation matérielle, Mise hors tension ou Cycle d'alimentation. |
| **Compte à rebours initial** | Nombre de secondes qui s'écoulent après la détection d'un *blocage système*, avant que l'iDRAC6 n'effectue une action de récupération. |
| **Compte à rebours actuel** | Valeur actuelle, en secondes, du compte à rebours. |

**Tableau 19-3. Adresses MAC du NIC intégré**

| Champ | Description |
|---|---|
| MAC virtuel | Affiche les adresses MAC virtuel (Media Access Control - Contrôle de l'accès au média).<br>Les données MAC virtuel sont obtenues depuis l'inventaire du matériel, ce qui signifie que l'inventaire du micrologiciel a besoin d'être recueilli une fois avant de visualiser les données VMAC.<br>Cliquez sur **Inventaire du système**. Les données de l'inventaire sont mises à jour et affichées sur la page **Inventaire du système**. Cliquez à nouveau sur **Détails du système**. Les MAC virtuels de chacun des ports LAN intégrés s'affichent maintenant sur la page **Détails du système**.<br>**REMARQUE :** La fonction vMAC sera utilisée par Dell AIM (Advanced Infrastructure Manager) dans des versions ultérieures. Si Dell AIM ne gère pas actuellement le serveur, l'adresse MAC Ethernet et l'adresse MAC virtuel sont identiques. |
| **NIC 1** | Affiche les adresses Ethernet, iSCSI (Internet Small Computer System Interface) et MAC virtuel du NIC (Network Interface Controller) 1 intégré.<br>Les NIC Ethernet prennent en charge la norme Ethernet câblé et se connectent au bus système du serveur.<br>Le NIC de l'iSCSI est un contrôleur d'interface réseau doté d'une pile iSCSI s'exécutant sur l'ordinateur hôte.<br>Les adresses MAC identifient de manière unique chaque nœud présent sur un réseau au niveau de la couche de contrôle de l'accès aux médias. |

**Tableau 19-3. Adresses MAC du NIC intégré *(suite)***

| Champ | Description |
|---|---|
| MAC virtuel | Affiche les adresses MAC virtuel (Media Access Control - Contrôle de l'accès au média).<br><br>Les données MAC virtuel sont obtenues depuis l'inventaire du matériel, ce qui signifie que l'inventaire du micrologiciel a besoin d'être recueilli une fois avant de visualiser les données VMAC.<br><br>Cliquez sur **Inventaire du système**. Les données de l'inventaire sont mises à jour et affichées sur la page **Inventaire du système**. Cliquez à nouveau sur **Détails du système**. Les MAC virtuels de chacun des ports LAN intégrés s'affichent maintenant sur la page **Détails du système**.<br><br>**REMARQUE :** La fonction vMAC sera utilisée par Dell AIM (Advanced Infrastructure Manager) dans des versions ultérieures. Si Dell AIM ne gère pas actuellement le serveur, l'adresse MAC Ethernet et l'adresse MAC virtuel sont identiques. |
| **NIC 2** | Affiche les adresses Ethernet, iSCSI et MAC virtuel du NIC (Network Interface Controller) 2 intégré qui l'identifie de manière unique dans le réseau. |
| **NIC 3** | Affiche les adresses Ethernet, iSCSI et MAC virtuel du NIC (Network Interface Controller) 3 intégré qui l'identifie de manière unique dans le réseau. |
| **NIC 4** | Affiche les adresses Ethernet, iSCSI et MAC virtuel du NIC (Network Interface Controller) 4 intégré qui l'identifie de manière unique dans le réseau. |

## Remote Access Controller

**Tableau 19-4. Informations sur le RAC**

| Champ | Description |
|---|---|
| **Name (Nom)** | iDRAC6 |
| **Informations produit** | Integrated Dell Remote Access Controller 6 - Entreprise |
| **Date/Heure** | Heure actuelle au format :<br>Jour Mois JJ HH:MM:SS:AAAA<br>Exemple : ven jan 28 16:27:29 2011 |

**Tableau 19-4. Informations sur le RAC *(suite)***

| Champ | Description |
|---|---|
| **Version du micrologiciel** | Version du micrologiciel iDRAC6 |
| **Micrologiciel mis à jour** | Date du dernier flashage du micrologiciel au format :<br>Jour Mois JJ HH:MM:SS:AAAA<br>Exemple : sam jan 29 2011 13:31:50 |
| **Version du matériel** | Version du Remote Access Controller |
| **Adresse MAC** | Adresse de contrôle de l'accès aux médias (MAC) qui identifie de manière unique chaque nœud d'un réseau. |

**Tableau 19-5. Informations sur IPv4**

| Champ | Description |
|---|---|
| **IPv4 activé** | **Oui** ou **Non** |
| **Adresse IP** | Adresse 32 bits identifiant la carte d'interface réseau (NIC) auprès d'un hôte. La valeur est affichée au format séparé par des points, par exemple 143.166.154.127. |
| **Masque de sous-réseau** | Le masque de sous-réseau identifie les parties de l'adresse IP constituant le préfixe du réseau étendu et le numéro d'hôte. La valeur est affichée au format séparé par des points, par exemple 255.255.0.0. |
| **par défaut** | Adresse d'un routeur ou d'un commutateur. La valeur est affichée au format séparé par des points, par exemple 143.166.154.1. |
| **DHCP activé** | **Oui** ou **Non**. Indique si le protocole de configuration dynamique de l'hôte (DHCP) est activé. |
| **Utiliser DHCP pour obtenir des adresses de serveur DNS** | **Oui** ou **Non**. Indique si vous souhaitez utiliser DHCP pour obtenir des adresses de serveur DNS. |
| **Serveur DNS préféré** | Indique l'adresse IPv4 statique du serveur DNS préféré. |
| **Autre serveur DNS** | Indique l'adresse IPv4 statique du serveur DNS alternatif. |

**Tableau 19-6. Champs d'informations IPv6**

| Champ | Description |
|---|---|
| **IPv6 activé** | Indique si la pile IPv6 est activée. |
| **Adresse IP 1** | Spécifie l'adresse/la longueur de préfixe IPv6 du NIC d'iDRAC6. La *longueur de préfixe* est combinée avec l'adresse IP 1. Il s'agit d'un entier spécifiant la longueur de préfixe de l'adresse IPv6. Il peut s'agir d'une valeur comprise entre 1 et 128. |
| **Passerelle IP** | Spécifie la passerelle du NIC d'iDRAC6. |
| **Adresse locale de liaison** | Spécifie l'adresse locale de liaison IPv6 du NIC de l'iDRAC6. |
| **Adresse IP 2...15** | Spécifie les adresses IPv6 supplémentaires du NIC d'iDRAC6, le cas échéant. |
| **Autoconfig activée** | **Oui** ou **Non.** AutoConfig permet à Server Administrator d'obtenir l'adresse IPv6 du NIC d'iDRAC à partir du serveur du protocole de configuration dynamique de l'hôte (DHCPv6). |
| **Utiliser DHCPv6 pour obtenir des adresses de serveur DNS** | **Oui** ou **Non**. Indique si vous souhaitez utiliser DHCPv6 pour obtenir des adresses de serveur DNS. |
| **Serveur DNS préféré** | Indique l'adresse IPv6 statique du serveur DNS préféré. |
| **Autre serveur DNS** | Indique l'adresse IPv6 statique du serveur DNS alternatif. |

## Inventaire du système

La page **Inventaire du système** affiche des informations sur les composants matériels et logiciels installés sur le système.

Pour accéder à la page **Inventaire du système**, développez l'arborescence du **système** et cliquez sur **Propriétés**→ onglet **Inventaire du système**.

### Inventaire matériel

Cette section affiche les informations sur les composants matériels actuellement présents sur le système. Si les données de l'inventaire du matériel ne sont pas disponibles lorsque vous cliquez sur l'onglet **Inventaire du système**, le message suivant s'affiche :

`L'inventaire du matériel n'est pas disponible.`

Réactualisez la page pour afficher les détails.

