Integrated Dell™ Remote Access Controller 6 (iDRAC6) Version 1.1 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.

Juin 2009

Retour á la page du sommaire

Glossaire

Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.1

AC

Une autorité de certification est une entité commerciale reconnue dans l'industrie de l'informatique pour ses critères élevés en matière de dépistage et d'identification fiables et d'autres critères de sécurité importants. Thawte et VeriSign sont des exemples de CA. Une fois que la CA a reçu votre CSR, elle examine et vérifie les informations contenues dans la CSR. 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.

Active Directory

Active Directory est un système centralisé et standardisé qui automatise la gestion réseau des données utilisateur, de la sécurité et des ressources distribuées, et permet l'interaction avec d'autres répertoires. Active Directory a été tout particulièrement conçu pour les environnements de mise en réseau distribués.

adresse MAC

Sigle de Media Access Control (contrôle d'accès aux médias), une adresse unique intégrée aux composants physiques d'un NIC.

ARP

Sigle d'Address Resolution Protocol (protocole de résolution d'adresse), une méthode pour trouver l'adresse Ethernet d'un hôte à partir de son adresse Internet.

ASCII

Sigle d'American Standard Code for Information Interchange (code standard pour l'échange d'informations), une représentation codée qui sert à afficher ou à imprimer des lettres, des chiffres et d'autres caractères.

BIOS

Sigle de Basic Input/Output System (système d'entrée/sortie de base), la partie d'un logiciel système qui fournit l'interface de plus bas niveau aux périphériques et qui contrôle la première étape du processus de démarrage du système, y compris l'installation du système d'exploitation dans la mémoire.

bus

Ensemble de conducteurs connectant les diverses unités fonctionnelles d'un ordinateur. Les bus sont nommés d'après le type de données qu'ils transportent, comme bus de données, bus d'adresse ou bus PCI.

Carte iDRAC6

Sigle d'Integrated Dell Remote Access Controller, système de contrôle/surveillance « Système sur une puce » intégré des serveurs Dell 11G PowerEdge.

Carte réseau (NIC)

Abréviation de Network Interface Card (carte d'interface réseau). Une carte adaptateur à circuits imprimés, installée dans un ordinateur pour fournir une connexion physique à un réseau.

CD

Abréviation de Compact Disc (disque compact).

CHAP

Sigle de Challenge-Handshake Authentication Protocol (protocole d'authentification sécurisée), une méthode d'authentification utilisée par les serveurs PPP pour valider l'identité de l'origine de la connexion.

CIM

Sigle de Common Information Model (modèle commun d'informations), un protocole conçu pour la gestion de systèmes par réseau.

CLI

Abréviation de Command Line Interface (interface de ligne de commande).

CLP

Abréviation de Command-Line Protocol (protocole de ligne de commande).

Console SAC

Sigle de Special Administration Console (console de gestion spéciale) de Microsoft.

DDNS

Abréviation de Dynamic Domain Name System (système de noms de domaine dynamique).

DHCP

Abréviation de Dynamic Host Configuration Protocol (protocole de configuration dynamique de l'hôte), un protocole qui permet d'attribuer des adresses IP de façon dynamique aux ordinateurs sur un réseau local.

disque RAM

Un programme résidant en mémoire qui émule un disque dur. L'iDRAC6 maintient un disque RAM dans sa mémoire.

DLL

Abréviation de Dynamic Link Library (bibliothèque de liens dynamiques), une bibliothèque de petits programmes qui peuvent être invoqués en cas de besoin par un programme plus grand qui s'exécute sur le système. Le petit programme qui permet à un programme plus grand de communiquer avec un périphérique spécifique comme une imprimante ou un scanner, par exemple, est souvent fourni sous la forme d'un programme (ou fichier) DLL.

DMTF

Abréviation de Distributed Management Task Force (force de tâches de gestion distribuées).

DNS

Abréviation de Domain Name System (système de noms de domaine).

DSU

Abréviation de Disk Storage Unit (unité de stockage sur disque).

FQDN

Sigle de Fully Qualified Domain Names (noms de domaines pleinement qualifiés). Microsoft® Active Directory® ne prend en charge que les noms FQDN de 64 octets ou moins.

FSMO

Flexible Single Master Operation (rôle d'opération en tant que maître unique flexible). C'est la façon de Microsoft de garantir l'atomicité de l'opération d'extension.

GMT

Abréviation de Greenwich Mean Time (temps moyen de Greenwich), l'heure standard commune à tous les endroits du monde. GMT reflète l'heure solaire moyenne le long du premier méridien (0 de longitude) qui passe par l'observatoire de Greenwich près de Londres, au Royaume-Uni.

GPIO

Abréviation de General Purpose Input/Output (Entrée/Sortie polyvalentes).

GRUB

Sigle de GRand Unified Bootloader, nouveau chargeur Linux très répandu.

GUI

Abréviation de Graphical User Interface (interface utilisateur graphique), une interface d'affichage informatique qui utilise des éléments comme des fenêtres, des boîtes de dialogue et des boutons par opposition à une interface d'invite de commande, dans laquelle toute l'interaction utilisateur est affichée et tapée en texte.

iAMT

Intel® Active Management Technology : offre des fonctions de gestion de systèmes plus sécurisées que l'ordinateur soit sous ou hors tension, et indépendamment du fait que le système d'exploitation réponde ou non.

ICMB

Abréviation de Intelligent Enclosure Management Bus (bus de gestion intelligente de l'enceinte).

ICMP

Abréviation d'Internet Control Message Protocol (protocole de messages de contrôle d'Internet).

ID

Abréviation d'identificateur, souvent utilisé pour faire référence à l'identificateur d'utilisateur (ID d'utilisateur) ou l'identificateur d'objet (ID d'objet).

interruption SNMP

Une notification (événement) générée par iDRAC6 et contenant des informations sur les modifications de l'état du système géré ou sur des problèmes matériels potentiels.

IP

Abréviation d'Internet Protocol (protocole Internet), la couche réseau de TCP/IP. Le protocole IP fournit le routage, la fragmentation et le réassemblage des paquets.

IPMB

Abréviation d'Intelligent Platform Management Bus (bus de gestion de plate-forme intelligente), un bus utilisé dans la technologie de gestion de systèmes.

IPMI

Abréviation d'Intelligent Platform Management Interface (interface de gestion de plate-forme intelligente), une partie de la technologie de gestion de systèmes.

journal du matériel

Enregistre les événements générés par iDRAC6.

Kb/s

Abréviation de kilobits par seconde, une vitesse de transfert des données.

LAN

Abréviation de Local Area Network (réseau local).

LDAP

Abréviation de Lightweight Directory Access Protocol (protocole allégé d'accès aux annuaires).

LOM

Abréviation de Local area network On Motherboard (réseau local sur carte mère).

LUN

Sigle d'unité logique.

MAC

Sigle de Media Access Control (contrôle d'accès aux médias), une sous-couche de réseau entre un nud de réseau et la couche physique du réseau.

MAP

Abréviation de Manageability Access Point (point d'accès de gérabilité).

Mb/s

Abréviation de mégabits par seconde, une vitesse de transfert des données.

MIB

Abréviation de Management Information Base (base d'informations de gestion).

MII

Abréviation de Media Independent Interface (interface de média indépendante).

NAS

Abréviation de Network Attached Storage (stockage connecté au réseau).

OID

Abréviation d'Object Identifier (identificateur d'objet).

Onduleur

Abréviation de Uninterruptible Power Supply (système d'alimentation sans coupure).

PCI

Abréviation de Peripheral Component Interconnect (interconnexion de composants périphériques), une technologie d'interface et de bus standard pour connecter des périphériques à un système et pour communiquer avec ces périphériques.

POST

Sigle de Power-On Self-Test (auto-test de démarrage), une séquence de tests de diagnostic exécutée automatiquement par un système lorsqu'il est mis sous tension.

PPP

Abréviation de Point-to-Point Protocol (protocole point à point), un protocole Internet standard pour la transmission de datagrammes de couches de réseau (comme les paquets IP) sur des liens point à point série.

RAC

Abréviation de Remote Access Controller.

RAM

Sigle de Random-Access Memory (mémoire vive). La RAM est une mémoire universelle lisible et inscriptible sur les systèmes et sur iDRAC6.

redirection de console

La redirection de console est une fonction qui transfère l'écran d'affichage, les fonctions de la souris et les fonctions du clavier d'un serveur géré aux périphériques correspondants d'une station de gestion. Vous pouvez ensuite utiliser la console du système de la station de gestion pour contrôler le serveur géré.

Restaurer

Revenir à une version antérieure d'un logiciel ou d'un micrologiciel.

ROM

Sigle de Read-Only Memory (mémoire morte), mémoire dont les données peuvent être lues, mais sur laquelle des données ne peuvent pas être écrites.

RSC

Abréviation de Certificate Signing Request (requête de signature de certificat).

SAP

Abréviation de Service Access Point (point d'accès de service).

schéma étendu

Solution utilisée avec Active Directory pour configurer l'accès utilisateur à iDRAC6 ; elle utilise des objets Active Directory définis par Dell.

schéma standard

Solution utilisée avec Active Directory pour configurer l'accès utilisateur à iDRAC6 ; elle utilise uniquement des objets de groupe Active Directory.

SEL

Sigle de System Event Log (journal des événements système).

serveur géré

Le serveur géré est le système dans lequel iDRAC6 est intégré.

SM-CLP

Abréviation de Server Management-Command Line Protocol. SM-CLP est un sous-composant de l'initiative DMTF SMASH destinée à rationaliser la gestion de serveur à travers des plateformes multiples. La spécification SM-CLP, conjointement à MEAS (Managed Element Addressing Specification) et à de nombreux profils SM-CLP, décrit les verbes et les cibles correspondant à l'exécution de diverses tâches de gestion.

SMI

Abréviation de Systems Management Interrupt (interruption de gestion de systèmes).

SMTP

Abréviation de Simple Mail Transfer Protocol (protocole simplifié de transfert de courrier), un protocole utilisé pour le transfert du courrier électronique entre systèmes, en général sur un Ethernet.

SMWG

Abréviation de Systems Management Working Group (groupe de travail de gestion de systèmes).

SSH

Abréviation de Secure Shell (protocole de connexions sécurisées).

SSL

Abréviation de Secure Sockets Layer (couche de sockets sécurisée).

Station de gestion

La station de gestion est le système à partir duquel un administrateur gère à distance un système Dell utilisant iDRAC6.

système géré

Un système surveillé par une station de gestion est désigné système géré.

TAP

Abréviation de Telelocator Alphanumeric Protocol (protocole alphanumérique télélocalisateur), un protocole utilisé pour envoyer des requêtes à un service de télémessagerie.

TCP/IP

Abréviation de Transmission Control Protocol/Internet Protocol (protocole de contrôle de transmission/protocole Internet), qui représente l'ensemble des protocoles Ethernet standard qui comprennent les protocoles de couche de réseau et de couche de transport.

TFTP

Abréviation de Trivial File Transfer Protocol (protocole simplifié de transfert de fichiers), un protocole simple de transfert de fichiers qui sert à télécharger le code de démarrage sur les périphériques ou systèmes sans disque.

tr/min

Abréviation de Red Hat® Package Manager (gestionnaire de paquetages Red Hat), un système de gestion de progiciels pour le système d'exploitation Red Hat Enterprise Linux® qui facilite l'installation de progiciels de logiciels. Il ressemble à un programme d'installation.

Unified Server Configurator

Dell Unified Server Configurator (USC) est un utilitaire intégré qui autorise les tâches de gestion de systèmes et de stockage depuis un environnement intégré tout au long du cycle de vie du serveur.

USB

Abréviation de Universal Serial Bus (bus série universel).

USC

Abréviation de Unified Server Configurator.

UTC

Abréviation d'Universal Coordinated Time (temps universel). *Voir* GMT.

VLAN

Abréviation de Virtual Local Area Network (réseau local virtuel).

VNC

Abréviation de Virtual Network Computing (informatique de réseau virtuel).

Voyant

Abréviation de Light-Emitting Diode (diode électroluminescente).

VT-100

Abréviation de Video Terminal (terminal vidéo) 100, utilisé par la plupart des programmes d'émulation de terminal.

WAN

Abréviation de Wide Area Network (réseau étendu).

WS-MAN

Abréviation du protocole Web Services for Management (WS-MAN). WS-MAN est un mécanisme de transport destiné à l'échange d'informations. WS-MAN offre un langage universel permettant aux dispositifs de partager des données de manière à pouvoir être gérés plus aisément.

Retour á la page du sommaire

Retour á la page du sommaire

Présentation de la sous-commande RACADM

Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.1

Cette section fournit des descriptions des sous-commandes qui sont disponibles dans l'interface de ligne de commande RACADM.

PRÉCAUTION : Racadm définit la valeur des objets sans effectuer de validation fonctionnelle sur ces derniers. Par exemple, RACADM permet de définir l'objet Validation du certificat sur 1 avec l'objet Active Directory défini sur 0, même si la validation du certificat se produit uniquement si Active Directory® est activé. De même, l'objet cfgADSSOEnable peut être défini sur 0 ou 1 même si l'objet cfgADEnable est défini sur 0, mais devient effectif uniquement si Active Directory est activé.

---

help

REMARQUE : Pour utiliser cette commande, vous devez disposer de l'autorisation **Ouvrir une session sur l'iDRAC**.

Le Tableau A-1 décrit la commande **help**.

Tableau A-1. Commande help

Commande	Définition
help	Répertorie toutes les sous-commandes qui peuvent être utilisées avec **RACADM** et les décrit brièvement.

Synopsis

```
racadm help

racadm help <sous-commande>
```

Description

La sous-commande **help** répertorie toutes les sous-commandes disponibles avec la commande **racadm,** avec une ligne de description. Vous pouvez aussi taper une sous-commande après **help** pour obtenir la syntaxe d'une sous-commande spécifique.

Résultat

La commande **racadm help** affiche une liste complète des sous-commandes.

La commande **racadm help** <*sous-commande*> n'affiche des informations que pour la sous-commande spécifiée.

Interfaces prises en charge

- RACADM locale
- RACADM distant
- RACADM telnet/ssh/série

---

arp

REMARQUE : Pour utiliser cette commande, vous devez avoir le droit **Exécuter des commandes de diagnostic**.

Le Tableau A-2 décrit la commande **arp**.

Tableau A-2. Commande arp

Commande	Définition
arp	Affiche le contenu de la table ARP. Les entrées de la table ARP ne peuvent être ni ajoutées ni supprimées.

Synopsis

```
racadm arp
```

Interfaces prises en charge

- RACADM distant
- RACADM telnet/ssh/série

---

clearasrscreen

REMARQUE : Pour utiliser cette commande, vous devez avoir le droit **Effacer les journaux**.

Le Tableau A-3 décrit la sous-commande **clearasrscreen**.

Tableau A-3. clearasrscreen

Sous-commande	Définition
clearasrscreen	Efface l'écran de la dernière panne stocké en mémoire.

Synopsis

```
racadm clearasrscreen
```

Interfaces prises en charge

- RACADM locale
- RACADM distant
- RACADM telnet/ssh/série

---

config

REMARQUE : Pour utiliser la commande **getconfig**, vous devez disposer de l'autorisation **Ouvrir une session sur l'iDRAC**.

Le Tableau A-4 décrit les sous-commandes **config** et **getconfig**.

Tableau A-4. config / getconfig

Sous-commande	Définition
config	Configure l'iDRAC6.
getconfig	Récupère les données de configuration iDRAC6.