**Inventaire de micrologiciel :**

Cette section affiche les versions du micrologiciel des composants Dell installés. Si les données de l'inventaire du micrologiciel ne sont pas disponibles lorsque vous cliquez sur l'onglet **Inventaire du système**, le message suivant s'affiche :

```
L'inventaire du matériel n'est pas disponible.
```

Réactualisez la page pour afficher les détails.

**REMARQUE :** si l'option CSIOR (Collect System Inventory on Reboot) n'est pas activée, la collection des données peut prendre un certain temps. Dell vous recommande donc d'exécuter CSIOR d'abord, de collecter l'inventaire du système à la réinitialisation, puis de cliquer sur l'onglet **Inventaire du système**.

Après l'ajout ou le retrait de nouveau matériel au système, la page **Inventaire du système** peut ne pas mettre les modifications à jour automatiquement car les données de l'inventaire collectées au cours du processus de fabrication peuvent ne pas avoir été mises à jour avec les nouvelles modifications.

Pour résoudre ce problème, sélectionnez l'option **Cntl+E** au cours du POST du BIOS, puis activez **Collecter l'inventaire du système** à la réinitialisation. Enregistrez puis fermez l'option **Cntl+E**.

Le système redémarre pour collecter le nouvel inventaire du système. Une fois la collection de l'inventaire effectuée, la page **Inventaire du système** affiche les données correctes de l'inventaire du matériel et du logiciel.

Pour plus d'informations, voir l'*aide en ligne d'iDRAC6*.

# Utilisation du journal des événements système (SEL)

La page **Journal SEL** affiche les événements critiques du système qui se produisent sur le système géré.

Pour afficher le journal des événements système :

1. Dans l'arborescence du **système**, cliquez sur **Système**.
2. Cliquez sur l'onglet **Journaux**, puis sur **Journal des événements système**.

   La page **Journal des événements système** affiche la gravité de l'événement et fournit d'autres informations comme indiqué dans le Tableau 19-7.
3. Cliquez sur le bouton approprié de la page **Journal des événements système** pour continuer. Pour des informations supplémentaires, voir l'aide en ligne d'iDRAC6.

4 Cliquez sur **Effacer le journal** pour effacer le journal SEL.

**REMARQUE :** le bouton Effacer le journal n'apparaît que si vous disposez du droit Effacer les journaux.

5 Cliquez sur **Enregistrer sous** pour enregistrer le journal SEL dans le répertoire de votre choix.

**Tableau 19-7. Icônes indicatrices de condition**

| Icône/Catégorie | Description |
|---|---|
|  | Une coche verte indique une condition intègre (normale). |
|  | Un triangle jaune contenant un point d'exclamation indique une condition d'avertissement (non critique). |
|  | Un X rouge indique une condition critique (défaillance). |
|  | Une icône représentant un point d'interrogation indique que la condition est inconnue. |
| **Date/Heure** | Date et heure auxquelles s'est produit l'événement. Si la date n'est pas renseignée, l'événement s'est alors produit lors du démarrage du système. Le format est le suivant : <jour> <mois> jj aaaa hh:mm:ss, basé sur un système horaire de 24 heures. |
| **Description** | Une brève description de l'événement |

### Activation/Désactivation des journaux d'évènements OEM

Les journaux d'évènements OEM sont automatiquement affichés sur la page **Journal des événements système**. Le bouton **Paramètres avancés** de l'onglet **Systèmes→ Journaux** permet d'activer/désactiver l'apparition des messages d'évènements OEM du système géré sur la page **Journal des événements système**.

Pour désactiver l'apparition des journaux d'évènements OEM sur la page **Journal des événements système**, sélectionnez l'option **Filtre d'évènements du journal SEL OEM activé**.

**REMARQUE :** l'option **Filtre d'évènements du journal SEL OEM activé** n'est pas sélectionné par défaut.

### Utilisation de la ligne de commande pour afficher le journal système

```
racadm getsel -i
```

La commande **getsel -i** affiche le nombre d'entrées du journal SEL.

```
racadm getsel <options>
```

**REMARQUE :** si aucun argument n'est spécifié, le journal est affiché dans son intégralité.

**REMARQUE :** pour des informations supplémentaires sur les options que vous pouvez utiliser, voir la sous-commande getsel dans le *Guide de référence de ligne de commande RACADM pour iDRAC6 et CMC* disponible sur le site Web de support à l'adresse **dell.com/support/manuals.**

La commande **clrsel** supprime tous les enregistrements existants du journal SEL.

```
racadm clrsel
```

## Utilisation des notes de travail

Les notes de travail sont des notes ou des commentaires qu'un utilisateur peut ajouter. N'importe quel utilisateur iDRAC peut ajouter une note de travail. Les notes de travail ne peuvent pas être supprimées. Jusqu'à 1000 notes de travail peuvent être visualisées simultanément. Pour une référence rapide, les dix dernières notes de travail s'affichent sur la page d'accueil de l'iDRAC.

**REMARQUE :** si plus de 800 notes de travail sont ajoutées, la page de l'interface utilisateur peut prendre quelques secondes de plus pour se charger. Cela est dû à un montant de données important passant de l'interface utilisateur à l'iDRAC6. Les notes de travail nouvellement ajoutées ne s'afficheront qu'après le chargement de la page. Pour résoudre ce problème, cliquez sur **Réactualiser.**

La page **Notes de travail** vous laisse saisir les notes de travail dans le journal Lifecycle. L'horodotage de la note est enregistré automatiquement.

Pour accéder à la page **Notes de travail**, développez l'arborescence du **système**, puis cliquez sur **Systèmes→ Journaux→ Notes de travail**.

Les affichages de la page **Notes de travail** vous permettent de saisir des notes de travail et offrent d'autres informations tel qu'illustré dans le Tableau 19-8.

Pour saisir les notes de travail :

1 Dans la page **Notes de travail**, sous **Ajouter des notes de travail**, saisissez la note de travail dans le champ affiché.

**REMARQUE :** un maximum de 50 caractères alphanumériques est pris en charge pour la note de travail.

2 Cliquez sur **Save** (Enregistrer).

La nouvelle note de travail s'affiche dans le tableau des notes de travail en dessous de la section **Ajouter des notes de travail**.

**Tableau 19-8. Notes de travail**

| Champ | Description |
|---|---|
| Date/Heure | Affiche l'horodotage enregistré pour chaque saisie de note de travail. Le format est aaaa-mm-jjHhh:mm:ssF, basé sur une horloge de 24 heures, où,<br>aaaa : Année<br>mm : Mois<br>jj : Jour<br>H : Heure<br>hh : Heures<br>mm : Minutes<br>ss : Secondes<br>F : Désignation de fuseau horaire.<br>**REMARQUE :** si le format de l'heure est UTC, ajouter un **F** tout de suite après l'heure sans un espace. **F** correspond à la désignation du fuseau horaire pour un décalage UTC correspondant à zéro. La représentation de **09:30** UTC est ainsi **09:30Z** ou **0930Z**. **14:45:15** UTC correspondrait donc à **14:45:15Z** ou **144515Z**. |
| Remarques | Affiche le contenu saisi de la note de travail. |

# Utilisation des journaux de démarrage POST

**REMARQUE :** Tous les journaux sont effacés une fois que vous avez redémarré iDRAC6.

La page **Capture au démarrage** permet d'accéder aux enregistrements des trois derniers cycles de démarrage disponibles. Ils sont disposés dans l'ordre du plus récent au plus ancien. Si le serveur n'a subi aucun cycle de démarrage, le message **Aucun enregistrement disponible** s'affiche alors. Cliquez sur **Lire** après avoir sélectionné un cycle de démarrage disponible pour l'afficher dans une nouvelle fenêtre.

**REMARQUE :** l'affichage de la capture au démarrage est prise en charge uniquement sous Java, et non sous Active-X.

Pour afficher les journaux de capture au démarrage :

1. Dans l'arborescence du **système**, cliquez sur **Système**.
2. Cliquez sur **l'onglet** Journaux, puis sur l'onglet **Capture au démarrage**.
3. Sélectionnez un cycle de démarrage et cliquez sur **Lire**.

   La vidéo des journaux est ouverte sur un nouvel écran.

   **REMARQUE :** vous devez fermer une vidéo de journal de capture au démarrage ouverte avant d'en lire une autre. Vous ne pouvez pas lire deux journaux simultanément.
4. Cliquez sur **Lecture→ Lire** pour lancer la vidéo de journal de capture au démarrage.
5. Cliquez sur **Lecture→ Commandes de média** pour arrêter la vidéo.

**REMARQUE :** un message vous demandant d'enregistrer un fichier **data.jnlp** au lieu d'ouvrir le visualiseur peut s'afficher. Pour résoudre ce problème, procédez comme suit dans Internet Explorer : accédez à **Outils→ Options Internet→** onglet **Avancé** et désélectionnez l'option *Ne pas enregistrer les pages cryptées sur le disque*.

**REMARQUE :** Si l'iDRAC est réinitialisé, la vidéo de capture au démarrage n'est pas disponible étant donné qu'elle est stockée sur une RAM et supprimée à la réinitialisation de l'iDRAC.

La carte iDRAC6 Express est liée à iDRAC6 lorsque vous entrez dans l'application Unified Server Configurator (USC) en appuyant sur **F10** au cours du démarrage. Si la liaison réussit, le message suivant est consigné dans le journal SEL et dans l'écran LCD : `Mise à niveau d'iDRAC6 réussie`. Si la liaison échoue, le message suivant est consigné dans le journal SEL et dans l'écran LCD : `Échec de la mise à niveau d'iDRAC6`. En outre, lorsqu'une carte iDRAC6 Express contenant un micrologiciel iDRAC6 ancien ou périmé ne prenant pas en charge la plateforme spécifique est insérée dans la carte mère et que le système est démarré, un journal est généré sur l'écran POST : `Le micrologiciel iDRAC est obsolète. Veuillez effectuer la mise à jour vers la version la plus récente du micrologiciel`. Mettez à jour la carte iDRAC6 Express avec le dernier micrologiciel iDRAC6 pour la plateforme spécifique. Pour plus d'informations, voir le *Guide d'utilisation de Dell Lifecycle Controller*.

# Affichage de l'écran du dernier plantage système

**REMARQUE :** la fonctionnalité Écran du dernier plantage exige que le système géré soit configuré avec la fonctionnalité **Récupération automatique** dans Server Administrator. De plus, assurez-vous que la fonctionnalité **Récupération automatique du système** est activée à l'aide d'iDRAC6. Naviguez vers la page **Services** dans l'onglet **Réseau/Sécurité** de la section **Paramètres iDRAC** pour activer cette fonctionnalité.

Pour afficher la page **Écran du dernier plantage** :

1. Dans l'arborescence du **système**, cliquez sur **Système**.
2. Cliquez sur l'onglet **Journaux**, puis sur **Écran du dernier plantage**.

   La page **Écran du dernier plantage** affiche l'écran du plantage le plus récent. Les informations sur le dernier plantage système sont enregistrées dans la mémoire d'iDRAC6 et sont accessibles à distance.

   Pour des informations supplémentaires sur les boutons affichés sur la page **Écran du dernier plantage**, voir l'*Aide en ligne iDRAC6*.

**REMARQUE :** en raison des fluctuations dans l'horloge de récupération automatique, l'**écran du dernier plantage** peut ne pas être saisi lorsque l'horloge de réinitialisation du système est définie sur une valeur inférieure à 30 secondes. Utilisez Server Administrator ou IT Assistant pour définir l'horloge de réinitialisation du système sur 30 secondes au moins et vous assurer que l'**écran du dernier plantage** fonctionne correctement. Pour plus d'informations, voir « Configuration du système géré pour la saisie de l'écran de la dernière panne », à la page 343.

# 20

# Récupération et dépannage d'iDRAC6

Cette section explique comment effectuer des tâches liées à la récupération et au dépannage d'un iDRAC6 en panne.

Vous pouvez utiliser un des outils suivants pour dépanner votre iDRAC6 :

- Journal du RAC
- Console de diagnostics
- Serveur d'identification
- Journal de suivi
- racdump
- coredump

## Utilisation du journal RAC

Le **journal RAC** est un journal permanent conservé dans le micrologiciel iDRAC6. Le journal contient une liste des actions d'utilisateur (ouverture et fermeture de session, modifications des règles de sécurité, par exemple) et des alertes émises par iDRAC6. Les entrées les plus anciennes sont écrasées quand le journal est plein.

Pour accéder au journal RAC depuis l'interface utilisateur (IU) iDRAC6 :

1. Dans l'arborescence du **Système**, cliquez sur **Paramètres iDRAC**.
2. Cliquez sur l'onglet **Journaux**, puis sur **Journal iDRAC**.

La page **Journal iDRAC** contient les informations répertoriées dans le Tableau 20-1.

**Tableau 20-1. Informations sur la page Journal iDRAC**

| Champ | Description |
|---|---|
| **Date/Heure** | Date et heure (par exemple, `Déc 19 16:55:47`).<br>Lorsque iDRAC6 démarre à l'initiale et qu'il ne parvient pas à communiquer avec le système géré, l'heure est affichée comme `Démarrage du système`. |
| **Source** | Interface qui a provoqué l'événement. |
| **Description** | Description brève de l'événement et nom d'utilisateur qui a ouvert une session sur iDRAC6. |

**REMARQUE :** pour des informations sur l'utilisation des boutons de la **Page du journal iDRAC**, voir l'*Aide en ligne iDRAC6*.

# Utilisation de la ligne de commande

Utilisez la commande `getraclog` pour afficher les entrées du journal iDRAC6.

```
racadm getraclog [options]
```

```
racadm getraclog -i
```

La commande **getraclog -i** affiche le nombre d'entrées du journal iDRAC6.

**REMARQUE :** pour des informations supplémentaires, voir getraclog dans le *Guide de référence de la ligne de commande RACADM pour iDRAC et CMC* disponible sur le site Web de support Dell à l'adresse **dell.com/support/manuals**.

Vous pouvez utiliser la commande `clrraclog` pour effacer toutes les entrées du journal iDRAC.

```
racadm clrraclog
```

# Utilisation de la console de diagnostics

L'iDRAC6 fournit un jeu standard d'outils de diagnostic réseau (voir Tableau 20-2) semblables aux outils fournis avec les systèmes Microsoft Windows ou Linux. À l'aide de l'interface Web iDRAC6, vous pouvez accéder aux outils de débogage réseau.

Cliquez sur **Réinitialiser iDRAC6** pour réinitialiser le contrôleur iDRAC. Une opération de démarrage normal s'exécute sur le contrôleur iDRAC.

Pour accéder à la page **Console de diagnostics** :

1. Dans l'arborescence du **système**, cliquez sur **Paramètres iDRAC→** onglet **Dépannage→ Console de diagnostics**.
2. Tapez une commande et cliquez sur **Envoyer**.Le Tableau 20-2 décrit les commandes pouvant être utilisées. Les résultats du débogage apparaissent sur la page **Console de diagnostics**.
3. Pour actualiser la page **Console de diagnostics**, cliquez sur **Actualiser**. Pour exécuter une autre commande, cliquez sur **Retour à la page Diagnostics**.

**Tableau 20-2. Commandes de diagnostic**

| Commande | Description |
|---|---|
| **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 de la table de routage. Si le numéro optionnel de l'interface est indiqué dans le champ de texte à droite de l'option **netstat**, netstat imprime des informations supplémentaires concernant le trafic sur l'interface, l'utilisation du tampon et d'autres informations sur l'interface réseau. |
| **ping** <*adresse IP*> | Vérifie que l'adresse IP de destination est accessible à partir d'iDRAC6 avec le contenu actuel de la table de routage. Une adresse IP de destination doit être entrée dans le champ 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 d'iDRAC6. Pour des informations supplémentaires, voir getraclog dans le *Guide de référence de la ligne de commande RACADM pour iDRAC et CMC* disponible sur le site Web de support Dell à l'adresse **dell.com/support/manuals**. |

# Utilisation du serveur d'identification

La page **Identifier** vous permet d'activer la fonctionnalité Identification du système.