Synopsis

```
racadm config [-c|-p] -f <nom de fichier>

racadm config -g <nom du groupe> -o <nom de l'objet> [-i <index>] <Valeur>
```

Interfaces prises en charge

- RACADM locale
- RACADM distant
- RACADM telnet/ssh/série

Description

La sous-commande **config** permet à l'utilisateur de définir les paramètres de configuration iDRAC6 individuellement ou de les regrouper dans un fichier de configuration. Si les données sont différentes, cet objet iDRAC6 est écrit avec la nouvelle valeur.

Entrée

Le Tableau A-5 décrit les options de la sous-commande **config**.

REMARQUE : Les options **-f** et **-p** ne sont pas prises en charge pour la console série/telnet/ssh.

Tableau A-5. Options et descriptions de la sous-commande config

Option	Description
-f	L'option **-f <*nom de fichier*>** force **config** à lire le contenu du fichier **<*nom de fichier*>** et à configurer l'iDRAC6. Le fichier doit contenir des données au format spécifié dans « Règles d'analyse ».
-p	L'option de mot de passe, **-p**, indique à **config** de supprimer les entrées de mots de passe contenues dans le fichier de configuration **-f <*nom de fichier*>** une fois la configuration terminée.
-g	L'option de groupe, **-g <*nom du groupe*>**, doit être utilisée avec l'option **-o**. Le <*nom du groupe*> spécifie le groupe contenant l'objet à définir.
-o	L'option d'objet, **-o <*nom de l'objet*> <*Valeur*>**, doit être utilisée avec l'option **-g**. Cette option spécifie le nom d'objet écrit avec la chaîne <*valeur*>.
-i	L'option d'index, **-i <*index*>,** n'est valide que pour les groupes indexés et peut être utilisée pour spécifier un groupe unique. L'<*index*> est un entier décimal compris entre 1 et 16. L'index est spécifié ici par la valeur de l'index et non pas par une valeur « nommée ».
-c	L'option de vérification, **-c**, est utilisée avec la sous-commande **config** et permet à l'utilisateur d'analyser le fichier **.cfg** afin de trouver les erreurs de syntaxe. Si des erreurs sont trouvées, le numéro de la ligne et une brève description de tout ce qui est inexact sont affichés. Il n'y a pas d'écritures sur l'iDRAC6. Cette option sert uniquement de vérification.

Résultat

Cette sous-commande crée une sortie d'erreur après avoir trouvé l'une des erreurs suivantes :

- Syntaxe, nom du groupe, nom de l'objet ou index non valide, ou autres éléments non valides de la base de données
- Échecs de la CLI RACADM

Cette sous-commande renvoie une indication du nombre d'objets de configuration écrits par rapport au nombre total d'objets du fichier **.cfg**.

Exemples

- `racadm config -g cfgLanNetworking -o cfgNicIpAddress 10.35.10.100`

Définit le paramètre de configuration (objet) **cfgNicIpAddress** sur la valeur 10.35.10.110. Cet objet d'adresse IP est contenu dans le groupe **cfgLanNetworking**.

- `racadm config -f myrac.cfg`

  Configure ou reconfigure l'iDRAC6. Le fichier **myrac.cfg** peut être créé à partir de la commande **getconfig**. Le fichier **myrac.cfg** peut être aussi modifié manuellement tant que les règles d'analyse sont suivies.

  REMARQUE : Le fichier **myrac.cfg** ne contient pas d'informations sur les mots de passe. Ces informations doivent être saisies manuellement pour pouvoir être incluses dans le fichier. Si vous souhaitez supprimer les informations sur les mots de passe du fichier **myrac.cfg** lors de la configuration, utilisez l'option **-p**.

---

getconfig

Description de la sous-commande getconfig

La sous-commande **getconfig** permet à l'utilisateur d'extraire les paramètres de configuration iDRAC6 un par un ou d'extraire et d'enregistrer dans un fichier l'ensemble des groupes de configuration iDRAC6.

Entrée

Le Tableau A-6 décrit les options de la sous-commande **getconfig**.

REMARQUE : L'option **-f** sans spécification de fichier affiche le contenu du fichier sur l'écran du terminal.

Tableau A-6. Options de la sous-commande getconfig

Option	Description
-f	L'option **-f <*nom de fichier*>** indique à getconfig d'écrire toute la configuration iDRAC6 dans un fichier de configuration. Ce fichier peut être utilisé pour les opérations de configuration par lot à l'aide de la sous-commande **config**. **REMARQUE :** L'option **-f** ne crée pas d'entrées pour les groupes **cfgIpmiPet** et **cfgIpmiPef**. Vous devez définir au moins une destination d'interruption pour capturer le groupe **cfgIpmiPet** dans le fichier.
-g	L'option de groupe, **-g <*nom du groupe*>**, **permet** d'afficher la configuration d'un groupe unique. Le **nom du groupe** est le nom du groupe utilisé dans les fichiers **racadm.cfg**. Si le groupe est indexé, l'option **-i** doit être utilisée.
-h	L'option d'**aide**, **-h**, affiche la liste de tous les groupes de configuration disponibles que vous pouvez utiliser. Cette option est utile si vous ne vous souvenez plus des noms exacts des groupes.
-i	L'option d'**index**, **-i <*index*>**, n'est valide que pour les groupes indexés et peut être utilisée pour spécifier un groupe unique. L'<*index*> est un entier décimal compris entre 1 et 16. Si **-i <*index*>** n'est pas spécifié, la valeur 1 est supposée pour les groupes, qui sont des tableaux à entrées multiples. L'index est spécifié ici par la valeur de l'index et non pas par une valeur « nommée ».
-o	L'option d'objet, -o **<*nom de l'objet*>**, spécifie le nom d'objet qui est utilisé dans la requête. Cette option est optionnelle et peut être utilisée avec l'option -g.
-u	L'option de **nom d'utilisateur**, **-u <*nom d'utilisateur*>**, permet d'afficher la configuration de l'utilisateur spécifié. L'option **<*nom d'utilisateur*>** est le nom d'ouverture de session de l'utilisateur.
-v	L'option **-v** affiche des détails supplémentaires avec l'affichage des propriétés et est utilisée avec l'option **-g**.

Résultat

Cette sous-commande crée une sortie d'erreur après avoir trouvé une des erreurs suivantes :

- Syntaxe, nom du groupe, nom de l'objet, index non valides, ou d'autres éléments non valides de la base de données
- Échecs de transport de l'interface de ligne de commande RACADM

Si aucune erreur n'a été trouvée, cette sous-commande affiche le contenu de la configuration indiquée.

Exemples

- `racadm getconfig -g cfgLanNetworking`

  Affiche toutes les propriétés de configuration (objets) qui sont contenues dans le groupe **cfgLanNetworking**.

- `racadm getconfig –f myrac.cfg`

  Enregistre tous les objets de configuration de groupe iDRAC6 sur **myrac.cfg**.

- `racadm getconfig -h`

  Affiche la liste des groupes de configuration disponibles sur l'iDRAC6.

- `racadm getconfig -u root`

  Affiche les propriétés de configuration de l'utilisateur appelé root.

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

  Affiche l'instance de groupe d'utilisateurs dans l'index 2 avec des informations claires sur les valeurs de propriétés.

Synopsis

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

racadm getconfig -g <nom du groupe> [-i <index>]

racadm getconfig -u <nom d'utilisateur>

racadm getconfig -h
```

Interfaces prises en charge

- RACADM locale
- RACADM distant
- RACADM telnet/ssh/série

---

coredump

REMARQUE : Pour utiliser cette commande, vous devez avoir le droit **Exécuter des commandes de débogage**.

Le Tableau A-7 décrit la sous-commande **coredump**.

Tableau A-7. coredump

Sous-commande	Définition
coredump	Affiche le dernier vidage de mémoire de l'iDRAC6.

Synopsis

```
racadm coredump
```

Description

La sous-commande **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 de l'iDRAC6 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-là, les informations coredump portent sur la dernière erreur critique qui s'est produite.

Reportez-vous à la sous-commande **coredumpdelete** pour plus d'informations sur l'effacement de **coredump**.

Interfaces prises en charge

- RACADM distant
- RACADM telnet/ssh/série

---

coredumpdelete

REMARQUE : Pour utiliser cette commande, vous devez avoir le droit **Effacer les journaux** ou **Exécuter les commandes de débogage**.

Le Tableau A-8 décrit la sous-commande **coredumpdelete**.

Tableau A-8. coredumpdelete

Sous-commande	Définition
coredumpdelete	Supprime le vidage de mémoire stocké sur l'iDRAC6.

Synopsis

```
racadm coredumpdelete
```

Description

La sous-commande **coredumpdelete** peut être utilisée pour effacer toutes les données **coredump** actuellement stockées dans le RAC.

REMARQUE : Si une commande **coredumpdelete** est émise et qu'aucune donnée coredump n'est actuellement stockée dans le RAC, la commande affiche un message de réussite. Ce comportement est prévu.

Reportez-vous à la sous-commande **coredump** pour plus d'informations sur l'affichage d'une donnée coredump.

Interfaces prises en charge

- RACADM locale
- RACADM distant
- RACADM telnet/ssh/série

---

fwupdate

REMARQUE : Pour utiliser cette commande, vous devez disposer de l'autorisation **Configurer l'iDRAC6**.

REMARQUE : Avant de commencer la mise à jour de votre micrologiciel, voir « Configuration avancée d'iDRAC6 » pour des instructions supplémentaires.

Le Tableau A-9 décrit la sous-commande **fwupdate**.

Tableau A-9. fwupdate

Sous-commande	Définition
fwupdate	Met à jour le micrologiciel de l'iDRAC6.

Synopsis

```
racadm fwupdate -s

racadm fwupdate -g -u -a <Adresse_IP_du_serveur_TFTP> [-d <chemin d'accès>]

racadm fwupdate -p -u -d <chemin d'accès>

racadm fwupdate -r
```

Description

La sous-commande **fwupdate** permet aux utilisateurs de mettre à jour le micrologiciel de l'iDRAC6. L'utilisateur peut :

- Vérifier l'état du processus de mise à jour du micrologiciel
- Mettre à jour le micrologiciel de l'iDRAC6 à partir d'un serveur TFTP en fournissant une adresse IP et un chemin d'accès optionnel
- Mettre à jour le micrologiciel de l'iDRAC6 à partir du système de fichiers local à l'aide de la RACADM locale
- Restaurer le micrologiciel auxiliaire

Interfaces prises en charge

- RACADM locale
- RACADM distant
- RACADM telnet/ssh/série

Entrée

Le Tableau A-10 décrit les options de la sous-commande **fwupdate**.

REMARQUE : L'option **-p** est uniquement prise en charge dans la RACADM locale et pas avec la console série/telnet/ssh ou à distance. L'option **-p** n'est pas non plus prise en charge sur les systèmes d'exploitation Linux.

Tableau A-10. Options de la sous-commande fwupdate

Option	Description
-u	L'option **update** effectue une somme de contrôle sur le fichier de mise à jour du micrologiciel et démarre le processus de mise à jour réel. Cette option peut être utilisée avec les options **-g** ou **-p**. À la fin de la mise à jour, l'iDRAC6 effectue une réinitialisation logicielle.
-s	L'option **status** renvoie l'état actuel du processus de mise à jour. Cette option est toujours utilisée seule.
-g	L'option **get** donne l'ordre au micrologiciel de recevoir le fichier de mise à jour de micrologiciel à partir du serveur TFTP. L'utilisateur doit aussi spécifier les options **-a** et **-d**. En l'absence de l'option **-a**, les valeurs par défaut sont lues dans les propriétés **cfgRhostsFwUpdateIpAddr** et **cfgRhostsFwUpdatePath** du groupe **cfgRemoteHosts**.
-a	L'option **Adresse IP** spécifie l'adresse IP du serveur TFTP.
-d	L'option de **répertoire**, **-d**, spécifie le répertoire où se trouve le fichier de mise à jour de micrologiciel, sur le serveur TFTP ou sur le serveur hôte de l'iDRAC6.
-p	L'option **-p**, ou **put**, est utilisée pour mettre à jour le fichier de micrologiciel du système géré vers l'iDRAC6. L'option **-u** doit être utilisée avec l'option **-p**.
-r	L'option **restaurer** est utilisée pour restaurer le micrologiciel auxiliaire.

Résultat

Affiche un message indiquant quelle opération est en train d'être effectuée.

Exemples

- `racadm fwupdate -g -u - a 143.166.154.143 -d <chemin d'accès>`

  Dans cet exemple, l'option **-g** indique au micrologiciel qu'il faut télécharger le fichier de mise à jour du micrologiciel d'un emplacement (spécifié par l'option **-d**) du serveur TFTP à une adresse IP spécifique (spécifiée par l'option **-a**). Lorsque le fichier image a été téléchargé à partir du serveur TFTP, le processus de mise à jour commence. Une fois terminé, l'iDRAC6 est réinitialisé.

- `racadm fwupdate -s`

  Cette option lit l'état actuel de la mise à jour du micrologiciel.

- `racadm fwupdate -p -u -d <chemin d'accès>`

  Dans cet exemple, l'image de micrologiciel pour la mise à jour est fournie par le système de fichiers de l'hôte.

REMARQUE : L'option **-p** n'est pas prise en charge dans l'interface RACADM distante pour la sous-commande fwupdate. La mise à jour du micrologiciel d'interface RACADM distante via le chemin local n'est pas prise en charge sur les systèmes d'exploitation Linux.

---

getssninfo

REMARQUE : Pour utiliser cette commande, vous devez disposer de l'autorisation **Ouvrir une session sur l'iDRAC**.

Le Tableau A-11 décrit la sous-commande **getssninfo**.

Tableau A-11. Sous-commande getssninfo

Sous-commande	Définition
getssninfo	Récupère les informations de session d'une ou de plusieurs sessions actives ou en attente dans le tableau de session du gestionnaire de session.

Synopsis

```
racadm getssninfo [-A] [-u <nom d'utilisateur> | *]
```

Description

La commande **getssninfo** renvoie la liste des utilisateurs connectés à l'iDRAC6. Le résumé fournit les informations suivantes :

- Le nom d'utilisateur
- L'adresse IP (si applicable)
- Le type de session (par exemple, série ou telnet)
- Les consoles utilisées (par exemple, média virtuel ou KVM virtuel)

Interfaces prises en charge

- RACADM locale
- RACADM distant
- RACADM telnet/ssh/série

Entrée

Le Tableau A-12 décrit les options de la sous-commande **getssninfo**.

Tableau A-12. Options de la sous-commande getssninfo

Option	Description
-A	L'option **-A** élimine l'impression des en-têtes de données.
-u	Avec l'option de nom d'utilisateur, **-u <nom d'utilisateur>**, la sortie imprimée ne contient que les enregistrements de session détaillés concernant le nom d'utilisateur donné. Si un symbole « * » est donné en tant que nom d'utilisateur, tous les utilisateurs sont répertoriés. Le résumé des informations n'est pas imprimé si cette option est spécifiée.

Exemples

- `racadm getssninfo`

Tableau A-13 fournit un exemple de sortie de la commande **racadm getssninfo**.

Tableau A-13. Exemple de sortie de la sous-commande getssninfo

Utilisateur	Adresse IP	Type	Consoles
root	192.168.0.10	Telnet	KVM virtuel

- `racadm getssninfo -A`

  `"root" "143.166.174.19" "Telnet" "NONE"("AUCUN")`

- `racadm getssninfo -A -u *`

  `"root" "143.166.174.19" "Telnet" "AUCUN"`

```
"bob" "143.166.174.19" "GUI" "AUCUN"
```

---

getsysinfo

REMARQUE : Pour utiliser cette commande, vous devez disposer de l'autorisation **Ouvrir une session sur l'iDRAC**.

Le Tableau A-14 décrit la sous-commande **racadm getsysinfo**.

Tableau A-14. getsysinfo

Commande	Définition
getsysinfo	Affiche des informations sur l'iDRAC6, sur le système et sur l'état de surveillance.

Synopsis

```
racadm getsysinfo [-d] [-s] [-w] [-A] [-c] [-4] [-6] [-r]
```

Description

La sous-commande **getsysinfo** affiche des informations relatives au RAC, au système géré et à la configuration de la surveillance.

Interfaces prises en charge

- RACADM locale
- RACADM distant
- RACADM telnet/ssh/série

Entrée

Le Tableau A-15 décrit les options de la sous-commande **getsysinfo**.

Tableau A-15. Options de la sous-commande getsysinfo

Option	Description
-4	Affiche les paramètres IPv4
-6	Affiche les paramètres IPv6
-c	Affiche les paramètres communs
-d	Affiche les informations iDRAC6.
-s	Affiche les informations sur le système
w	Affiche les informations sur la surveillance
-A	Élimine l'impression des en-têtes/noms.

Si l'option **-w** n'est pas spécifiée, les autres options sont utilisées par défaut.

Résultat

La sous-commande **getsysinfo** affiche des informations relatives au RAC, au système géré et à la configuration de la surveillance.

Exemple de sortie

```
RAC Information:
RAC Date/Time = 10/01/2008 09:39:53
Firmware Version = 0.32
Firmware Build = 55729
Last Firmware Update = 09/25/2008 18:08:31
```

```
Hardware Version = 0.01
MAC Address = 00:1e:c9:b2:c7:1f

Common settings:
Register DNS RAC Name = 0
DNS RAC Name = iDRAC6
Current DNS Domain =
Domain Name from DHCP = 0

IPv4 settings:
Enabled = 1
Current IP Address = 192.168.0.120
Current IP Gateway = 192.168.0.1
Current IP Netmask = 255.255.255.0
DHCP Enabled = 0
Current DNS Server 1 = 0.0.0.0
Current DNS Server 2 = 0.0.0.0
DNS Servers from DHCP = 0

IPv6 settings:
Enabled = 0
Current IP Address 1 = 2002:0000:0000::0001
Current IP Gateway = ::
Prefix Length = 64
Autoconfig              = 1
DNS Server from DHCPv6  = 0
Current DNS Server 1    = ::
Current DNS Server 2    = ::

System Information:
System Model = PowerEdge R610
System BIOS Version = 0.2.4
BMC Firmware Version = 0.32
Service Tag = AC056
Host Name =
OS Name =
Power Status = ON

Watchdog Information:
Recovery Action = None
Present countdown value = 15 seconds
Initial countdown value = 15 seconds
```

Exemples

- `racadm getsysinfo -A -s`

  `"System Information:" "PowerEdge 2900" "A08" "1.0" "EF23VQ-0023" "Hostname"`

  `"Microsoft Windows 2000 version 5.0, Build Number 2195, Service Pack 2" "ON"`

- `racadm getsysinfo -w -s`

```
System Information:
System Model             = PowerEdge 2900
System BIOS Version      = 0.2.3
BMC Firmware Version     = 0.17
Service Tag              = 48192
Host Name                = racdev103
OS Name                  = Microsoft Windows Server 2003
Power Status            = OFF


Watchdog Information:
Recovery Action          = None
Present countdown value  = 0 seconds
Initial countdown value = 0 seconds
```

Restrictions

Les champs Nom de l'hôte et Nom du système d'exploitation dans la sortie **getsysinfo** affichent des informations exactes seulement si le logiciel système Dell™ OpenManage™ est installé sur le système géré. Si OpenManage n'est pas installé sur le système géré, ces champs peuvent être vides ou inexacts.

---

getractime

REMARQUE : Pour utiliser cette commande, vous devez disposer de l'autorisation **Ouvrir une session sur l'iDRAC**.

Le Tableau A-16 décrit la sous-commande **getractime**.

Tableau A-16. getractime

Sous-commande	Définition
getractime	Affiche l'heure actuelle à partir du contrôleur RAC.

Synopsis

```
racadm getractime [-d]
```

Description

Sans options, la sous-commande **getractime** affiche l'heure dans un format lisible commun.

Avec l'option **-d**, **getractime** affiche la date dans un format, *aaaammjjhhmmss.mmmmmms*, qui est le même format renvoyé par la commande **date** d'UNIX.

Résultat

La sous-commande **getractime** affiche la sortie sur une ligne.

Exemple de sortie

```
racadm getractime

Thu Dec 8 20:15:26 2005

racadm getractime -d

20051208201542.000000
```

Interfaces prises en charge

- RACADM locale
- RACADM distant
- RACADM telnet/ssh/série

---

ifconfig

REMARQUE : Pour utiliser cette commande, vous devez disposer de l'autorisation **Exécution des commandes de diagnostic** ou **Configurer l'iDRAC**.

Le Tableau A-17 décrit la sous-commande **ifconfig**.

Tableau A-17. ifconfig

Sous-commande	Définition
ifconfig	Affiche le contenu de la table d'interface réseau.

Synopsis

```
racadm ifconfig
```

---

netstat

REMARQUE : Pour utiliser cette commande, vous devez avoir le droit **Exécuter des commandes de diagnostic**.

Le Tableau A-18 décrit la sous-commande **netstat**.

Tableau A-18. netstat

Sous-commande	Définition
netstat	Affiche la table de routage et les connexions actuelles.

Synopsis

```
racadm netstat
```

Interfaces prises en charge

- RACADM distant
- RACADM telnet/ssh/série

---

ping

REMARQUE : Pour utiliser cette commande, vous devez disposer de l'autorisation **Exécution des commandes de diagnostic** ou **Configurer l'iDRAC**.

Le Tableau A-19 décrit la sous-commande **ping**.

Tableau A-19. ping

Sous-commande	Définition
ping	Vérifie que l'adresse IP de destination est accessible à partir de l'iDRAC6 avec le contenu actuel du tableau de routage. Une adresse IP de destination est nécessaire. Un paquet d'écho ICMP est envoyé à l'adresse IP de destination en fonction du contenu actuel de la table de routage.

Synopsis

```
racadm ping <adresse IP>
```

Interfaces prises en charge

- RACADM distant
- RACADM telnet/ssh/série

---

setniccfg

REMARQUE : Pour utiliser cette commande, vous devez disposer de l'autorisation **Configurer l'iDRAC**.

Le Tableau A-20 décrit la sous-commande **setniccfg**.

Tableau A-20. setniccfg

Sous-commande	Définition
setniccfg	Définit la configuration IP du contrôleur.

REMARQUE : Les termes NIC et port de gestion Ethernet peuvent être interchangés.

Synopsis

```
racadm setniccfg -d

racadm setniccfg -d6

racadm setniccfg -s <adresseIPv4> <masque de réseau> <passerelle IPV4>

racadm setniccfg -s6 <adresse IPv6> <longueur du préfixe IPv6> <passerelle IPv6>

racadm setniccfg -o
```

Description

La sous-commande **setniccfg** définit l'adresse IP du contrôleur.

- L'option **-d** active le protocole DHCP pour le port de gestion Ethernet (la valeur par défaut est DHCP désactivé).
- L'option **-d6** active AutoConfig pour le port de gestion Ethernet. Il est activé par défaut.
- L'option **-s** active les paramètres IP statiques. L'adresse IPv4, le masque de réseau et la passerelle peuvent être spécifiés. Sinon, les paramètres statiques existants sont utilisés. <*adresse IPv4*>, <*masque de réseau*>, et <*passerelle*> doivent être tapés sous forme de chaînes séparées par des points.
- L'option **-s6** active les paramètres IPv6 statiques. L'adresse IPv6, la longueur du préfixe et la passerelle IPv6 peuvent être spécifiés.
- L'option **-o** désactive le port de gestion Ethernet complètement.

Résultat

La sous-commande **setniccfg** affiche un message d'erreur approprié si l'opération a échoué. En cas de succès, un message est affiché.

Interfaces prises en charge

- RACADM locale
- RACADM distant
- RACADM telnet/ssh/série

---

getniccfg

REMARQUE : Pour utiliser cette commande, vous devez disposer de l'autorisation **Ouvrir une session sur l'iDRAC**.

Le Tableau A-21 décrit les sous-commandes **setniccfg** et **getniccfg**.

Tableau A-21. setniccfg / getniccfg

Sous-commande	Définition
getniccfg	Affiche la configuration IP actuelle du contrôleur.

Synopsis

```
racadm getniccfg
```

Description

La sous-commande **getniccfg** affiche les paramètres actuels du port de gestion Ethernet.

Exemple de sortie

La sous-commande **getniccfg** affiche un message d'erreur approprié si l'opération a échoué. Sinon, en cas de réussite, le résultat est affiché au format suivant :

```
NIC Enabled     = 1
```

```
DHCP Enabled    = 1

IP Address      = 192.168.0.1

Subnet Mask     = 255.255.255.0

Gateway         = 192.168.0.1
```

Interfaces prises en charge

- RACADM locale
- RACADM distant
- RACADM telnet/ssh/série

---

getsvctag

REMARQUE : Pour utiliser cette commande, vous devez disposer de l'autorisation **Ouvrir une session sur l'iDRAC**.

Le Tableau A-22 décrit la sous-commande **getsvctag**.

Tableau A-22. getsvctag

Sous-commande	Définition
getsvctag	Affiche un numéro de service.

Synopsis

```
racadm getsvctag
```

Description

La sous-commande **getsvctag** affiche le numéro de service du système hôte.

Exemple

Tapez `getsvctag` à l'invite de commande. La sortie s'affiche de la façon suivante :

```
Y76TP0G
```

La commande renvoie `0` en cas de réussite et des valeurs autres que zéro en cas d'erreur.

Interfaces prises en charge

- RACADM locale
- RACADM distant
- RACADM telnet/ssh/série

---

racdump

REMARQUE : Pour utiliser cette commande, vous devez avoir le droit **Déboguer**.

Le Tableau A-23 décrit la sous-commande **racdump**.

Tableau A-23. racdump

Sous-commande	Définition
racdump	Affiche des informations générales et d'état concernant l'iDRAC6.

Synopsis

```
racadm racdump
```

Description

La sous-commande **racdump** utilise une seule commande pour obtenir les informations sur le vidage et l'état, ou des informations générales sur une carte iDRAC6.

Les informations suivantes sont affichées lorsque la sous-commande **racdump** est traitée :

- Informations générales sur le système/sur le RAC
- Coredump
- Informations sur les sessions
- Informations sur le traitement
- Informations sur le build de micrologiciel

Interfaces prises en charge

- RACADM distant
- RACADM telnet/ssh/série

---

racreset

REMARQUE : Pour utiliser cette commande, vous devez disposer de l'autorisation **Configurer l'iDRAC**.

Le Tableau A-24 décrit la sous-commande **racreset**.

Tableau A-24. racreset

Sous-commande	Définition
racreset	Réinitialise l'iDRAC6.

REMARQUE : Lorsque vous émettez une sous-commande racreset, il faut jusqu'à une minute à l'iDRAC6 pour revenir à un état utilisable.

Synopsis

```
racadm racreset [hard | soft]
```

Description

La sous-commande **racreset** envoie une réinitialisation à l'iDRAC6. L'événement de réinitialisation est écrit dans le journal iDRAC6.

Une réinitialisation matérielle effectue une opération de réinitialisation approfondie sur le RAC. Une réinitialisation matérielle doit uniquement avoir lieu en dernier recours pour récupérer le RAC.

REMARQUE : Vous devez redémarrer votre système après avoir effectué une réinitialisation matérielle de l'iDRAC6 comme décrit dans Tableau A-25.

Le Tableau A-25 décrit les options de la sous-commande **racreset**.

Tableau A-25. Options de la sous-commande racreset

Option	Description

hard	Une réinitialisation *matérielle* effectue une opération de réinitialisation approfondie sur le contrôleur RAC. Une réinitialisation matérielle doit uniquement avoir lieu en dernier recours pour réinitialiser le contrôleur iDRAC6 à des fins de récupération.
soft	Une réinitialisation *logicielle* effectue une opération de redémarrage normale sur le RAC.

Exemples

- `racadm racreset`

  Démarre la séquence de réinitialisation logicielle de l'iDRAC6.

- `racadm racreset hard`

  Démarre la séquence de réinitialisation matérielle de l'iDRAC6.

Interfaces prises en charge

- RACADM locale
- RACADM distant
- RACADM telnet/ssh/série

---

racresetcfg

REMARQUE : Pour utiliser cette commande, vous devez disposer de l'autorisation **Configurer l'iDRAC**.

Le Tableau A-26 décrit la sous-commande **racresetcfg**.

Tableau A-26. racresetcfg

Sous-commande	Définition
racresetcfg	Réinitialise les valeurs d'usine par défaut de toute la configuration de l'iDRAC6.

Synopsis

```
racadm racresetcfg
```

Interfaces prises en charge

- RACADM locale
- RACADM distant
- RACADM telnet/ssh/série

Description

La commande **racresetcfg** supprime toutes les entrées de propriétés de la base de données configurées par l'utilisateur. La base de données a des propriétés par défaut pour toutes les entrées utilisées pour restaurer les paramètres par défaut d'origine du contrôleur. Après avoir réinitialisé les propriétés de la base de données, l'iDRAC6 se réinitialise automatiquement.

REMARQUE : Cette commande supprime votre configuration iDRAC6 actuelle et réinitialise les paramètres par défaut d'origine de la configuration iDRAC6 et de la configuration série. Après la réinitialisation, le nom d'utilisateur et le mot de passe par défaut sont **root** et **calvin**, respectivement, et l'adresse IP est 192.168.0.120. Si vous émettez une commande **racresetcfg** à partir d'un client réseau (par exemple, un navigateur Web pris en charge, telnet/ssh ou la RACADM distante), vous devez utiliser l'adresse IP par défaut.

REMARQUE : Certains processus de micrologiciel de l'iDRAC6 doivent être arrêtés et redémarrés pour terminer la réinitialisation des paramètres par défaut. L'iDRAC6 ne répond pas pendant environ 30 secondes pendant que cette opération se termine.

---

serveraction

REMARQUE : Pour utiliser cette commande, vous devez avoir le droit **Exécuter des commandes de contrôle du serveur**.

Le Tableau A-27 décrit la sous-commande **serveraction**.

Tableau A-27. serveraction

Sous-commande	Définition
serveraction	Exécute une réinitialisation ou une mise sous et hors tension et un cycle du système géré.

Synopsis

```
racadm serveraction <action>
```

Description

La sous-commande serveraction permet aux utilisateurs d'effectuer des opérations de gestion de l'alimentation sur le système hôte. Le Tableau A-28 décrit les options de contrôle de l'alimentation **serveraction**.

Tableau A-28. Options de la sous-commande serveraction

Chaîne	Définition
<*action***>**	Spécifie l'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 semblable à une pression sur le bouton d'alimentation situé sur le panneau avant du système pour mettre hors tension, puis sous tension le 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.

Résultat

La sous-commande **serveraction** affiche un message d'erreur si l'opération demandée n'a pas pu être effectuée ou un message de réussite si l'opération s'est terminée avec succès.

Interfaces prises en charge

- RACADM locale
- RACADM distant
- RACADM telnet/ssh/série

---

getraclog

REMARQUE : Pour utiliser cette commande, vous devez disposer de l'autorisation **Ouvrir une session sur l'iDRAC**.

Le Tableau A-29 décrit la commande **racadm getraclog**.

Tableau A-29. getraclog

Commande	Définition
getraclog -i	Affiche le nombre d'entrées présentes dans le journal iDRAC6.
getraclog	Affiche les entrées du journal iDRAC6.

Synopsis