Pour identifier le serveur :

1. Cliquez sur **Système→ Paramètres iDRAC→ Dépannage→ Identifier**.
2. Sur l'écran **Identifier**, sélectionnez la case à cocher **Identifier le serveur** pour activer le clignotement de l'écran LCD et la LED de serveur d'identification arrière.
3. Le champ **Délai d'attente d'identification du serveur** affiche le nombre de secondes durant lesquelles l'écran LCD clignote. Entrez la durée (en secondes) durant laquelle vous souhaitez que l'écran LCD clignote. La plage du délai d'attente est comprise entre 1 et 255 secondes. Si le délai d'attente est défini sur 0 seconde, l'écran LCD clignote de manière continue.
4. Cliquez sur **Appliquer**.

Si vous avez entré **0** seconde, effectuez les étapes suivantes pour le désactiver :

1. Cliquez sur **Système→ Paramètres iDRAC→ Dépannage→ Identifier**.
2. Sur l'écran **Identifier**, désélectionnez l'option **Identifier le serveur**, puis cliquez sur **Appliquer**.

# Utilisation du journal de suivi

Le journal de suivi interne iDRAC6 est utilisé par les administrateurs pour déboguer les problèmes d'alerte et de mise en réseau d'iDRAC6.

Pour accéder au journal de suivi depuis l'interface Web iDRAC6 :

1. Dans l'arborescence du **Système**, cliquez sur **Paramètres iDRAC**.
2. Cliquez sur l'onglet **Diagnostics**.
3. Tapez la commande **gettracelog** ou la commande **racadm gettracelog** dans le champ **Commande**.

   **REMARQUE :** vous pouvez également utiliser cette commande à partir de l'interface de ligne de commande. Pour des informations supplémentaires, voir getraclog dans le *Guide de référence de la ligne de commande RACADM pour iDRAC et CMC* disponible sur le site Web de support Dell à l'adresse **dell.com/support/manuals**.

Le journal de suivi enregistre les informations suivantes :

- DHCP : effectue le suivi des paquets envoyés à un serveur DHCP et reçus de celui-ci.
- IP : effectue le suivi des paquets IP envoyés et reçus.

Le journal de suivi peut en outre contenir des codes d'erreur spécifiques au micrologiciel iDRAC6 qui sont liées au micrologiciel iDRAC6 interne, et non pas au système d'exploitation du système géré.

**REMARQUE :** iDRAC6 ne renvoie pas d'ICMP (ping) si la taille du paquet dépasse 1 500 octets.

# Utilisation de racdump

La commande `racadm racdump` fournit une commande unique pour obtenir des informations sur le vidage et la condition ainsi que des informations générales sur la carte iDRAC6.

**REMARQUE :** cette commande est uniquement disponible sur Telnet, SSH et les interface racadm distantes. Pour des informations supplémentaires, voir racdump dans le *Guide de référence de la ligne de commande RACADM pour iDRAC et CMC* disponible sur le site Web de support Dell à l'adresse **dell.com/support/manuals**.

# Utilisation de coredump

La commande `racadm coredump` affiche des informations détaillées concernant les problèmes critiques récents qui se sont produits avec le RAC. Les informations coredump peuvent être utilisées pour diagnostiquer ces problèmes critiques.

Si disponibles, les informations coredump sont permanentes sur les cycles d'alimentation du RAC et restent disponibles jusqu'à ce qu'une des conditions suivantes se produise :

- Les informations coredump sont effacées avec la sous-commande `coredumpdelete`.
- Une autre condition critique se produit sur le RAC. Dans ce cas, les informations coredump portent sur la dernière erreur critique qui s'est produite.

La commande `racadm coredumpdelete` peut être utilisée pour effacer toutes les données **coredump** actuellement stockées dans le RAC. Pour des informations supplémentaires, voir les sous-commandes `coredump` et `coredumpdelete` dans le *Guide de référence de la ligne de commande RACADM pour iDRAC et CMC* disponible sur le site Web de support Dell à l'adresse **dell.com/support/manuals**.

# 21

# Capteurs

Les capteurs de matériel vous aident à surveiller les systèmes sur votre réseau plus efficacement en vous permettant de prendre les mesures appropriées pour prévenir les sinistres, tels que l'instabilité ou les dommages du système.

Vous pouvez utiliser iDRAC6 pour surveiller les capteurs de matériel pour les batteries, les capteurs de ventilateurs, l'intrusion dans le châssis, les blocs d'alimentation, l'alimentation consommée, la température et les tensions.

## Sondes de batterie

Les capteurs de batterie donnent des informations concernant les batteries de CMOS de la carte système et de la mémoire vive sur la carte mère (ROMB) de stockage.

**REMARQUE :** les paramètres de la batterie ROMB de stockage sont disponibles uniquement si le système dispose d'une ROMB.

## Sondes de ventilateurs

Le capteur des capteurs du ventilateur donne des informations concernant :

- La redondance du ventilateur : la capacité du ventilateur secondaire à remplacer le ventilateur primaire si celui-ci n'arrive pas à dissiper la chaleur à une vitesse prédéfinie.
- La liste des capteurs de ventilateurs : fournit des informations concernant la vitesse de ventilation de tous les ventilateurs du système.

## Sondes d'intrusion dans le châssis

Les capteurs d'intrusion dans le châssis indiquent la condition du châssis, que celui-ci soit ouvert ou fermé.

## Sondes des blocs d'alimentation

Les capteurs des blocs d'alimentation fournissent des informations concernant :

- La condition des blocs d'alimentation
- La redondance du bloc d'alimentation, c'est-à-dire la capacité du bloc d'alimentation redondant à remplacer le bloc d'alimentation primaire si celui-ci fonctionne mal.

**REMARQUE :** s'il n'y a qu'un seul bloc d'alimentation dans le système, la redondance du bloc d'alimentation sera définie sur **Désactivé**.

## Sondes du média Flash amovible

Le capteur du média Flash amovible fournit des informations relatives à la condition de la carte SD vFlash (active ou absente). Pour plus d'informations sur la carte SD vFlash, voir « Configuration de la carte SD vFlash et gestion des partitions vFlash », à la page 295.

## Sondes de surveillance de l'alimentation

La surveillance de l'alimentation donne des informations concernant la consommation d'alimentation en *temps réel*, en watts et en ampères.

Vous pouvez également afficher une représentation graphique de la consommation d'alimentation de la dernière minute, de la dernière heure, du dernier jour ou de la dernière semaine à partir de l'heure actuelle définie dans iDRAC6.

## Capteur de température

Le capteur de température donne des informations concernant la température ambiante de la carte système. Le capteur de température indique si la condition du capteur entre dans la valeur prédéfinie de seuil critique et d'avertissement.

## Sondes de tension

Les capteurs de tension types sont les suivants. Votre système est peut-être doté de celles-ci et/ou d'autres.

- UC [n] VCORE
- Carte système 0,9 V PG
- Carte système 1,5 V ESB2 PG
- Carte système 1,5 V PG
- Carte système 1,8 V PG
- Carte système 3,3 V PG
- Carte système 1,5 V PG
- Carte système fond de panier PG
- Carte système UC VTT
- Carte système linéaire PG

Les capteurs de tension indiquent si la condition des capteurs entre dans la valeur prédéfinie de seuil critique et d'avertissement.

# 22

# Configuration des fonctionnalités de sécurité

iDRAC6 dispose des fonctionnalités de sécurité suivantes :

- Options de sécurité avancée pour l'administrateur d'iDRAC6 :
  - L'option de désactivation de la console virtuelle permet à l'utilisateur du système *local* de désactiver la console virtuelle à l'aide de la fonctionnalité Console virtuelle d'iDRAC6.
  - Les fonctionnalités de désactivation de la configuration locale permettent à l'administrateur d'iDRAC6 *distant* de désactiver de manière sélective la capacité de configuration d'iDRAC6 depuis les éléments suivants :
    - Option ROM du POST du BIOS
    - Système d'exploitation à l'aide de la RACADM locale et des utilitaires Dell OpenManage Server Administrator
- CLI RACADM et interface Web qui prennent en charge le cryptage SSL 128 bits et 40 bits (dans les pays où le cryptage 128 bits n'est pas accepté)

  **REMARQUE :** Telnet ne prend pas en charge le cryptage SSL.
- Configuration du délai d'expiration de la session (en secondes) via l'interface Web ou la CLI RACADM
- Ports IP configurables (si applicable)
- Secure Shell (SSH), qui utilise une couche de transport cryptée pour une sécurité plus élevée
- 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
- Plage d'adresses IP limitée pour les clients se connectant à iDRAC6

# Options de sécurité pour l'administrateur d'iDRAC6

## Désactivation de la configuration locale d'iDRAC6

Les administrateurs peuvent désactiver la configuration locale via l'interface utilisateur graphique (GUI) d'iDRAC6 en sélectionnant **Paramètres iDRAC→ Réseau/Sécurité→ Services**. Lorsque la case à cocher **Désactiver la configuration locale d'iDRAC à l'aide de l'option ROM** est sélectionnée, l'utilitaire de configuration d'iDRAC6 (accessible en appuyant sur <Ctrl+E> lors du démarrage du système) fonctionne en mode Lecture seule, empêchant ainsi les utilisateurs locaux de configurer le périphérique. Lorsque l'administrateur sélectionne la case à cocher **Désactiver la configuration locale d'iDRAC à l'aide de la RACADM**, les utilisateurs locaux ne peuvent pas configurer iDRAC6 via l'utilitaire RACADM ou Dell OpenManage Server Administrator, bien qu'ils puissent toujours lire les paramètres de configuration.

Les administrateurs peuvent activer l'une de ces options ou les deux en même temps à l'aide de l'interface Web.

### Désactivation de la configuration locale lors du redémarrage du système

Cette fonctionnalité désactive la capacité de l'utilisateur du système géré à configurer iDRAC6 pendant le redémarrage du système.

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

**REMARQUE :** cette option n'est prise en charge que par l'utilitaire de configuration d'iDRAC6. Pour une mise à niveau vers cette version, vous devez mettre le BIOS à niveau. Mettez le BIOS à niveau à l'aide du progiciel de mise à jour du BIOS depuis le site Web de support Dell à l'adresse **support.dell.com**.

#### Désactivation de la configuration locale depuis la RACADM locale

Cette fonctionnalité désactive la capacité de l'utilisateur du système géré à configurer iDRAC6 à l'aide de la RACADM locale ou des utilitaires de Dell OpenManage Server Administrator.

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

**PRÉCAUTION : ces fonctionnalités limitent considérablement la capacité de l'utilisateur local à configurer iDRAC6 depuis le système local, y compris la réinitialisation sur les valeurs par défaut de la configuration. Il est recommandé d'utiliser ces fonctionnalités comme bon vous semble. Désactivez uniquement une interface à la fois pour éviter de perdre les privilèges d'ouverture de session dans leur ensemble.**

**REMARQUE :** voir le livre blanc sur la *Désactivation de la configuration locale et du KVM virtuel distant dans DRAC* sur le site du support de Dell à l'adresse **support.dell.com** pour plus d'informations.

Bien que les administrateurs puissent définir les options de configuration locale à l'aide des commandes de la RACADM locale, ils peuvent les réinitialiser uniquement depuis une interface Web iDRAC6 hors bande ou une interface de ligne de commande pour des raisons de sécurité. L'option `cfgRacTuneLocalConfigDisable` s'applique une fois que l'auto-test de mise sous tension du système est terminé et que le système a démarré dans un environnement de système d'exploitation. Le système d'exploitation peut être un système d'exploitation Microsoft Windows Server ou Enterprise Linux capable d'exécuter des commandes de la RACADM locale, ou un système d'exploitation à usage limité tel que Microsoft Windows Preinstallation Environment ou vmlinux servant à exécuter les commandes de la RACADM locale de Dell OpenManage Deployment Toolkit.

Plusieurs situations peuvent amener les administrateurs à désactiver la configuration locale. Par exemple, dans un centre de données ayant plusieurs administrateurs pour les serveurs et les périphériques d'accès distant, les administrateurs chargés de maintenir les piles de logiciels de serveurs peuvent ne pas avoir besoin d'un accès administratif aux périphériques d'accès distant. De même, les techniciens peuvent disposer d'un accès physique aux serveurs lors de la maintenance de routine des systèmes (au cours de laquelle ils peuvent redémarrer les systèmes et accéder au BIOS protégé par mot de passe), mais ils ne doivent pas être en mesure de configurer des périphériques d'accès distant. Dans de telles situations, les administrateurs des périphériques d'accès distant peuvent vouloir désactiver la configuration locale.

Les administrateurs doivent garder à l'esprit que, comme la désactivation de la configuration locale limite considérablement les privilèges de configuration locale, y compris la capacité à réinitialiser iDRAC6 sur sa configuration par défaut, ils doivent uniquement utiliser ces options lorsque cela est nécessaire et ils doivent généralement désactiver une seule interface à la fois pour éviter de perdre entièrement les privilèges d'ouverture de session. Par exemple, si les administrateurs ont désactivé tous les utilisateurs iDRAC6 locaux et n'autorisent que les utilisateurs du service de répertoire Microsoft Active Directory à ouvrir une session sur iDRAC6 et si l'infrastructure d'authentification d'Active Directory échoue par la suite, les administrateurs risquent de ne plus pouvoir ouvrir de session. De même, si les administrateurs ont désactivé toute la configuration locale et placent un iDRAC6 ayant une adresse IP statique sur un réseau comprenant déjà un serveur DHCP (protocole de configuration dynamique d'hôte) et que le serveur DHCP attribue par la suite l'adresse IP d'iDRAC6 à un autre périphérique sur le réseau, le conflit qui en résulte risque de désactiver la connectivité hors bande du DRAC, obligeant les administrateurs à réinitialiser le micrologiciel sur ses paramètres par défaut via une connexion série.

### Désactivation de la console virtuelle d'iDRAC6

Les administrateurs peuvent désactiver de manière sélective la console virtuelle distante d'iDRAC6, offrant ainsi un mécanisme sécurisé flexible permettant à un utilisateur local de travailler sur le système sans qu'un tiers ne voie les actions de l'utilisateur par le biais de la console virtuelle. L'utilisation de cette fonctionnalité nécessite l'installation du logiciel du nœud géré d'iDRAC sur le serveur. Les administrateurs peuvent désactiver la console virtuelle à l'aide de la commande suivante :

```
racadm LocalConRedirDisable 1
```

La commande LocalConRedirDisable désactive les fenêtres de la session de console virtuelle existante lorsqu'elle est exécutée avec l'argument 1

Pour éviter qu'un utilisateur distant n'annule les paramètres de l'utilisateur local, cette commande est uniquement disponible pour la RACADM locale. Les administrateurs peuvent utiliser cette commande sur les systèmes d'exploitation prenant en charge la RACADM, notamment Microsoft Windows Server 2003 et SUSE Linux Enterprise Server 10. Cette commande persistant au fur et à mesure des redémarrages du système, les administrateurs doivent expressément l'annuler pour réactiver la console virtuelle. Pour ceci, Ils peuvent utiliser l'argument 0 :

```
racadm LocalConRedirDisable 0
```

Plusieurs situations peuvent obliger à désactiver la console virtuelle d'iDRAC6. Par exemple, les administrateurs peuvent vouloir empêcher un utilisateur iDRAC6 distant d'afficher les paramètres du BIOS qu'ils configurent sur un système, auquel cas ils peuvent désactiver la console virtuelle lors du POST du système en utilisant la commande `LocalConRedirDisable`. Ils peuvent aussi vouloir renforcer la sécurité en désactivant automatiquement la console virtuelle chaque fois qu'un administrateur ouvre une session sur le système, ce qu'ils peuvent faire en exécutant la commande `LocalConRedirDisable` à partir des scripts d'ouverture de session de l'utilisateur.

**REMARQUE :** voir le livre blanc sur la *Désactivation de la configuration locale et du KVM virtuel distant dans DRAC* sur le site du support de Dell à l'adresse **support.dell.com** pour plus d'informations.