```
racadm getraclog -i

racadm getraclog [-A] [-o] [-c nombre] [-s démarrer-l'enregistrement] [-m]
```

Description

La commande **getraclog -i** affiche le nombre d'entrées du journal iDRAC6.

Les options suivantes permettent à la commande **getraclog** de lire les entrées :

- **-A** : affiche la sortie sans en-tête ou nom.
- **-c** : fournit le nombre maximum d'entrées à renvoyer.
- **-m** : affiche un écran d'informations à la fois et invite l'utilisateur à continuer (semblable à la commande **more** d'UNIX).
- **-o** : affiche la sortie sur une seule ligne.
- **-s** : spécifie l'enregistrement de démarrage utilisé pour l'affichage

REMARQUE : Si aucune option n'est fournie, tout le journal est affiché.

Résultat

L'affichage par défaut de la sortie indique le numéro d'enregistrement, l'horodatage, la source et la description. L'horodatage commence à minuit, le 1er janvier, et augmente jusqu'à ce que le système démarre. Après le démarrage du système, l'horodatage du système est utilisé.

Exemple de sortie

```
Record:       1
Date/Time:    Dec 8 08:10:11
Source:       login[433]
Description:  root login from 143.166.157.103
```

Interfaces prises en charge

- RACADM locale
- RACADM distant
- RACADM telnet/ssh/série

---

clrraclog

REMARQUE : Pour utiliser cette commande, vous devez avoir le droit **Effacer les journaux**.

Synopsis

```
racadm clrraclog
```

Description

La sous-commande **clrraclog** supprime tous les enregistrements existants du journal iDRAC6. Un nouvel enregistrement est créé pour enregistrer la date et l'heure auxquelles le journal a été effacé.

---

getsel

REMARQUE : Pour utiliser cette commande, vous devez disposer de l'autorisation **Ouvrir une session sur l'iDRAC**.

Le Tableau A-30 décrit la commande **getsel**.

Tableau A-30. getsel

Commande	Définition
getsel -i	Affiche le nombre d'entrées du journal des événements système.

getsel	Affiche les entrées du journal SEL.

Synopsis

```
racadm getsel -i
```

```
racadm getsel [-E] [-R] [-A] [-o] [-c nombre] [-s nombre] [-m]
```

Description

La commande **getsel -i** affiche le nombre d'entrées du journal SEL.

Les options **getsel** suivantes (sans l'option **-i**) servent à lire les entrées.

-A : spécifie la sortie sans affichage d'en-tête ou de nom.

-c : fournit le nombre maximum d'entrées à renvoyer.

-o : affiche la sortie sur une seule ligne.

-s : spécifie l'enregistrement de démarrage utilisé pour l'affichage

-E : place les 16 octets du journal SEL brut à la fin de chaque ligne de sortie sous forme de séquence de valeurs hexadécimales.

-R : seules les données brutes sont imprimées.

-m : affiche un écran à la fois et invite l'utilisateur à continuer (semblable à la commande **more** d'UNIX).

REMARQUE : Si aucun argument n'est spécifié, tout le journal est affiché.

Résultat

L'affichage de la sortie par défaut indique le numéro d'enregistrement, l'horodatage, la gravité et la description.

Par exemple :

```
Record:      1
Date/Time:   11/16/2005 22:40:43
Severity:    Ok
Description: System Board SEL: event log sensor for System Board, log cleared was asserted
```

Interfaces prises en charge

- RACADM locale
- RACADM distant
- RACADM telnet/ssh/série

---

clrsel

REMARQUE : Pour utiliser cette commande, vous devez avoir le droit **Effacer les journaux**.

Synopsis

```
racadm clrsel
```

Description

La commande **clrsel** supprime tous les enregistrements existants du journal des événements système (SEL).

Interfaces prises en charge

- RACADM locale

- RACADM distant
- RACADM telnet/ssh/série

---

gettracelog

REMARQUE : Pour utiliser cette commande, vous devez disposer de l'autorisation **Ouvrir une session sur l'iDRAC**.

Le Tableau A-31 décrit la sous-commande **gettracelog**.

Tableau A-31. gettracelog

Commande	Définition
gettracelog -i	Affiche le nombre d'entrées du journal de suivi de l'iDRAC6.
gettracelog	Affiche le journal de suivi de l'iDRAC6.

Synopsis

```
racadm gettracelog -i

racadm gettracelog [-A] [-o] [-c nombre] [-s démarrer l'enregistrement] [-m]
```

Description

La commande **gettracelog** (sans l'option **-i**) sert à lire les entrées. Les entrées **gettracelog** suivantes sont utilisées pour lire les entrées :

-i : Affiche le nombre d'entrées du journal de suivi de l'iDRAC6.

-m : affiche un écran à la fois et invite l'utilisateur à continuer (semblable à la commande **more** d'UNIX).

-o : affiche la sortie sur une seule ligne.

-c : spécifie le nombre d'enregistrements à afficher

-s : spécifie l'enregistrement de démarrage à afficher

-A : n'affiche pas d'en-tête ou d'étiquette

Résultat

L'affichage par défaut de la sortie indique le numéro d'enregistrement, l'horodatage, la source et la description. L'horodatage commence à minuit, le 1er janvier, et augmente jusqu'à ce que le système démarre. Après le démarrage du système, l'horodatage du système est utilisé.

Par exemple :

```
Record: 1

Date/Time: Dec 8 08:21:30

Source: ssnmgrd[175]

Description: root from 143.166.157.103: session timeout sid 0be0aef4
```

Interfaces prises en charge

- RACADM locale
- RACADM distant
- RACADM telnet/ssh/série

---

sslcsrgen

REMARQUE : Pour utiliser cette commande, vous devez disposer de l'autorisation **Configurer l'iDRAC**.

Le Tableau A-32 décrit la sous-commande **sslcsrgen**.

Tableau A-32. sslcsrgen

Sous-commande	Description
sslcsrgen	Génère et télécharge une requête de signature de certificat (CSR) SSL à partir du RAC.

Synopsis

```
racadm sslcsrgen [-g] [-f <nom de fichier>]

racadm sslcsrgen -s
```

Description

La sous-commande **sslcsrgen** peut être utilisée pour générer une CSR et télécharger le fichier dans le système de fichiers local du client. La CSR peut être utilisée pour créer un certificat SSL personnalisé qui peut être utilisé pour les transactions SSL sur le RAC.

Options

REMARQUE : L'option **-f** n'est pas prise en charge pour la console série/telnet/ssh.

Le Tableau A-33 décrit les options de la sous-commande **sslcsrgen**.

Tableau A-33. Options de la sous-commande sslcsrgen

Option	Description
-g	Crée une nouvelle CSR.
-s	Renvoie l'état du processus de création d'une CSR (génération en cours, active ou aucune).
-f	Spécifie le nom de fichier de l'emplacement, *<nom de fichier>*, où la CSR sera téléchargée.

REMARQUE : Si l'option **-f** n'est pas spécifiée, le nom de fichier sera **sslcsr** par défaut dans votre répertoire actuel.

Si aucune option n'est spécifiée, une CSR est générée et téléchargée dans le système de fichiers local comme **sslcsr** par défaut. L'option **-g** ne peut pas être utilisée avec l'option **-s** et l'option **-f** peut seulement être utilisée avec l'option **-g**.

La sous-commande **sslcsrgen -s** renvoie un des codes d'état suivants :

- La CSR a été générée avec succès.
- La CSR n'existe pas.
- La création d'une CSR est en cours.

Restrictions

La sous-commande **sslcsrgen** peut seulement être exécutée à partir d'un client de la RACADM locale ou distante et ne peut pas être utilisée dans l'interface série, telnet ou SSH.

REMARQUE : Avant de pouvoir générer une CSR, les champs de la CSR doivent être configurés dans le groupe **cfgRacSecurity** RACADM. Par exemple : racadm config-g cfgRacSecurity-o cfgRacSecCsrCommonName MyCompany

Exemples

```
racadm sslcsrgen -s

ou

racadm sslcsrgen -g -f c:\csr\csrtest.txt
```

Interfaces prises en charge

- RACADM locale
- RACADM distant
- RACADM telnet/ssh/série

---

sslcertupload

REMARQUE : Pour utiliser cette commande, vous devez disposer de l'autorisation **Configurer l'iDRAC**.

Le Tableau A-34 décrit la sous-commande **sslcertupload**.

Tableau A-34. sslcertupload

Sous-commande	Description
sslcertupload	Téléverse un serveur SSL personnalisé ou un certificat CA à partir du client sur le RAC.

Synopsis

```
racadm sslcertupload -t <type> [-f <nom de fichier>]
```

Options

Le Tableau A-35 décrit les options de la sous-commande **sslcertupload**.

Tableau A-35. Options de la sous-commande sslcertupload

Option	Description
-t	Spécifie le type de certificat à téléverser, soit le certificat CA, soit le certificat du serveur. 1 = certificat du serveur 2 = certificat CA
-f	Spécifie le nom de fichier du certificat à téléverser. Si le fichier n'est pas spécifié, le fichier **sslcert** dans le répertoire actuel est sélectionné.

La commande **sslcertupload** renvoie `0` si elle réussit et un chiffre différent de zéro si elle ne réussit pas.

Restrictions

La sous-commande **sslcertupload** peut seulement être exécutée à partir d'un client de la RACADM locale ou distante. La sous-commande **sslcsrgen** ne peut pas être utilisée dans l'interface série, telnet ou SSH.

Exemple

```
racadm sslcertupload -t 1 -f c:\cert\cert.txt
```

Interfaces prises en charge

- RACADM locale
- RACADM distant

---

sslcertdownload

REMARQUE : Pour utiliser cette commande, vous devez disposer de l'autorisation **Configurer l'iDRAC**.

Le Tableau A-36 décrit la sous-commande **sslcertdownload**.

Tableau A-36. sslcertdownload

Sous-commande	Description
sslcertupload	Télécharge un certificat SSL à partir de l'iDRAC6 sur le système de fichiers du client.

Synopsis

```
racadm sslcertdownload -t <type> [-f <nom de fichier>]
```

Options

Le Tableau A-37 décrit les options de la sous-commande **sslcertdownload**.

Tableau A-37. Options de la sous-commande sslcertdownload

Option	Description
-t	Spécifie le type de certificat à télécharger, le certificat Microsoft® Active Directory® ou le certificat du serveur. 1 = certificat du serveur 2 = certificat Microsoft Active Directory
-f	Spécifie le nom de fichier du certificat à télécharger. Si l'option **-f** ou le nom de fichier n'est pas spécifié, le fichier **sslcert** dans le répertoire actuel est sélectionné.

La commande **sslcertdownload** renvoie `0` si elle réussit et un chiffre différent de zéro si elle ne réussit pas.

Restrictions

La sous-commande **sslcertdownload** peut seulement être exécutée à partir d'un client de la RACADM locale ou distante. La sous-commande **sslcsrgen** ne peut pas être utilisée dans l'interface série, telnet ou SSH.

Exemple

```
racadm sslcertdownload -t 1 -f c:\cert\cert.txt
```

Interfaces prises en charge

- RACADM locale
- RACADM distant

---

sslcertview

REMARQUE : Pour utiliser cette commande, vous devez disposer de l'autorisation **Configurer l'iDRAC**.

Le Tableau A-38 décrit la sous-commande **sslcertview**.

Tableau A-38. sslcertview

Sous-commande	Description
sslcertview	Affiche le serveur SSL ou le certificat CA qui existe sur le RAC.

Synopsis

```
racadm sslcertview -t <type> [-A]
```

Options

Le Tableau A-39 décrit les options de la sous-commande **sslcertview**.

Tableau A-39. Options de la sous-commande sslcertview

Option	Description
-t	Spécifie le type de certificat à afficher, soit le certificat Microsoft Active Directory, soit le certificat du serveur. 1 = certificat du serveur 2 = certificat Microsoft Active Directory
-A	Empêche d'imprimer les en-têtes et les noms.

Exemple de sortie

```
racadm sslcertview -t 1

Serial Number             : 00

Subject Information:
Country Code (CC)         : US
State (S)                 : Texas
Locality (L)              : Round Rock
Organization (O)          : Dell Inc.
Organizational Unit (OU)  : Remote Access Group
Common Name (CN)          : iDRAC6 default certificate

Issuer Information:
Country Code (CC)         : US
State (S)                 : Texas
Locality (L)              : Round Rock
Organization (O)          : Dell Inc.
Organizational Unit (OU)  : Remote Access Group
Common Name (CN)          : iDRAC6 default certificate

Valid From                : Jul 8 16:21:56 2005 GMT
Valid To                  : Jul 7 16:21:56 2010 GMT

racadm sslcertview -t 1 -A

00
US
Texas
Round Rock
Dell Inc.
Remote Access Group
iDRAC6 default certificate
US
Texas
Round Rock
Dell Inc.
Remote Access Group
iDRAC6 default certificate
Jul 8 16:21:56 2005 GMT
Jul 7 16:21:56 2010 GMT
```

Interfaces prises en charge

- RACADM locale
- RACADM distant
- RACADM telnet/ssh/série

---

sslkeyupload

REMARQUE : Pour utiliser cette commande, vous devez disposer de l'autorisation **Configurer l'iDRAC**.

Le Tableau A-40 décrit la sous-commande **sslkeyupload**.

Tableau A-40. sslkeyupload

Sous-commande	Description
sslkeyupload	Téléverse la clé SSL du client sur l'iDRAC6.

Synopsis

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

Options

Le Tableau A-41 décrit les options de la sous-commande **sslkeyupload**.

Tableau A-41. Options de la sous-commande sslkeyupload

Option	Description
-t	Spécifie la clé à téléverser. 1 = clé SSL utilisée pour générer le certificat du serveur
-f	Spécifie le nom de fichier de la clé SSL à téléverser.

La commande **sslkeyupload** renvoie `0` si elle réussit et un chiffre différent de zéro si elle ne réussit pas.

Restrictions

La sous-commande **sslkeyupload** peut seulement être exécutée à partir d'un client de la RACADM locale ou distante. Elle ne peut pas être utilisée dans l'interface série, telnet, ou SSH.

Exemple

```
racadm sslkeyupload -t 1 -f c:\sslkey.txt
```

Interfaces prises en charge

- RACADM locale
- RACADM distant

---

testemail

Le Tableau A-42 décrit la sous-commande **testemail**.

Tableau A-42. configuration de testemail

Sous-commande	Description
testemail	Teste la fonctionnalité d'alerte par e-mail du RAC.

Synopsis

```
racadm testemail -i <index>
```

Description

Envoie un e-mail test à partir de l'iDRAC6 vers une destination spécifiée.

Avant d'exécuter la commande testemail, assurez-vous que l'index indiqué dans le groupe **cfgEmailAlert** RACADM est activé et configuré correctement. Le Tableau A-43 fournit une liste et les commandes associées pour le groupe **cfgEmailAlert**.

Tableau A-43. configuration de testemail

Action	Commande
Activer l'alerte	racadm config -g cfgEmailAlert -o cfgEmailAlertEnable -i 1 1
Définir l'adresse e-mail de destination	racadm config -g cfgEmailAlert -o cfgEmailAlertAddress -i 1 user1@mycompany.com
Définir le message personnalisé qui est envoyé à l'adresse e-mail de destination	racadm config -g cfgEmailAlert -o cfgEmailAlertCustomMsg -i 1 "This is a test!" (« C'est un test ! »)
Vérifier si l'adresse IP SMTP est configurée correctement	racadm config -g cfgRemoteHosts -o cfgRhostsSmtpServerIpAddr 192.168.0.152
Afficher les paramètres d'alerte par e-mail actuels	racadm getconfig -g cfgEmailAlert -i <*index*> où <*index*> est un numéro de 1 à 4

Options

Le Tableau A-44 décrit les options de la sous-commande **testemail**.

Tableau A-44. Sous-commandes testemail

Option	Description
-i	Spécifie l'index de l'alerte par e-mail à tester.

Résultat

Aucune.

Interfaces prises en charge

- RACADM locale
- RACADM distant
- RACADM telnet/ssh/série

---

testtrap

REMARQUE : Pour utiliser cette commande, vous devez avoir le droit **Tester les alertes**.

Le Tableau A-45 décrit la sous-commande **testtrap**.

Tableau A-45. testtrap

Sous-commande	Description
testtrap	Teste la fonctionnalité d'alerte d'interruption SNMP du RAC.

Synopsis

```
racadm testtrap -i <index>
```

Description

La sous-commande **testtrap** teste la fonctionnalité d'alerte d'interruption SNMP du RAC en envoyant une interruption test de l'iDRAC6 vers une interruption de destination spécifiée sur le réseau.

Avant d'exécuter la sous-commande **testtrap**, assurez-vous que l'index indiqué dans le groupe **cfgIpmiPet** RACADM est configuré correctement.

Tableau A-46 fournit une liste et les commandes associées pour le groupe **cfgIpmiPet**.

Tableau A-46. Commandes cfgEmailAlert

Action	Commande
Activer l'alerte	racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 1 1
Définir l'adresse IP de l'e-mail de destination	racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIpAddr -i 1 192.168.0.110
Afficher les paramètres d'interruption test actuels	racadm getconfig -g cfgIpmiPet -i <*index*> où <*index*> est un numéro de 1 à 4

Entrée

Le Tableau A-47 décrit les options de la sous-commande **testtrap**.

Tableau A-47. Options de la sous-commande testtrap

Option	Description
-i	Spécifie l'index de la configuration d'interruption à utiliser pour le test, les valeurs valides sont comprises entre 1 et 4.

Interfaces prises en charge

- RACADM locale
- RACADM distant
- RACADM telnet/ssh/série

---

vmdisconnect

REMARQUE : Pour utiliser cette commande, vous devez avoir le droit **Accéder au média virtuel**.

Le Tableau A-48 décrit la sous-commande **vmdisconnect**.

Tableau A-48. vmdisconnect

Sous-commande	Description
vmdisconnect	Ferme toutes les connexions du média virtuel iDRAC6 ouvertes à partir des clients distants.

Synopsis

```
racadm vmdisconnect
```

Description

La sous-commande **vmdisconnect** permet à un utilisateur de fermer la session du média virtuel d'un autre utilisateur. Une fois la session fermée, l'interface Web reflète l'état de connexion approprié. Cette sous-commande n'est disponible que si vous utilisez la racadm locale ou distante.

La sous-commande **vmdisconnect** permet à un utilisateur iDRAC6 de fermer toutes les sessions de média virtuel actives. Les sessions de média virtuel actives peuvent être affichées dans l'interface Web de l'iDRAC6 ou à l'aide de la sous-commande RACAD **getsysinfo**.

Interfaces prises en charge

- RACADM locale

- RACADM distant
- RACADM telnet/ssh/série

---

vmkey

REMARQUE : Pour utiliser cette commande, vous devez avoir le droit **Accéder au média virtuel**.

Le Tableau A-49 décrit la sous-commande **vmkey**.

Tableau A-49. vmkey

Sous-commande	Description
vmkey	Effectue des opérations concernant la clé du média virtuel.

Synopsis

```
racadm vmkey <action>
```

Si *<action>* est configuré sur `reset`, la mémoire flash virtuelle est réinitialisée à 256 Mo, sa taille par défaut.

Description

Quand une image de clé de média virtuel personnalisée est téléversée dans le RAC, la taille de la clé devient la taille de l'image. La sous-commande `vmkey` peut être utilisée pour réinitialiser la taille par défaut d'origine de la clé, qui est de 256 Mo sur l'iDRAC6.

Interfaces prises en charge

- RACADM locale
- RACADM distant
- RACADM telnet/ssh/série

---

usercertupload

REMARQUE : Pour utiliser cette commande, vous devez disposer de l'autorisation **Configurer l'iDRAC**.

Le Tableau A-50 décrit la sous-commande **usercertupload**.

Tableau A-50. usercertupload

Sous-commande	Description
usercertupload	Téléverse un certificat d'utilisateur ou un certificat CA d'utilisateur du client sur l'iDRAC6.

Synopsis

```
racadm usercertupload -t <type> [-f <nom de fichier>] -i <index>
```

Options

Le Tableau A-51 décrit les options de la sous-commande **usercertupload**.

Tableau A-51. Options de la sous-commande usercertupload

Option	Description

-t	Spécifie le type de certificat à téléverser, soit le certificat CA, soit le certificat du serveur. 1 = certificat d'utilisateur 2 = certificat CA d'utilisateur
-f	Spécifie le nom de fichier du certificat à téléverser. Si le fichier n'est pas spécifié, le fichier **sslcert** dans le répertoire actuel est sélectionné.
-i	Numéro d'index de l'utilisateur. Valeurs valides : 1-16.

La commande **usercertupload** renvoie `0` si elle réussit et un chiffre différent de zéro si elle ne réussit pas.

Restrictions

La sous-commande **usercertupload** peut seulement être exécutée à partir d'un client de la RACADM locale ou distante.

Exemple

```
racadm usercertupload -t 1 -f c:\cert\cert.txt -i 6
```

Interfaces prises en charge

- RACADM locale
- RACADM distant

---

usercertview

REMARQUE : Pour utiliser cette commande, vous devez disposer de l'autorisation **Configurer l'iDRAC**.

Le Tableau A-52 décrit la sous-commande **usercertview**.

Tableau A-52. usercertview

Sous-commande	Description
usercertview	Affiche le certificat d'utilisateur ou le certificat CA d'utilisateur qui existe sur l'iDRAC6.

Synopsis

```
racadm sslcertview -t <type> [-A] -i <index>
```

Options

Le Tableau A-53 décrit les options de la sous-commande **sslcertview**.

Tableau A-53. Options de la sous-commande sslcertview

Option	Description
-t	Spécifie le type de certificat à afficher, soit le certificat d'utilisateur, soit le certificat CA d'utilisateur. 1 = certificat d'utilisateur 2 = certificat CA d'utilisateur
-A	Empêche d'imprimer les en-têtes et les noms.
-i	Numéro d'index de l'utilisateur. Valeurs valides : 1-16.

Interfaces prises en charge

- RACADM locale
- RACADM distant
- RACADM telnet/ssh/série

---

localConRedirDisable

REMARQUE : Seul un utilisateur de la racadm locale peut exécuter cette commande.

Le Tableau A-54 décrit la sous-commande **localConRedirDisable**.

Tableau A-54. localConRedirDisable

Sous-commande	Description
localConRedirDisable	Désactive la redirection de console vers la station de gestion.

Synopsis

`racadm localConRedirDisable <option>`

Si *<option>* est défini sur 1, la redirection de console est désactivée.

Si *<option>* est défini sur 0, la redirection de console est activée.

Interfaces prises en charge

- RACADM locale

---

krbkeytabupload

REMARQUE : Pour utiliser cette commande, vous devez disposer de l'autorisation **Configurer l'iDRAC**.

Le Tableau A-55 décrit la sous-commande **kerbkeytabupload**.

Tableau A-55. kerbkeytabupload

Sous-commande	Description
krbkeytabupload	Téléverse le fichier keytab Kerberos.

Synopsis

`racadm krbkeytabupload [-f <nomdefichier>]`

<nom de fichier> est le nom du fichier incluant le chemin.

Options

Le Tableau A-56 décrit les options de la sous-commande **krbkeytabupload**.

Tableau A-56. Options de la sous-commande kerbkeytabupload

Option	Description
-f	Spécifie le nom de fichier du keytab à téléverser. Si le fichier n'est pas spécifié, le fichier keytab dans le répertoire actuel est sélectionné.

La commande **krbkeytabupload** renvoie `0` si elle réussit et un chiffre différent de zéro si elle ne réussit pas.

Restrictions

La sous-commande **krbkeytabupload** peut seulement être exécutée à partir d'un client de la RACADM locale ou distante.

Exemple

```
racadm krbkeytabupload -f c:\keytab\krbkeytab.tab
```

Interfaces prises en charge

- RACADM locale
- RACADM distant

Retour á la page du sommaire

Retour á la page du sommaire

Définitions des groupes et des objets de la base de données des propriétés iDRAC6

Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.1

La base de données de propriétés iDRAC6 contient les informations de configuration iDRAC6. Les données sont organisées par objet associé et les objets sont organisés par groupe d'objets. Les ID des groupes et des objets pris en charge par la base de données des propriétés sont répertoriés dans cette section.

Utilisez les numéros des groupes et des objets avec l'utilitaire RACADM pour configurer l'iDRAC6. Les sections suivantes décrivent chaque objet et indiquent si l'on peut lire et/ou écrire sur l'objet.

△ **PRÉCAUTION : Racadm définit la valeur des objets sans effectuer de validation fonctionnelle sur ces derniers. Par exemple, RACADM permet de définir l'objet Validation de certificat sur 1 avec l'objet Active Directory défini sur 0, même si la validation de certificat peut se produire uniquement si Active Directory® est activé. De même, l'objet cfgADSSOEnable peut être défini sur 0 ou 1 même si l'objet cfgADEnable est défini sur 0, mais devient effectif uniquement si Active Directory est activé.**

Toutes les valeurs de chaîne de caractères sont limitées aux caractères ASCII affichables, sauf spécification contraire.

Caractères affichables

Les caractères affichables comprennent le jeu suivant :