Pour plus d'informations sur les scripts d'ouverture de session, voir **technet2,microsoft.com/windowsserver/en/library/31340f46-b3e5-4371-bbb9-6a73e4c63b621033.mspx**.

# Sécurisation des communications iDRAC6 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 votre iDRAC6 :


- « Secure Sockets Layer (SSL) », à la page 381
- « Requête de signature de certificat (RSC) », à la page 382
- « Accès au menu principal SSL », à la page 383
- « Génération d'une requête de signature de certificat », à la page 383


## Secure Sockets Layer (SSL)

iDRAC6 utilise un serveur Web qui est 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 répandue permettant la communication authentifiée et cryptée entre les clients et les serveurs afin d'empêcher toute écoute indiscrète sur un réseau.

Un système activé SSL :

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

Ce processus de cryptage fournit un haut niveau de protection des données. iDRAC6 applique la norme de cryptage SSL à 128 bits, la forme la plus sécurisée de cryptage généralement disponible pour les navigateurs Internet en Amérique du Nord.

Le serveur Web d'iDRAC6 inclut un certificat numérique SSL Dell auto-signé (référence serveur). Pour assurer une haute sécurité sur Internet :

1. Remplacez le certificat SSL du serveur Web avec un certificat valide depuis un certificat d'autorité de certification.
2. Générez une Requête de signature de certificat (RSC) en soumettant une requête à l'iDRAC6.
3. Fournissez la RSC au certificat d'autorité de certification afin d'obtenir un certificat valide.

### Requête de signature de certificat (RSC)

Une RSC est une requête numérique adressée à une autorité de certification (AC) pour un certificat de serveur sécurisé. Les certificats de serveur sécurisé protègent 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 assurer la sécurité de votre DRAC, il est vivement recommandé de générer une RSC, de l'envoyer à une AC et de téléverser le certificat renvoyé par l'AC.

Une AC est une entité commerciale reconnue dans l'industrie informatique comme répondant à des normes élevées de filtrage et d'identification fiables, ainsi qu'à d'autres critères de sécurité importants. Thawte et VeriSign sont des exemples d'AC. Une fois que l'AC  a reçu votre RSC, elle examine et vérifie les informations contenues dans la RSC. Si le demandeur satisfait aux normes de sécurité de l'autorité de certification, celle-ci lui émet un certificat qui identifie le demandeur de manière unique pour les transactions réseau et Internet.

Une fois que l'AC approuve la RSC et vous envoie un certificat, vous devez le téléverser vers le micrologiciel iDRAC6. Les informations de la RSC stockés sur le micrologiciel iDRAC6 doivent correspondre aux informations contenues dans le certificat.

## Accès au menu principal SSL

1 Étendez l'arborescence du **Système**, puis cliquez sur **Paramètres iDRAC**.

2 Cliquez sur l'onglet **Réseau/Sécurité**, puis sur **SSL**.

Utilisez la page **Menu principal SSL** (voir le Tableau 22-1) pour générer une RSC, téléverser un certificat de serveur existant ou afficher un certificat de serveur existant. Les informations de la RSC sont stockées dans le micrologiciel iDRAC6. Pour des informations sur les boutons disponibles sur la page **SSL**, voir l'*Aide en ligne iDRAC6*.

**Tableau 22-1. Menu principal SSL**

| Champ | Description |
|---|---|
| **Générer une requête de signature de certificat (RSC)** | Cliquez sur **Suivant** pour ouvrir la page qui vous permet de générer une RSC à envoyer à une AC pour demander un certificat Web sécurisé. |
| **Téléverser un certificat de serveur** | Cliquez sur **Suivant** pour téléverser un certificat existant qui appartient à votre société et qu'elle utilise pour contrôler l'accès à iDRAC6.<br>**REMARQUE :** iDRAC6 accepte uniquement les certificats X509 encodés en base 64. Les certificats encodés DER ne sont pas acceptés. Téléversez un nouveau certificat pour remplacer le certificat par défaut que vous avez reçu avec votre iDRAC6. |
| **Afficher le certificat de serveur** | Cliquez sur **Suivant** pour afficher un certificat de serveur existant. |

## Génération d'une requête de signature de certificat

**REMARQUE :** chaque RSC écrase la RSC qui se trouve déjà dans le micrologiciel. Avant qu'iDRAC accepte votre certificat signé, la RSC du micrologiciel doit correspondre au certificat renvoyé par la CA.

1 Sur la page **Menu principal SSL**, sélectionnez **Générer une requête de signature de certificat (RSC)** et cliquez sur **Suivant**.

2 Sur la page **Générer une requête de signature de certificat (RSC)**, tapez une valeur pour chaque attribut RSC.

Le Tableau 22-2 décrit les options de la page **Générer une requête de signature de certificat (RSC)**.

3 Cliquez sur **Générer** pour ouvrir ou enregistrer la RSC.

4 Cliquez sur le bouton approprié de la page **Générer une requête de signature de certificat (RSC)** pour continuer. Pour des informations supplémentaires sur les boutons disponibles de la page **Requête de signature de certificat (RSC)**, voir l'*Aide en ligne iDRAC6*.

**Tableau 22-2. 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 **sociétéxyz.com**). Les caractères alphanumériques, les tirets et les points sont valides. |
| **Nom de l'organisation** | Nom associé à cette organisation (par exemple, Compagnie XYZ). Les caractères alphanumériques, les tirets et les points sont valides. |
| **Unité organisationnelle** | Nom associé au service de l'organisation, comme un département (par exemple, Groupe de l'entreprise). Les caractères alphanumériques, les tirets et les points sont valides. |
| **Ville** | Ville ou autre lieu où se trouve l'entité à certifier (par exemple, Round Rock). Les caractères alphanumériques, les tirets et les points sont valides. |
| **Nom de l'état** | État ou province où se trouve l'entité qui fait la demande de certification (par exemple, Texas). Les caractères alphanumériques, les tirets et les points sont valides. |
| **Code de pays** | Nom du pays où se trouve l'entité qui fait la demande de certification. Utilisez le menu déroulant pour sélectionner le pays. |
| **E-mail** | Adresse e-mail associée à la RSC. Vous pouvez taper l'adresse e-mail de votre société ou une adresse e-mail que vous voulez associer à la RSC. Ce champ est optionnel. |

### Affichage d'un certificat de serveur

1 Sur la page **Menu principal SSL**, sélectionnez **Afficher le certificat de serveur** et cliquez sur **Suivant**.

Le Tableau 22-3 décrit les champs et les descriptions associées énumérés dans la fenêtre **Certificat**.

2 Cliquez sur le bouton approprié de la page **Afficher le certificat de serveur** pour continuer.

**Tableau 22-3. Informations relatives au certificat**

| Champ | Description |
|---|---|
| **Numéro de série** | Numéro de série du certificat |
| **Informations sur le sujet** | Attributs du certificat saisis par le sujet |
| **Informations sur l'émetteur** | Attributs du certificat renvoyés par l'émetteur |
| **Valide du** | Date d'émission du certificat |
| **Valide jusqu'au** | Date d'expiration du certificat |

# Utilisation de Secure Shell (SSH)

Pour des informations sur l'utilisation de SSH, voir « Utilisation de Secure Shell (SSH) », à la page 95.

# Configuration des services

**REMARQUE :** pour modifier ces paramètres, vous devez avoir le droit **Configurer iDRAC**. De plus, l'utilitaire de ligne de commande de la RACADM distante peut être activé uniquement si l'utilisateur a ouvert une session en tant que **root**.

1 Développez l'arborescence **Système**, puis cliquez sur **Paramètres iDRAC**.

2 Cliquez sur l'onglet **Réseau/Sécurité**, puis sur **Services**.

3 Configurez les services suivants, si nécessaire :

- Configuration locale (Tableau 22-4)
- Tableau 22-5Serveur Web ()
- SSH (Tableau 22-6)
- Telnet (Tableau 22-7)

- RACADM distant (Tableau 22-8)
- Agent SNMP (Tableau 22-9)
- Agent de récupération de système automatique (Tableau 22-10)

Utilisez l'**agent de récupération de système automatique** pour activer la fonctionnalité **Écran du dernier plantage** d'iDRAC6.