```
abcdefghijklmnopqrstuvwxwz

ABCDEFGHIJKLMNOPQRSTUVWXYZ

0123456789~`!@#$%^&*()_+-={}[]|\:";',.?/
```

---

idRacInfo

Ce groupe contient des paramètres d'affichage pour les informations sur les spécifications du contrôleur iDRAC6 interrogé.

Une seule instance du groupe est autorisée. Les sous-sections suivantes décrivent les objets de ce groupe.

idRacProductInfo (lecture seule)

Valeurs valides

Chaîne de 63 caractères ASCII maximum.

Valeur par défaut

Integrated Dell Remote Access Controller

Description

Une chaîne de texte qui identifie le produit.

idRacDescriptionInfo (lecture seule)

Valeurs valides

Chaîne de 255 caractères ASCII maximum.

Valeur par défaut

Ce composant système fournit aux serveurs Dell PowerEdge un ensemble complet de fonctions de gestion à distance.

Description

Une description textuelle du type de l'iDRAC.

idRacVersionInfo (lecture seule)

Valeurs valides

Chaîne de 63 caractères ASCII maximum.

Valeur par défaut

<numéro de version actuelle>

Description

Chaîne de caractères contenant la version actuelle du micrologiciel du produit.

idRacBuildInfo (lecture seule)

Valeurs valides

Chaîne de 16 caractères ASCII maximum.

Valeur par défaut

Numéro de version du micrologiciel de l'iDRAC actuel.

Description

Chaîne de caractères contenant le numéro de version du produit actuel.

idRacName (lecture seule)

Valeurs valides

Chaîne de 15 caractères ASCII maximum.

Valeur par défaut

iDRAC

Description

Un nom attribué par l'utilisateur pour identifier ce contrôleur.

idRacType (lecture seule)

Valeurs valides

ID de produit

Valeur par défaut

10

Description

Identifie le type de Remote Access Controller comme iDRAC6.

---

cfgLanNetworking

Ce groupe contient les paramètres qui permettent de configurer le NIC de l'iDRAC.

Une seule instance du groupe est autorisée. Certains objets de ce groupe nécessitent une réinitialisation du NIC de l'iDRAC, ce qui peut interrompre brièvement la connectivité. Les objets qui modifient les paramètres de l'adresse IP du NIC de l'iDRAC entraînent la fermeture de toutes les sessions utilisateur actives ; les utilisateurs doivent alors se reconnecter en utilisant les nouveaux paramètres de l'adresse IP.

cfgNicIPv4Enable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

1

Description

Active ou désactive l'adresse IPv4 de l'iDRAC.

cfgNicSelection (lecture/écriture)

Valeurs valides

0 = Partagé

1 = Partagé avec basculement LOM2

2 = Dédié

3= Partagé avec basculement de tous les LOM (iDRAC6 Enterprise uniquement)

Valeur par défaut

0 (iDRAC6 Express)

2 (iDRAC6 Enterprise)

Description

Spécifie le mode de fonctionnement actuel pour le contrôleur d'interface réseau du RAC (NIC). Le Tableau B-1 décrit les modes pris en charge.

Tableau B-1. Modes pris en charge par cfgNicSelection

Mode	Description
Partagé	Utilisé si le NIC intégré au serveur hôte est partagé avec le RAC sur le serveur hôte. Ce mode permet aux configurations d'utiliser la même adresse IP sur le serveur hôte et le RAC pour l'accessibilité commune sur le réseau.
Partagé avec basculement : LOM 2	Active les capacités de partage entre les contrôleurs d'interface réseau LOM 2 intégrés au serveur hôte.
Dédié	Spécifie que le NIC du RAC est utilisé comme NIC dédié pour l'accessibilité à distance.
Partagé avec Basculement de tous les LOM	Active les capacités de partage entre tous les LOM sur les contrôleurs d'interface réseau intégrés au serveur hôte. L'interface réseau du périphérique d'accès à distance est complètement fonctionnelle lorsque 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. Le basculement se produit à partir du NIC 2 vers le NIC 3 et ensuite vers le NIC 4. Si le NIC 4 est défectueux, le périphérique d'accès à distance refait basculer toutes les données transmises vers le NIC 1, mais uniquement si l'échec initial du NIC 1 a été corrigé.

cfgNicVLanEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Active ou désactive les capacités VLAN du RAC/BMC.

cfgNicVLanId (lecture/écriture)

Valeurs valides

1-4094

Valeur par défaut

1

Description

Spécifie l'ID du VLAN pour la configuration du VLAN réseau. Cette propriété n'est valide que si **cfgNicVLanEnable** est défini sur **1** (activé).

cfgNicVLanPriority (lecture/écriture)

Valeurs valides

0 – 7

Valeur par défaut

0

Description

Spécifie la priorité du VLAN pour la configuration du VLAN réseau. Cette propriété n'est valide que si cfgNicVLanEnable est défini sur 1 (activé).

cfgDNSDomainNameFromDHCP (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Spécifie que le nom de domaine DNS de l'iDRAC doit être attribué à partir du serveur DHCP réseau.

cfgDNSDomainName (lecture/écriture)

Valeurs valides

Chaîne de 254 caractères ASCII maximum. Au moins l'un des caractères doit être alphabétique. Les caractères sont limités aux caractères alphanumériques, « - » et « . ».

REMARQUE : Microsoft® Active Directory® ne prend en charge que les noms de domaine pleinement qualifiés (FQDN) de 64 octets ou moins.

Valeur par défaut

<vide>

Description

Il s'agit du nom de domaine DNS.

cfgDNSRacName (lecture/écriture)

Valeurs valides

Chaîne de 63 caractères ASCII maximum. Au moins un caractère doit être alphabétique.

REMARQUE : Certains serveurs DNS ne peuvent enregistrer que des noms de 31 caractères maximum.

Valeur par défaut

idrac-<numéro de service>

Description

Affiche le nom de l'iDRAC, qui est rac-*numéro de service* par défaut. Ce paramètre n'est valide que si **cfgDNSRegisterRac** est défini sur 1 (VRAI).

cfgDNSRegisterRac (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Enregistre le nom de l'iDRAC sur le serveur DNS.

cfgDNSServersFromDHCP (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Spécifie que les adresses IPv4 du serveur DNS doivent être attribuées à partir du serveur DHCP sur le réseau.

cfgDNSServer1 (lecture/écriture)

Valeurs valides

Chaîne de caractères représentant une adresse IPv4 valide. Par exemple : 192.168.0.20.

Valeur par défaut

0.0.0.0

Description

Spécifie l'adresse IPv4 du serveur DNS 1.

cfgDNSServer2 (lecture/écriture)

Valeurs valides

Chaîne de caractères représentant une adresse IPv4 valide. Par exemple : 192.168.0.20.

Valeur par défaut

0.0.0.0

Description

Récupère l'adresse IPv4 du serveur DNS 2.

cfgNicEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

1

Description

Active ou désactive le contrôleur d'interface réseau iDRAC6. Si le NIC est désactivé, les interfaces réseau à distance vers l'iDRAC6 ne sont plus accessibles.

cfgNicIpAddress (lecture/écriture)

REMARQUE : Ce paramètre n'est configurable que si le paramètre **cfgNicUseDhcp** est défini sur 0 (FAUX).

Valeurs valides

Chaîne de caractères représentant une adresse IPv4 valide. Par exemple : 192.168.0.20.

Valeur par défaut

192.168.0.120

Description

Spécifie l'adresse IPv4 attribuée à l'iDRAC

cfgNicNetmask (lecture/écriture)

REMARQUE : Ce paramètre n'est configurable que si le paramètre **cfgNicUseDhcp** est défini sur 0 (FAUX).

Valeurs valides

Chaîne de caractères représentant un masque de sous-réseau valide. Par exemple : 255.255.255.0.

Valeur par défaut

255.255.255.0

Description

Le masque de sous-réseau utilisé pour l'adresse IP du iDRAC6.

cfgNicGateway (lecture/écriture)

REMARQUE : Ce paramètre n'est configurable que si le paramètre **cfgNicUseDhcp** est défini sur 0 (FAUX).

Valeurs valides

Chaîne de caractères représentant une adresse IPv4 de passerelle valide. Par exemple : 192.168.0.1.

Valeur par défaut

192.168.0.1

Description

Adresse IPv4 de la passerelle de l'iDRAC.

cfgNicUseDhcp (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Spécifie si le DHCP est utilisé pour attribuer l'adresse IPv4 de l'iDRAC. Si cette propriété est définie sur 1 (VRAI), l'adresse IPv4, le masque de sous-réseau et la passerelle de l'iDRAC sont attribués à partir du serveur DHCP sur le réseau. Si cette propriété est définie sur **0** (FAUX), l'utilisateur peut configurer les propriétés **cfgNicIpAddress**, **cfgNicNetmask** et **cfgNicGateway**.

cfgNicMacAddress (lecture seule)

Valeurs valides

Chaîne de caractères représentant l'adresse MAC de l'iDRAC

Valeur par défaut

Adresse MAC actuelle du NIC de l'iDRAC. Par exemple, 00:12:67:52:51:A3.

Description

Adresse MAC du NIC de l'iDRAC.

---

cfgRemoteHosts

Ce groupe fournit des propriétés qui autorisent la configuration du serveur SMTP pour les alertes par e-mail.

cfgRhostsFwUpdateTftpEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

1

Description

Active ou désactive la mise à jour du micrologiciel de l'iDRAC à partir d'un serveur TFTP réseau.

cfgRhostsFwUpdateIpAddr (lecture/écriture)

Valeurs valides

Chaîne de caractères représentant une adresse IPv4 valide. Par exemple, 192.168.0.61.

Valeur par défaut

0.0.0.0

Description

Spécifie l'adresse IPv4 du serveur TFTP réseau qui est utilisée pour les opérations de mise à jour du micrologiciel de l'iDRAC via TFTP.

cfgRhostsFwUpdatePath (lecture/écriture)

Valeurs valides

Une chaîne de caractères dont la longueur est limitée à 255 caractères ASCII.

Valeur par défaut

<vide>

Description

Spécifie le chemin d'accès TFTP où le fichier image du micrologiciel de l'iDRAC existe sur le serveur TFTP. Le chemin TFTP est relatif au chemin d'accès racine TFTP sur le serveur TFTP.

REMARQUE : Le serveur peut vous demander de spécifier le lecteur (par exemple, **C:**).

cfgRhostsSmtpServerIpAddr (lecture/écriture)

Valeurs valides

Chaîne de caractères représentant une adresse IPv4 valide du serveur SMTP. Par exemple, 192.168.0.55.

Valeur par défaut

0.0.0.0

Description

L'adresse IPv4 du serveur de réseau SMTP ou du serveur TFTP. Le serveur SMTP transmet les alertes par e-mail de l'iDRAC si les alertes sont configurées et activées. Le serveur TFTP transmet les fichiers depuis et vers l'iDRAC6.

---

cfgUserAdmin

Ce groupe fournit des informations de configuration sur les utilisateurs qui ont le droit d'accéder à l'iDRAC via les interfaces distantes disponibles.

Jusqu'à 16 instances du groupe d'utilisateurs sont autorisées. Chaque instance représente la configuration d'un utilisateur individuel.

cfgUserAdminIndex (lecture seule)

Valeurs valides

1 – 16

Valeur par défaut

<instance>

Description

Ce chiffre représente l'interface utilisateur.

cfgUserAdminIpmiLanPrivilege (lecture/écriture)

Valeurs valides

2 (utilisateur)

3 (opérateur)

4 (administrateur)

15 (pas d'accès)

Valeur par défaut

4 (utilisateur 2)

15 (tous les autres)

Description

Privilège maximum sur le canal LAN IPMI.

cfgUserAdminPrivilege (lecture/écriture)

Valeurs valides

0x00000000 à 0x000001ff, et 0x0

Valeur par défaut

0x00000000

Description

Cette propriété spécifie les privilèges basés sur le rôle qui sont autorisés pour l'utilisateur. La valeur est représentée comme un masque binaire qui autorise n'importe quelle combinaison de valeurs de privilège. Le Tableau B-2 décrit les valeurs binaires des droits d'utilisateur pouvant être combinées pour créer des masques binaires.

Tableau B-2. Masques binaires pour les privilèges utilisateur

Privilège utilisateur	Masque binaire de privilège
Ouvrir une session iDRAC	0x0000001
Configurer iDRAC	0x0000002
Configurer les utilisateurs	0x0000004
Effacer les journaux	0x0000008
Exécuter les commandes de contrôle du serveur	0x0000010
Accéder à la redirection de console	0x0000020
Accéder au média virtuel	0x0000040
Tester les alertes	0x0000080
Exécuter les commandes de débogage	0x0000100

Exemples

Le Tableau B-3 fournit des exemples de masques binaires de privilèges pour les utilisateurs avec un ou plusieurs privilèges.

Tableau B-3. Exemple de masques binaires pour les privilèges utilisateur

Privilège(s) utilisateur	Masque binaire de privilège
L'utilisateur n'est pas autorisé à accéder à iDRAC.	0x00000000
L'utilisateur peut uniquement se connecter à iDRAC et afficher les informations de configuration iDRAC et du serveur.	0x00000001
L'utilisateur peut se connecter à iDRAC et modifier la configuration.	0x00000001 + 0x00000002 = 0x00000003
L'utilisateur peut ouvrir une session sur l'iDRAC et accéder au média virtuel et à la redirection de console.	0x00000001 + 0x00000040 + 0x00000080 = 0x000000C1

cfgUserAdminUserName (lecture/écriture)

REMARQUE : Cette valeur de propriété doit être unique parmi les noms d'utilisateur.

Valeurs valides

Chaîne de 16 caractères ASCII maximum.

Valeur par défaut

racine (Utilisateur 2)

<vide> (Tous les autres)

Description

Le nom d'utilisateur pour cet index. L'index utilisateur est créé en écrivant une chaîne de caractères dans ce champ de nom si l'index est vide. L'écriture d'une chaîne de guillemets anglais ("") supprime l'utilisateur qui correspond à cet index. La chaîne ne peut pas contenir de barre oblique (/), de barre oblique inverse (\), de point (.), d'arobase (@) ou de guillemets.

REMARQUE : Cette valeur de propriété doit être unique parmi les noms d'utilisateur.

cfgUserAdminPassword (lecture seule)

Valeurs valides

Chaîne de 20 caractères ASCII maximum.

Valeur par défaut

****

Description

Le mot de passe de cet utilisateur. Les mots de passe utilisateur sont cryptés et ne peuvent être ni vus ni affichés une fois la propriété écrite.

cfgUserAdminEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

1 (utilisateur 2)

0 (tous les autres)

Description

Active ou désactive un utilisateur individuel.

cfgUserAdminSolEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Active ou désactive l'accès utilisateur aux communications série sur le LAN (SOL) pour l'utilisateur.

cfgUserAdminIpmiSerialPrivilege (lecture/écriture)

Valeurs valides

2 (utilisateur)

3 (opérateur)

4 (administrateur)

15 (pas d'accès)

Valeur par défaut

4 (utilisateur 2)

15 (tous les autres)

Description

Privilège maximum sur le canal LAN IPMI.

---

cfgEmailAlert

Ce groupe contient des paramètres pour configurer les capacités d'alerte par e-mail de l'iDRAC.

Les sous-sections suivantes décrivent les objets de ce groupe. Jusqu'à quatre instances de ce groupe sont autorisées.

cfgEmailAlertIndex (lecture seule)

Valeurs valides

1–4

Valeur par défaut

<instance>

Description

Index unique d'une instance d'alerte.

cfgEmailAlertEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Active ou désactive l'instance d'alerte.

cfgEmailAlertAddress (lecture/écriture)

Valeurs valides

Format d'adresse e-mail, avec une longueur maximum de 64 caractères ASCII.

Valeur par défaut

<vide>

Description

Spécifie l'adresse e-mail de destination pour les alertes par e-mail, par exemple, utilisateur1@compagnie.com

cfgEmailAlertCustomMsg (lecture/écriture)

Valeurs valides

Chaîne de 32 caractères maximum.

Valeur par défaut

<vide>

Description

Spécifie le message personnalisé qui constitue l'objet de l'alerte

---

cfgSessionManagement

Ce groupe contient les paramètres de configuration du nombre de sessions qui peuvent se connecter à l'iDRAC.

Une seule instance du groupe est autorisée. Les sous-sections suivantes décrivent les objets de ce groupe.

cfgSsnMgtRacadmTimeout (lecture/écriture)

Valeurs valides

10 –1 920

Valeur par défaut

60

Description

Définit le délai d'attente en secondes pour l'interface RACADM distante. Si une session RACADM distante reste inactive plus longtemps que spécifié, la session est fermée.

cfgSsnMgtConsRedirMaxSessions (lecture/écriture)

Valeurs valides

1 - 4

Valeur par défaut

2

Description

Spécifie le nombre maximum de sessions de redirection de console autorisées sur l'iDRAC6.

cfgSsnMgtWebserverTimeout (lecture/écriture)

Valeurs valides

60 – 10800

Valeur par défaut

1800

Description

Définit le délai d'attente du serveur Web. Cette propriété définit la durée en secondes pendant laquelle une connexion peut rester inactive (il n'y a aucune entrée de la part de l'utilisateur). La session est annulée une fois la durée définie par cette propriété atteinte. Les modifications de ce paramètre n'affectent pas les sessions déjà ouvertes ; vous devez fermer la session et la rouvrir pour que les nouveaux paramètres soient pris en compte.

cfgSsnMgtSshIdleTimeout (lecture/écriture)

Valeurs valides

0 (pas de délai d'attente)

60 – 1 920

Valeur par défaut

300

Description

Définit le délai d'attente en cas d'inactivité attribuée à Secure Shell (protocole de connexions sécurisées). Cette propriété définit la durée en secondes pendant laquelle une connexion peut rester inactive (il n'y a aucune entrée de la part de l'utilisateur). La session est annulée une fois la durée définie par cette propriété atteinte. Les modifications de ce paramètre n'affectent pas les sessions déjà ouvertes ; vous devez fermer la session et la rouvrir pour que les nouveaux paramètres soient pris en compte.

Une session Secure Shell qui a expiré affiche le message d'erreur suivant :

```
Connection timed out (Le délai de connexion a expiré.)
```

Une fois le message affiché, le système vous renvoie à l'environnement qui a généré la session Secure Shell.

cfgSsnMgtTelnetTimeout (lecture/écriture)

Valeurs valides

0 (pas de délai d'attente)

60 – 1 920

Valeur par défaut

300

Description

Définit le délai d'attente en cas d'inactivité Telnet. Cette propriété définit la durée en secondes pendant laquelle une connexion peut rester inactive (sans entrée de la part de l'utilisateur). La session est annulée une fois la durée définie par cette propriété atteinte. Les modifications de ce paramètre n'affectent pas la session ouverte (vous devez fermer la session et la rouvrir pour que les nouveaux paramètres soient pris en compte).

Une session Telnet expirée affiche le message d'erreur suivant :