**REMARQUE :** Server Administrator doit être installé avec sa fonctionnalité **Récupération automatique** activée en configurant **Action** sur **Redémarrer le système**, **Arrêter le système** ou **Exécuter un cycle d'alimentation sur le système** pour que l'**Écran du dernier plantage** fonctionne dans iDRAC6.

4 Cliquez sur **Appliquer les changements** pour appliquer les paramètres de la page de services.

**Tableau 22-4. Paramètres de configuration locale**

| Paramètre | Description |
|---|---|
| Désactiver la configuration locale d'iDRAC avec l'option ROM | Désactive la configuration locale d'iDRAC à l'aide de l'option ROM. L'option ROM vous invite à saisir le module de configuration en appuyant sur <Ctrl+E> pendant le redémarrage du système. |
| Désactiver la configuration locale d'iDRAC avec la RACADM | Désactive la configuration locale d'iDRAC à l'aide de la RACADM locale. |

**Tableau 22-5. Paramètres du serveur Web**

| Paramètre | Description |
|---|---|
| **Enabled (Activé)** | Active ou désactive le serveur Web. Coché = Activé ; décoché = Désactivé. |
| **Nombre maximal de sessions** | Nombre maximal de sessions simultanées autorisées pour ce système. |
| **Sessions actives** | Nombre de sessions en cours sur le système, inférieur ou égal au **Nombre maximal de sessions**. |

**Tableau 22-5. Paramètres du serveur Web *(suite)***

| Paramètre | Description |
|---|---|
| Délai d'attente | Durée, en secondes, pendant laquelle une connexion peut rester inactive. La session est annulée quand le délai d'expiration est atteint. Les modifications apportées au paramètre Délai d'expiration prennent immédiatement effet et mettent fin à la session d'interface Web en cours. Le serveur Web est également réinitialisé. Veuillez attendre quelques minutes avant d'ouvrir une nouvelle session d'interface Web. La plage du délai d'expiration est comprise entre 60 et 10 800 secondes. La valeur par défaut est de 1 800 secondes. |
| Numéro de port HTTP | Port utilisé par iDRAC qui écoute une connexion serveur. Le paramètre par défaut est 80. |
| Numéro de port HTTPS | Port utilisé par iDRAC qui écoute une connexion serveur. Le paramètre par défaut est 443. |

**Tableau 22-6. Paramètres SSH**

| Paramètre | Description |
|---|---|
| Enabled (Activé) | Active ou désactive SSH. Lorsqu'il est coché, SSH est activé. |
| Délai d'attente | Délai d'expiration en cas d'inactivité Secure Shell, en secondes. La plage du délai d'expiration est comprise entre 60 et 1 920 secondes. Saisissez 0 seconde pour désactiver la fonctionnalité Délai d'expiration. Le délai d'expiration par défaut est 300. |
| Numéro de port | Port sur lequel iDRAC6 écoute une connexion SSH. Le numéro de port par défaut est 22. |

**Tableau 22-7. Paramètres Telnet**

| Paramètre | Description |
|---|---|
| Enabled (Activé) | Active ou désactive Telnet. Lorsqu'il est coché, Telnet est activé. |
| Délai d'attente | Délai d'expiration en cas d'inactivité Telnet, en secondes. La plage du délai d'expiration est comprise entre 60 et 1 920 secondes. Saisissez 0 seconde pour désactiver la fonctionnalité Délai d'expiration. Le délai d'expiration par défaut est 300. |
| Numéro de port | Port sur lequel iDRAC6 écoute une connexion Telnet. Le numéro de port par défaut est 23. |

**Tableau 22-8. Paramètres de RACADM distant**

| Paramètre | Description |
|---|---|
| Enabled (Activé) | Active/Désactive la RACADM distante. Lorsque la case est cochée, la RACADM distante est activée. |
| Sessions actives | Nombre de sessions en cours sur le système. |

**Tableau 22-9. Paramètres de l'agent SNMP**

| Paramètre | Description |
|---|---|
| Enabled (Activé) | Active ou désactive l'agent SNMP. Coché = Activé ; décoché = Désactivé. |
| Nom de communauté | Définissez la chaîne de la communauté SNMP à utiliser. Le nom de communauté peut comporter jusqu'à 31 caractères non blancs. Le paramètre par défaut est public. |

**Tableau 22-10. Paramètre de l'agent de récupération de système automatique**

| Paramètre | Description |
|---|---|
| Enabled (Activé) | Active l'agent de récupération de système automatique. |

# Activation d'options de sécurité iDRAC6 supplémentaires

Pour empêcher tout accès non autorisé à votre système distant, iDRAC6 fournit les fonctionnalités suivantes :

- Filtrage des adresses IP (IPRange) : définit une plage spécifique d'adresses IP auxquelles peut accéder iDRAC6.
- Blocage des adresses IP : limite le nombre d'échecs de tentatives d'ouverture de session à partir d'une adresse IP spécifique

Ces fonctionnalités sont désactivées dans la configuration par défaut d'iDRAC6. Utilisez la sous-commande suivante ou l'interface Web pour activer ces fonctionnalités :

```
racadm config -g cfgRacTuning -o <nom_objet> <valeur>
```

De plus, utilisez ces fonctionnalités en association avec les valeurs de délai d'expiration de la session en cas d'inactivité appropriées et un plan de sécurité défini pour votre réseau.

Les sous-sections suivantes fournissent des informations supplémentaires sur ces fonctionnalités.

#### Filtrage IP (IpRange)

Le filtrage des adresses IP (ou *contrôle de plage IP*) permet un accès à iDRAC6 uniquement à partir des clients ou des stations de gestion dont les adresses IP sont comprises dans une plage spécifique à l'utilisateur. Toutes les autres ouvertures de session sont refusées.

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

- cfgRacTuneIpRangeAddr
- cfgRacTuneIpRangeMask

La propriété **cfgRacTuneIpRangeMask** est appliquée à la fois à l'adresse IP entrante et aux propriétés **cfgRacTuneIpRangeAddr**. Si les résultats des deux propriétés sont identiques, la demande d'ouverture de session entrante est autorisée à accéder à iDRAC6. Les ouvertures de session à partir d'adresses IP situées à l'extérieur de cette plage reçoivent une erreur.

L'ouverture de session a lieu si l'expression suivante est égale à zéro :

`cfgRacTuneIpRangeMask & (<adresse_IP_entrante> ^ cfgRacTuneIpRangeAddr)`

où & est l'opérateur de bits AND des quantités et ^ est l'opérateur de bits OR exclusif.

Voir le *Guide de référence de la ligne de commande RACADM pour iDRAC6 et CMC* disponible sur le site Web de support Dell à l'adresse **dell.com/support/manuals** pour une liste complète des propriétés **cfgRacTuning**.

**Tableau 22-11. Propriétés de filtrage des adresses IP (IpRange)**

| Propriété | Description |
|---|---|
| **cfgRacTuneIpRangeEnable** | Active la fonctionnalité Contrôle de plage IP. |
| **cfgRacTuneIpRangeAddr** | Détermine le format binaire d'adresse IP accepté en fonction des 1 dans le masque de sous-réseau.<br><br>Cette propriété correspond à l'opérateur de bits AND avec **cfgRacTuneIpRangeMask** pour déterminer la partie supérieure de l'adresse IP autorisée. Toute adresse IP comportant ce format binaire dans ses bits supérieurs est autorisée à établir une session iDRAC6. Les ouvertures de session à partir des adresses IP qui sont situées à l'extérieur de cette plage échouent. Les valeurs par défaut dans chaque propriété permettent à une plage d'adresses de 192.168.1.0 à 192.168.1.255 d'établir une session iDRAC6. |
| **cfgRacTuneIpRangeMask** | Définit les positions binaires significatives dans l'adresse IP. Le masque de sous-réseau doit avoir la forme d'un masque de réseau où les bits de plus fort poids sont tous des 1 avec une transition simple vers tous les zéros dans les bits de niveau inférieur. |

### Activation du filtrage IP

Voir l'exemple de commande suivant pour la configuration du filtrage IP.

voir « Utilisation de la RACADM à distance », à la page 117 pour plus d'informations sur la RACADM et les commandes RACADM.