```
Connection timed out (Le délai de connexion a expiré.)
```

Une fois le message affiché, le système vous renvoie à l'environnement qui a généré la session Telnet.

---

cfgSerial

Ce groupe contient les paramètres de configuration des services iDRAC6.

Une seule instance du groupe est autorisée. Les sous-sections suivantes décrivent les objets de ce groupe.

cfgSerialBaudRate (lecture/écriture)

Valeurs valides

9600, 28800, 57600, 115200

Valeur par défaut

57600

Description

Définit le débit en bauds du port série iDRAC6.

cfgSerialConsoleEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Active ou désactive l'interface de console série du RAC.

cfgSerialConsoleQuitKey (lecture/écriture)

Valeurs valides

Chaîne de 4 caractères maximum.

Valeur par défaut

^\ (<Ctrl><\>)

REMARQUE : « ^ » est la touche <Ctrl>.

Description

Cette touche ou combinaison de touches interrompt la redirection de console de texte lorsque vous utilisez la commande **console com2**. La valeur **cfgSerialConsoleQuitKey** peut être représentée par ce qui suit :

- Valeur décimale - Par exemple : « 95 »
- Valeur hexadécimale - Par exemple : « 0x12 »
- Valeur octale - Par exemple : « 007 »
- Valeur ASCII - Par exemple : « ^a »

  Les valeurs ASCII peuvent être représentées à l'aide des séquences de touches d'échappement suivantes :

  (a) ^ suivi par n'importe quelle lettre de l'alphabet (a-z, A-Z)

  (b) ^ suivi par les caractères spéciaux énumérés : [] \ ^ _

cfgSerialConsoleIdleTimeout (lecture/écriture)

Valeurs valides

0 = aucun délai d'attente

60 – 1 920

Valeur par défaut

300

Description

Nombre maximum de secondes d'attente avant la fermeture d'une session série inactive.

cfgSerialConsoleNoAuth (lecture/écriture)

Valeurs valides

0 (active l'authentification d'ouverture de session série)

1 (désactive l'authentification d'ouverture de session série)

Valeur par défaut

0

Description

Active ou désactive l'authentification d'ouverture de session de console série du RAC.

cfgSerialConsoleCommand (lecture/écriture)

Valeurs valides

Chaîne de 128 caractères maximum.

Valeur par défaut

<vide>

Description

Spécifie une commande série exécutée après qu'un utilisateur ouvre une session sur l'interface de console série.

cfgSerialHistorySize (lecture/écriture)

Valeurs valides

0 – 8 192

Valeur par défaut

8192

Description

Spécifie la taille maximale du tampon de l'historique série.

cfgSerialCom2RedirEnable (lecture/écriture)

Valeur par défaut

1

Valeurs valides

1 (VRAI)

0 (FAUX)

Description

Active ou désactive la console pour la redirection de port COM 2.

cfgSerialSshEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

1

Description

Active ou désactive l'interface Secure Shell (SSH) sur l'iDRAC6.

cfgSerialTelnetEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Active ou désactive l'interface de console Telnet sur l'iDRAC6.

---

cfgOobSnmp

Ce groupe présente des paramètres de configuration de l'agent SNMP et des capacités d'interruption de l'iDRAC.

Une seule instance du groupe est autorisée. Les sous-sections suivantes décrivent les objets de ce groupe.

cfgOobSnmpAgentCommunity (lecture/écriture)

Valeurs valides

Chaîne de 31 caractères maximum.

Valeur par défaut

public

Description

Spécifie le nom de communauté SNMP utilisé pour les interruptions SNMP.

cfgOobSnmpAgentEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Active ou désactive l'agent SNMP dans l'iDRAC6.

---

cfgRacTuning

Ce groupe est utilisé pour configurer diverses propriétés de configuration iDRAC6, comme par exemple les ports valides et les restrictions de port de sécurité.

cfgRacTuneConRedirPort (lecture/écriture)

Valeurs valides

1 – 65 535

Valeur par défaut

5900

Description

Spécifie le port à utiliser pour le clavier, la souris, la vidéo et le trafic du médial virtuel sur le RAC.

cfgRacTuneRemoteracadmEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

1

Description

Active ou désactive l'interface RACADM distante dans l'iDRAC.

cfgRacTuneCtrlEConfigDisable

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Active ou désactive la possibilité de désactiver la capacité de l'utilisateur local à configurer l'iDRAC à partir de l'option ROM du POST du BIOS.

cfgRacTuneHttpPort (lecture/écriture)

Valeurs valides

1 – 65 535

Valeur par défaut

80

Description

Spécifie le numéro de port à utiliser pour la communication réseau HTTP avec l'iDRAC6.

cfgRacTuneHttpsPort (lecture/écriture)

Valeurs valides

1 – 65 535

Valeur par défaut

443

Description

Spécifie le numéro de port à utiliser pour la communication réseau HTTPS avec l'iDRAC6.

cfgRacTuneIpRangeEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Active ou désactive la fonctionnalité de validation de la plage d'adresse IPv4 de l'iDRAC.

cfgRacTuneIpRangeAddr (lecture/écriture)

Valeurs valides

Une chaîne représentant une adresse IPv4 formatée, par exemple, 192.168.0.44.

Valeur par défaut

192.168.1.1

Description

Spécifie la séquence binaire de l'adresse IPv4 acceptable dans les positions déterminées par les « 1 » dans la propriété du masque de plage (**cfgRacTuneIpRangeMask**)

cfgRacTuneIpRangeMask (lecture/écriture)

Valeurs valides

Chaîne représentant une adresse IPv4 formatée, par exemple, 255.255.255.0

Valeur par défaut

255.255.255.0

Description

Valeurs de masque IP standard avec bits justifiés à gauche Par exemple, 255.255.255.0.

cfgRacTuneIpBlkEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Active ou désactive la fonctionnalité Blocage de l'adresse IPv4 de l'iDRAC

cfgRacTuneIpBlkFailCount (lecture/écriture)

Valeurs valides

2 – 16

Valeur par défaut

5

Description

Nombre maximum d'échecs d'ouverture de session dans la fenêtre (**cfgRacTuneIpBlkFailWindow**) avant que les tentatives d'ouverture de session de l'adresse IP soient rejetées

cfgRacTuneIpBlkFailWindow (lecture/écriture)

Valeurs valides

10 – 65 535

Valeur par défaut

60

Description

Définit la période en secondes pendant laquelle les tentatives échouées sont comptées. Lorsque le nombre d'échecs dépasse cette limite, les échecs sont déduits du compte.

cfgRacTuneIpBlkPenaltyTime (lecture/écriture)

Valeurs valides

10 – 65 535

Valeur par défaut

300

Description

Définit la période en secondes pendant laquelle les requêtes de session d'une adresse IP avec échecs excessifs sont rejetées.

cfgRacTuneSshPort (lecture/écriture)

Valeurs valides

1 – 65 535

Valeur par défaut

22

Description

Spécifie le numéro de port utilisé pour l'interface SSH de l'iDRAC.

cfgRacTuneTelnetPort (lecture/écriture)

Valeurs valides

1 – 65 535

Valeur par défaut

23

Description

Spécifie le numéro de port utilisé pour l'interface Telnet de l'iDRAC

cfgRacTuneConRedirEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

1

Description

Active la redirection de console

cfgRacTuneConRedirEncryptEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

1

Description

Crypte la vidéo dans une session de redirection de console

cfgRacTuneAsrEnable (lecture/écriture)

REMARQUE : Cet objet nécessite une réinitialisation de l'iDRAC pour devenir actif.

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Active ou désactive la fonctionnalité de capture d'écran de la dernière panne d'iDRAC6.

cfgRacTuneDaylightOffset (lecture/écriture)

Valeurs valides

0 – 60

Valeur par défaut

0

Description

Spécifie le décalage des économies d'heure d'été (en minutes) à utiliser pour l'heure du RAC.

cfgRacTuneTimezoneOffset (lecture/écriture)

Valeurs valides

–720 – 780

Valeur par défaut

0

Description

Spécifie le décalage de fuseau horaire (en minutes) par rapport au temps moyen de Greenwich/temps universel coordonné à utiliser pour l'heure

du RAC. Certains décalages de fuseau horaire courants pour les fuseaux horaires des États-Unis

sont affichés ci-dessous :

-480 (PST : heure normale du Pacifique)

-420 (MST : heure normale des Rocheuses)

-360 (CST : heure normale du Centre)

-300 (EST : heure normale de l'Est)

cfgRacTuneLocalServerVideo (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

1

Description

Active (met en marche) ou désactive (met à l'arrêt) la vidéo du serveur local.

cfgRacTuneLocalConfigDisable (lecture/écriture)

Valeurs valides

0 (VRAI)

1 (FAUX)

Valeur par défaut

0

Description

Désactive l'accès en écriture aux données de configuration de l'iDRAC en le définissant sur 1

cfgRacTuneWebserverEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

1

Description

Active ou désactive le serveur Web de l'iDRAC. Si cette propriété est désactivée, l'iDRAC6 n'est pas accessible à l'aide de navigateurs Web clients. Cette propriété n'a aucun effet sur les interfaces Telnet/SSH ou RACADM.

---

ifcRacManagedNodeOs

Ce groupe contient des propriétés qui décrivent le système d'exploitation du serveur géré.

Une seule instance du groupe est autorisée. Les sous-sections suivantes décrivent les objets de ce groupe.

ifcRacMnOsHostname (lecture seule)

Valeurs valides

Chaîne de 255 caractères maximum.

Valeur par défaut

<vide>

Description

Le nom d'hôte du serveur géré.

ifcRacMnOsOsName (lecture seule)

Valeurs valides

Chaîne de 255 caractères maximum.

Valeur par défaut

<vide>

Description

Nom du système d'exploitation du serveur géré

---

cfgRacSecurity

Ce groupe est utilisé pour configurer les paramètres relatifs à la fonctionnalité de requête de signature de certificat (CSR) SSL d'iDRAC6. Les propriétés de ce groupe doivent être configurées avant de générer une RSC à partir d'iDRAC6.

Reportez-vous aux détails de la sous-commande RACADM **sslcsrgen** pour plus d'informations sur la génération de requêtes de signature de certificat.

cfgRacSecCsrCommonName (lecture/écriture)

Valeurs valides

Chaîne de 255 caractères maximum.

Valeur par défaut

<vide>

Description

Spécifie le nom de domaine (CN) de la RSC qui doit être un nom IP ou le nom de l'iDRAC donné dans le certificat.

cfgRacSecCsrOrganizationName (lecture/écriture)

Valeurs valides

Chaîne de 255 caractères maximum.

Valeur par défaut

<vide>

Description

Spécifie le nom de l'organisation (O) pour la RSC.

cfgRacSecCsrOrganizationUnit (lecture/écriture)

Valeurs valides

Chaîne de 255 caractères maximum.

Valeur par défaut

<vide>

Description

Spécifie le service de la compagnie (OU) pour la RSC.

cfgRacSecCsrLocalityName (lecture/écriture)

Valeurs valides

Chaîne de 255 caractères maximum.

Valeur par défaut

<vide>

Description

Spécifie la ville (L) pour la RSC.

cfgRacSecCsrStateName (lecture/écriture)

Valeurs valides

Chaîne de 255 caractères maximum.

Valeur par défaut

<vide>

Description

Spécifie le nom d'état (S) pour la RSC.

cfgRacSecCsrCountryCode (lecture/écriture)

Valeurs valides

Chaîne de 255 caractères maximum.

Valeur par défaut

<vide>

Description

Spécifie l'indicatif de pays (CC) de la CSR

cfgRacSecCsrEmailAddr (lecture/écriture)

Valeurs valides

Chaîne de 255 caractères maximum.

Valeur par défaut

<vide>

Description

Spécifie l'adresse e-mail de la RSC.

cfgRacSecCsrKeySize (lecture/écriture)

Valeurs valides

1024

2048

4096

Valeur par défaut

1024

Description

Spécifie la taille de la clé asymétrique SSL pour la RSC.

---

cfgRacVirtual

Ce groupe contient les paramètres qui permettent de configurer la fonctionnalité de média virtuel de l'iDRAC. Une seule instance du groupe est autorisée. Les sous-sections suivantes décrivent les objets de ce groupe.

cfgVirMediaAttached (lecture/écriture)

Valeurs valides

0 = Déconnecter

1 = Connecter

2 = Auto-Attach

Valeur par défaut

0

Description

Cet objet est utilisé pour connecter les périphériques virtuels au système via le bus USB. Lorsque les périphériques sont reliés, le serveur reconnaît les périphériques de stockage de masse USB valides reliés au système. Cela revient à relier un lecteur de CD-ROM/disquette USB local à un port USB sur le système. Lorsque les périphériques sont reliés, vous pouvez alors vous connecter aux périphériques virtuels à distance à l'aide de l'interface Web de l'iDRAC ou de la CLI. Lorsque cet objet est défini sur **0**, les périphériques ne sont plus reliés au bus USB.

cfgVirtualBootOnce (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Active ou désactive la fonctionnalité de démarrage unique de média virtuel de l'iDRAC.

cfgVirMediaFloppyEmulation (lecture/écriture)

REMARQUE : Le média virtuel doit être reconnecté (à l'aide de cfgVirMediaAttached) pour que ce changement prenne effet.

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Lorsqu'il est défini sur 0, le lecteur de disquette virtuel est reconnu comme un disque amovible par les systèmes d'exploitation Windows. Les systèmes d'exploitation Windows attribuent une lettre de lecteur C: ou supérieure pendant l'énumération. Lorsqu'elle est définie sur 1, le lecteur de disquette virtuel est considéré comme un lecteur de disquette par les systèmes d'exploitation Windows. Les systèmes d'exploitation Windows attribuent une lettre de lecteur, A: ou B:.

cfgVirMediaKeyEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Active ou désactive la fonctionnalité Clé de média virtuel du RAC.

---

cfgActiveDirectory

Ce groupe contient les paramètres qui permettent de configurer la fonctionnalité Active Directory de l'iDRAC.

cfgADRacDomain (lecture/écriture)

Valeurs valides

Une chaîne de texte imprimable contenant jusqu'à 254 caractères, avec ou sans espace.

Valeur par défaut

<vide>

Description

Domaine Active Directory où se trouve l'iDRAC6.

cfgADRacName (lecture/écriture)

Valeurs valides

Une chaîne de texte imprimable contenant jusqu'à 254 caractères, avec ou sans espace.

Valeur par défaut

<vide>

Description

Nom de l'iDRAC enregistré dans la forêt Active Directory.

cfgADEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Active ou désactive l'authentification utilisateur Active Directory sur l'iDRAC6. Si cette propriété est désactivée, seule l'authentification iDRAC6 locale est utilisée pour les ouvertures de session utilisateur.

cfgADSSOEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Active ou désactive l'authentification d'ouverture de session individuelle Active Directory sur l'iDRAC6.

cfgADSmartCardLogonEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Active ou désactive l'ouverture de session par carte à puce sur l'iDRAC6.

cfgADCRLEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Active ou désactive la vérification de la liste de révocation de certificat (CRL) pour les utilisateurs de la carte à puce basée sur Active Directory.

cfgADDomainController1 (lecture/écriture)

Valeurs valides

Une chaîne contenant jusqu'à 254 caractères ASCII représentant une adresse IP valide ou un nom de domaine pleinement qualifié (FQDN).

Valeur par défaut

<vide>

Description

L'iDRAC6 utilise la valeur que vous spécifiez pour rechercher les noms d'utilisateur dans le serveur LDAP.

cfgADDomainController2 (lecture/écriture)

Valeurs valides

Une chaîne contenant jusqu'à 254 caractères ASCII représentant une adresse IP valide ou un nom de domaine pleinement qualifié (FQDN).

Valeur par défaut

<vide>

Description

L'iDRAC6 utilise la valeur que vous spécifiez pour rechercher les noms d'utilisateur dans le serveur LDAP.

cfgADDomainController3 (lecture/écriture)

Valeurs valides

Une chaîne contenant jusqu'à 254 caractères ASCII représentant une adresse IP valide ou un nom de domaine pleinement qualifié (FQDN).

Valeur par défaut

<vide>

Description

L'iDRAC6 utilise la valeur que vous spécifiez pour rechercher les noms d'utilisateur dans le serveur LDAP.

cfgADAuthTimeout (lecture/écriture)

Valeurs valides

15 – 300 secondes

Valeur par défaut

120

Description