**REMARQUE :** les commandes RACADM suivantes bloquent toutes les adresses IP sauf 192.168.0.57.

Pour restreindre l'ouverture de session à une seule adresse IP (par exemple, 192.168.0.57), utilisez le masque complet, comme illustré dans la section suivante :

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

racadm config -g cfgRacTuning -o
cfgRacTuneIpRangeAddr 192.168.0.57

racadm config -g cfgRacTuning -o
cfgRacTuneIpRangeMask 255.255.255.255
```

Pour restreindre les ouvertures de session à un petit ensemble de quatre adresses IP adjacentes (par exemple, 192.168.0.212 à 192.168.0.215), sélectionnez tout, sauf les deux bits inférieurs dans le masque, comme illustré dans la section suivante :

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

racadm config -g cfgRacTuning -o
cfgRacTuneIpRangeAddr 192.168.0.212

racadm config -g cfgRacTuning -o
cfgRacTuneIpRangeMask 255.255.255.252
```

#### Instructions concernant le filtrage IP

Observez les instructions suivantes lorsque vous activez le filtrage IP :

- Assurez-vous que **cfgRacTuneIpRangeMask** est configuré sous forme de masque de réseau, où les bits de plus fort poids sont des 1 (ce qui définit le sous-réseau dans le masque) avec une transition de tous les 0 dans les bits de niveau inférieur.
- Utilisez l'adresse de base de la plage de votre choix comme valeur pour **cfgRacTuneIpRangeAddr**. La valeur binaire de 32 bits de cette adresse doit avoir des zéros dans tous les bits de niveau inférieur où il y a des zéros dans le masque.

#### Blocage IP

Le blocage IP détermine de manière dynamique à quel moment un nombre excessif d'échecs d'ouverture de session se produit à partir d'une adresse IP particulière et (bloque (ou empêche) l'adresse d'ouvrir une session sur iDRAC6 pendant une période présélectionnée.

Le paramètre Blocage IP utilise les fonctionnalités de groupe **cfgRacTuning** telles que :

- Le nombre d'échecs d'ouverture de session autorisés
- L'intervalle de temps en secondes au cours duquel ces échecs doivent se produire
- La durée en secondes pendant laquelle l'adresse IP *coupable»* n'est pas autorisée à établir une session une fois que le nombre total d'échecs autorisés est dépassé

Comme les échecs d'ouverture de session s'accumulent à partir d'une adresse IP spécifique, ils sont *datés»* par un compteur interne. Lorsque l'utilisateur ouvre une session avec succès, l'historique des échecs est effacé et le compteur interne est remis à zéro.

**REMARQUE :** lorsque des tentatives d'ouverture de session sont refusées à partir de l'adresse IP client, certains clients SSH peuvent afficher le message suivant : `identification d'échange ssh : connexion fermée par l'hôte distant`.

Voir le *Guide de référence de la ligne de commande RACADM pour iDRAC6 et CMC* disponible sur le site Web de support Dell à l'adresse **dell.com/support/manuals** pour une liste complète des propriétés **cfgRacTuning**.

Le Tableau 22-12 répertorie les paramètres définis par l'utilisateur.

**Tableau 22-12. Propriétés de restriction des nouvelles tentatives d'ouverture de session**

| Propriété | Définition |
|---|---|
| **cfgRacTuneIpBlkEnable** | Active la fonctionnalité Blocage IP.<br>Lorsque des échecs consécutifs (**cfgRacTuneIpBlkFailCount**) à partir d'une seule adresse IP sont rencontrés pendant une période de temps spécifique (**cfgRacTuneIpBlkFailWindow**), toutes les tentatives ultérieures d'établissement d'une session à partir de cette adresse sont rejetées pendant un certain temps (**cfgRacTuneIpBlkPenaltyTime**). |
| **cfgRacTuneIpBlkFailCount** | Définit le nombre d'échecs d'ouverture de session à partir d'une adresse IP avant que les tentatives d'ouverture de session ne soient rejetées. |
| **cfgRacTuneIpBlkFailWindow** | Intervalle de temps en secondes pendant lequel les échecs d'ouverture de session sont comptés. Lorsque le nombre d'échecs dépasse cette limite, le compteur est remis à zéro. |
| **cfgRacTuneIpBlkPenaltyTime** | Définit l'intervalle de temps en secondes au cours duquel toutes les tentatives d'ouverture de session à partir d'une adresse IP avec des échecs excessifs sont rejetées. |

### Activation du blocage IP

L'exemple suivant empêche une adresse IP client d'établir une session pendant cinq minutes si ce client a échoué à ses cinq tentatives d'ouverture de session en l'espace d'une minute.

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

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailCount 5

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailWindows 60

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkPenaltyTime 300
```

L'exemple suivant empêche plus de trois échecs de tentatives en l'espace d'une minute et empêche toute tentative d'ouverture de session supplémentaire pendant une heure.

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

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailCount 3

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkFailWindows 60

racadm config -g cfgRacTuning -o
cfgRacTuneIpBlkPenaltyTime 3600
```

### Configuration des paramètres de sécurité réseau à l'aide de l'interface GUI iDRAC6

**REMARQUE :** vous devez disposer du droit **Configurer iDRAC6** pour effectuer les étapes suivantes.

1. Dans l'arborescence du **Système**, cliquez sur **Paramètres iDRAC**.
2. Cliquez sur l'onglet **Réseau/Sécurité**, puis sur **Réseau**.
3. Sur la page **Configuration réseau**, cliquez sur **Paramètres avancés**.
4. Sur la page **Sécurité réseau**, configurez les valeurs d'attribut, puis cliquez sur **Appliquer les changements**.

   Le Tableau 22-13 décrit les paramètres de la page **Sécurité réseau**.
5. Cliquez sur le bouton approprié de la page **Sécurité réseau** pour continuer. Pour des informations supplémentaires sur les boutons de la page **Sécurité du réseau**, voir l'*Aide en ligne iDRAC6*.

**Tableau 22-13. Paramètres de la page Sécurité réseau**

| Paramètres | Description |
|---|---|
| **Plage IP activée** | Active la fonctionnalité Contrôle de la plage IP, qui définit une plage d'adresses IP spécifique pouvant accéder à iDRAC6. |
| **Adresse de la plage IP** | Détermine le format binaire d'adresse IP accepté, en fonction des 1 dans le masque de sous-réseau. Cette valeur correspond à l'opérateur de bits AND avec le masque de sous-réseau de la plage IP pour déterminer la partie supérieure de l'adresse IP autorisée. Toute adresse IP comportant ce format binaire dans ses bits supérieurs est autorisée à établir une session iDRAC6. Les ouvertures de session à partir des adresses IP qui sont situées à l'extérieur de cette plage échouent. Les valeurs par défaut dans chaque propriété permettent à une plage d'adresses de 192.168.1.0 à 192.168.1.255 d'établir une session iDRAC6. |
| **Masque de sous-réseau de la plage IP** | Définit les positions binaires significatives dans l'adresse IP. Le masque de sous-réseau doit avoir la forme d'un masque de réseau, où les bits de plus fort poids sont tous des 1 avec une transition simple vers tous les zéros dans les bits de niveau inférieur.<br>Par exemple, **255.255.255.0**. |
| **Blocage IP activé** | Active la fonctionnalité Blocage d'adresse IP, qui limite le nombre d'échecs de tentatives d'ouverture de session à partir d'une adresse IP spécifique pendant une durée présélectionnée. |
| **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. |
| **Plage d'échecs avant blocage IP** | Détermine la période en secondes pendant laquelle des échecs du nombre d'échecs avant blocage IP doivent se produire pour déclencher la période de pénalité avant blocage IP. |
| **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. |

# Index

## D



## E



## F



## G

## I



## J



## K

## L



## M



## N



## O

## S

## T



## U

## V