Spécifie le délai d'attente en secondes pour que les requêtes d'authentification Active Directory soient exécutées.

cfgADType (lecture/écriture)

Valeurs valides

1 (schéma étendu)

2 (schéma standard)

Valeur par défaut

1

Description

Détermine le type de schéma à utiliser avec Active Directory.

cfgADGlobalCatalog1 (lecture/écriture)

Valeurs valides

Une chaîne contenant jusqu'à 254 caractères ASCII représentant une adresse IP valide ou un nom de domaine pleinement qualifié (FQDN).

Valeur par défaut

<vide>

Description

L'iDRAC6 utilise la valeur que vous avez spécifiée pour rechercher des noms d'utilisateur sur le serveur de catalogue global.

cfgADGlobalCatalog2 (lecture/écriture)

Valeurs valides

Une chaîne contenant jusqu'à 254 caractères ASCII représentant une adresse IP valide ou un nom de domaine pleinement qualifié (FQDN).

Valeur par défaut

<vide>

Description

L'iDRAC6 utilise la valeur que vous avez spécifiée pour rechercher des noms d'utilisateur sur le serveur de catalogue global.

cfgADGlobalCatalog3 (lecture/écriture)

Valeurs valides

Une chaîne contenant jusqu'à 254 caractères ASCII représentant une adresse IP valide ou un nom de domaine pleinement qualifié (FQDN).

Valeur par défaut

<vide>

Description

L'iDRAC6 utilise la valeur que vous avez spécifiée pour rechercher des noms d'utilisateur sur le serveur de catalogue global.

cfgADCertValidationEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

1

Description

Active ou désactive la validation du certificat Active Directory dans le cadre du processus de configuration d'Active Directory.

---

cfgStandardSchema

Ce groupe contient les paramètres qui permettent de configurer les paramètres du schéma standard d'Active Directory.

cfgSSADRoleGroupIndex (lecture seule)

Valeurs valides

Un nombre entier compris entre 1 et 5.

Valeur par défaut

<instance>

Description

Index du groupe de rôles tel qu'enregistré dans Active Directory

cfgSSADRoleGroupName (lecture/écriture)

Valeurs valides

Toute chaîne de texte imprimable incluant jusqu'à 254 caractères.

Valeur par défaut

<vide>

Description

Nom du groupe de rôles tel qu'enregistré dans la forêt Active Directory.

cfgSSADRoleGroupDomain (lecture/écriture)

Valeurs valides

Une chaîne de texte imprimable contenant jusqu'à 254 caractères, avec ou sans espace.

Valeur par défaut

<vide>

Description

Domaine Active Directory où se trouve le groupe de rôles.

cfgSSADRoleGroupPrivilege (lecture/écriture)

Valeurs valides

0x00000000 à **0x000001ff**

Valeur par défaut

<vide>

Description

Utilisez les nombres de masque binaire dans le Tableau B-4 pour définir les privilèges d'autorité basés sur les rôles pour un groupe de rôles.

Tableau B-4. Masques binaires pour des privilèges de groupes de rôles

Privilège Groupe de rôles	Masque binaire
Ouvrir une session iDRAC	0x00000001
Configurer iDRAC	0x00000002
Configurer les utilisateurs	0x00000004
Effacer les journaux	0x00000008
Exécuter les commandes de contrôle du serveur	0x00000010
Accéder à la redirection de console	0x00000020
Accéder au média virtuel	0x00000040
Tester les alertes	0x00000080
Exécuter les commandes de débogage	0x00000100

---

cfgIpmiSol

Ce groupe est utilisé pour configurer les capacités SOL (communications série sur le LAN) du système.

cfgIpmiSolEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

1

Description

Active ou désactive les communications série sur le LAN.

cfgIpmiSolBaudRate (lecture/écriture)

Valeurs valides

9600, 19200, 57600, 115200

Valeur par défaut

115200

Description

Débit en bauds pour les communications série sur le LAN.

cfgIpmiSolMinPrivilege (lecture/écriture)

Valeurs valides

2 (utilisateur)

3 (opérateur)

4 (administrateur)

Valeur par défaut

4

Description

Spécifie le niveau de privilège minimum requis en vue de l'accès SOL.

cfgIpmiSolAccumulateInterval (lecture/écriture)

Valeurs valides

1 - 255

Valeur par défaut

10

Description

Spécifie le temps d'attente type de l'iDRAC avant de transmettre un paquet de données de caractères SOL partiel. Cette valeur est basée sur des incréments de 5 ms.

cfgIpmiSolSendThreshold (lecture/écriture)

Valeurs valides

1 - 255

Valeur par défaut

255

Description

Valeur seuil SOL. Spécifie le nombre maximum d'octets à mettre en mémoire tampon avant d'envoyer un paquet de données SOL.

---

cfgIpmiLan

Ce groupe est utilisé pour configurer les capacités IPMI sur le LAN du système.

cfgIpmiLanEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Active ou désactive l'interface IPMI sur le réseau local.

cfgIpmiLanPrivilegeLimit (lecture/écriture)

Valeurs valides

2 (utilisateur)

3 (opérateur)

4 (administrateur)

Valeur par défaut

4

Description

Spécifie le niveau de privilège maximum autorisé pour l'accès IPMI sur le réseau local.

cfgIpmiLanAlertEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Active ou désactive les alertes globales par e-mail. Cette propriété remplace toutes les propriétés individuelles d'activation/de désactivation d'alertes par e-mail.

cfgIpmiEncryptionKey (lecture/écriture)

Valeurs valides

Chaîne de chiffres hexadécimaux de 0 à 40 caractères sans espace. Seule une quantité égale de caractères est autorisée.

Valeur par défaut

00000000000000000000

Description

Clé de cryptage IPMI.

cfgIpmiPetCommunityName (lecture/écriture)

Valeurs valides

Chaîne allant jusqu'à 18 caractères.

Valeur par défaut

public

Description

Nom de communauté SNMP pour les interruptions.

---

cfgIpmiPetIpv6

Ce groupe est utilisé pour configurer des interruptions d'événements sur plate-forme IPv6 d'un serveur géré.

cfgIpmiPetIPv6Index (lecture seule)

Valeurs valides

1 - 4

Valeur par défaut

<valeur de l'index>

Description

Identifiant unique pour l'index correspondant à l'interruption.

cfgIpmiPetIPv6AlertDestIpAddr

Valeurs valides

Adresse IPv6

Valeur par défaut

<vide>

Description

Configure l'adresse IP de destination des alertes IPv6 pour l'interruption.

cfgIpmiPetIPv6AlertEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Active ou désactive la destination des alertes IPv6 pour l'interruption.

---

cfgIpmiPef

Ce groupe est utilisé pour configurer les filtres d'événements sur plate-forme disponibles sur le serveur géré.

Les filtres d'événements peuvent être utilisés pour contrôler les règles associées aux actions qui sont déclenchées lorsque des événements critiques se produisent sur le serveur géré.

cfgIpmiPefName (lecture seule)

Valeurs valides

Chaîne de 255 caractères maximum.

Valeur par défaut

Nom du filtre d'index

Description

Spécifie le nom du filtre d'événements sur plate-forme.

cfgIpmiPefIndex (lecture/écriture)

Valeurs valides

1 – 19

Valeur par défaut

Valeur d'index d'un objet de filtre d'événements sur plate-forme.

Description

Spécifie l'index d'un filtre d'événements sur plate-forme spécifique.

cfgIpmiPefAction (lecture/écriture)

Valeurs valides

0 (aucun)

1 (mise hors tension)

2 (réinitialisation)

3 (cycle d'alimentation)

Valeur par défaut

0

Description

Spécifie l'action qui est effectuée sur le serveur géré lorsque l'alerte est déclenchée.

cfgIpmiPefEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

1

Description

Active ou désactive un filtre d'événements sur plate-forme spécifique.

---

cfgIpmiPet

Ce groupe est utilisé pour configurer des interruptions d'événements sur plateforme d'un serveur géré.

cfgIpmiPetIndex (lecture seule)

Valeurs valides

1 - 4

Valeur par défaut

La valeur de l'index d'une interruption d'événements de plate-forme spécifique.

Description

Identifiant unique pour l'index correspondant à l'interruption.

cfgIpmiPetAlertDestIpAddr (lecture/écriture)

Valeurs valides

Chaîne de caractères représentant une adresse IPv4 valide. Par exemple, `192.168.0.67`.

Valeur par défaut

0.0.0.0

Description

Spécifie l'adresse IPv4 de destination pour le récepteur d'interruption sur le réseau. Le récepteur d'interruption reçoit une interruption SNMP lorsqu'un événement est déclenché sur le serveur géré.

cfgIpmiPetAlertEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Active ou désactive une interruption spécifique.

---

cfgUserDomain

Ce groupe est utilisé pour configurer les noms de domaine utilisateur Active Directory. Un maximum de 40 noms de domaine peuvent être configurés simultanément.

cfgUserDomainIndex (lecture seule)

Valeurs valides

1 – 40

Valeur par défaut

La valeur de l'index

Description

Représente un domaine spécifique.

cfgUserDomainName (lecture seule)

Valeurs valides

Chaîne de 255 caractères ASCII maximum.

Valeur par défaut

<vide>

Description

Spécifie le nom de domaine utilisateur Active Directory.

---

cfgServerPower

Ce groupe fournit plusieurs fonctionnalités de gestion de l'alimentation.

cfgServerPowerStatus (lecture seule)

Valeurs valides

1 (ON)

0 (OFF)

Valeur par défaut

<état d'alimentation actuel du serveur>

Description

Représente l'état d'alimentation du serveur (ON ou OFF)

cfgServerPowerAllocation (lecture seule)

REMARQUE : Dans le cas de plusieurs blocs d'alimentation, cette propriété représente le bloc d'alimentation de moindre capacité.

Valeurs valides

Chaîne de 32 caractères maximum.

Valeur par défaut

<vide>

Description

Représente le bloc d'alimentation disponible attribué pour utiliser le serveur.

cfgServerActualPowerConsumption (lecture seule)

Valeurs valides

Chaîne de 32 caractères maximum.

Valeur par défaut

<vide>

Description

Représente la consommation électrique actuelle du serveur.

cfgServerMinPowerCapacity (lecture seule)

Valeurs valides

Chaîne de 32 caractères maximum.

Valeur par défaut

<vide>

Description

Représente la capacité d'alimentation minimale du serveur.

cfgServerMaxPowerCapacity (lecture seule)

Valeurs valides

Chaîne de 32 caractères maximum.

Valeur par défaut

<vide>

Description

Représente la capacité d'alimentation maximum du serveur.

cfgServerPeakPowerConsumption (lecture seule)

Valeurs valides

Chaîne de 32 caractères maximum.

Valeur par défaut

<consommation énergétique maximale actuelle du serveur>

Description

Représente la consommation électrique maximale du serveur jusqu'à présent.

cfgServerPeakPowerConsumptionTimestamp (lecture seule)

Valeurs valides

Chaîne de 32 caractères maximum.

Valeur par défaut

Horodatage de la consommation énergétique maximale

Description

Heure à laquelle le pic de consommation électrique a été enregistré.

cfgServerPowerConsumptionClear (lecture seule)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

****

Description

Réinitialise la propriété cfgServerPeakPowerConsumption (lecture/écriture) sur 0 et la propriété cfgServerPeakPowerConsumptionTimestamp sur l'heure actuelle sur l'iDRAC.

cfgServerPowerCapWatts (lecture/écriture)

Valeurs valides

Chaîne de 32 caractères maximum.

Valeur par défaut

Seuil énergétique du serveur en Watts.

Description

Représente le seuil énergétique du serveur en Watts.

cfgServerPowerCapBtuhr (lecture/écriture)

Valeurs valides

Chaîne de 32 caractères maximum.

Valeur par défaut

Seuil énergétique du serveur en BTU/h.

Description

Représente le seuil énergétique du serveur en BTU/h.

cfgServerPowerCapPercent (lecture/écriture)

Valeurs valides

Chaîne de 32 caractères maximum.

Valeur par défaut

Seuil énergétique du serveur en pourcentage.

Description

Représente le seuil énergétique du serveur en pourcentage.

---

cfgIPv6LanNetworking

Ce groupe est utilisé pour configurer les capacités IPv6 de mise en réseau sur le réseau local.

cfgIPv6Enable

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Active ou désactive l'adresse IPv6 de l'iDRAC.

cfgIPv6Address1 (lecture/écriture)

Valeurs valides

Chaîne de caractères représentant une entrée IPv6 valide.

Valeur par défaut

::

Description

Adresse IPv6 de l'iDRAC.

cfgIPv6Gateway (lecture/écriture)

Valeurs valides

Chaîne de caractères représentant une entrée IPv6 valide.

Valeur par défaut

::

Description

Adresse IPv6 de la passerelle de l'iDRAC.

cfgIPv6PrefixLength (lecture/écriture)

Valeurs valides

1-128

Valeur par défaut

64

Description

Longueur de préfixe pour l'adresse IPv6 de l'iDRAC.

cfgIPv6AutoConfig (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

1

Description

Active ou désactive l'option Auto Config IPv6

cfgIPv6LinkLocalAddress (lecture seule)

Valeurs valides

Chaîne de caractères représentant une entrée IPv6 valide.

Valeur par défaut

::

Description

Adresse locale de lien IPv6 de l'iDRAC.

cfgIPv6Address2 (lecture seule)

Valeurs valides

Chaîne de caractères représentant une entrée IPv6 valide.

Valeur par défaut

::

Description

Adresse IPv6 de l'iDRAC.

cfgIPv6DNSServersFromDHCP6 (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Spécifie si cfgIPv6DNSServer1 et cfgIPv6DNSServer2 sont statiques ou des adresses IPv6 du DHCP.

cfgIPv6DNSServer1 (lecture/écriture)

Valeurs valides

Chaîne de caractères représentant une entrée IPv6 valide.

Valeur par défaut

::

Description

Adresse IPV6 du serveur DNS.

cfgIPv6DNSServer2 (lecture/écriture)

Valeurs valides

Chaîne de caractères représentant une entrée IPv6 valide.

Valeur par défaut

::

Description

Adresse IPV6 du serveur DNS.

---

cfgIPv6URL

Ce groupe spécifie les propriétés utilisées pour configurer l'adresse URL IPv6 de l'iDRAC.

cfgIPv6URLstring (lecture seule)

Valeurs valides

Chaîne de 80 caractères maximum.

Valeur par défaut

<vide>

Description

Adresse URL IPv6 de l'iDRAC.

---

cfgIpmiSerial

Ce groupe spécifie les propriétés utilisées pour configurer l'interface série IPMI du BMC.

cfgIpmiSerialConnectionMode (lecture/écriture)

Valeurs valides

0 (terminal)

1 (de base)

Valeur par défaut

1

Description

Lorsque la propriété **cfgSerialConsoleEnable** de l'iDRAC est définie sur 0 (désactivé), le port série de l'iDRAC devient le port série IPMI. Cette propriété détermine le mode défini IPMI du port série.

En mode de base, le port utilise des données binaires dans l'intention de communiquer avec un logiciel d'application sur le client série. En mode terminal, le port suppose qu'un terminal ASCII passif est connecté et permet la saisie de commandes très simples.

cfgIpmiSerialBaudRate (lecture/écriture)

Valeurs valides

9600, 19200, 57600, 115200

Valeur par défaut

57600

Description

Spécifie le débit en bauds pour une connexion série sur IPMI.

cfgIpmiSerialChanPrivLimit (lecture/écriture)

Valeurs valides

2 (utilisateur)

3 (opérateur)

4 (administrateur)

Valeur par défaut

4

Description

Spécifie le niveau de privilège maximum autorisé sur le canal série IPMI.

cfgIpmiSerialFlowControl (lecture/écriture)

Valeurs valides

0 (aucun)

1 (CTS/RTS)

2 (XON/XOFF)

Valeur par défaut

1

Description

Spécifie le paramètre de contrôle du débit pour le port série IPMI.

cfgIpmiSerialHandshakeControl (lecture/écriture)

Valeurs valides

0 (FAUX)

1 (VRAI)

Valeur par défaut

1

Description

Active ou désactive le contrôle de liaison du mode terminal IPMI.

cfgIpmiSerialLineEdit (lecture/écriture)

Valeurs valides

0 (FAUX)

1 (VRAI)

Valeur par défaut

1

Description

Active ou désactive la modification de ligne sur l'interface série IPMI.

cfgIpmiSerialEchoControl (lecture/écriture)

Valeurs valides

0 (FAUX)

1 (VRAI)

Valeur par défaut

1

Description

Active ou désactive le contrôle d'écho sur l'interface série IPMI.

cfgIpmiSerialDeleteControl (lecture/écriture)

Valeurs valides

0 (FAUX)

1 (VRAI)

Valeur par défaut

0

Description

Active ou désactive la commande de suppression sur l'interface série IPMI.

cfgIpmiSerialNewLineSequence (lecture/écriture)

Valeurs valides

0 (aucun)

1 (CR-LF)

2 (NULL)

3 (<CR>)

4 (<LF-CR>)

5 (<LF>)

Valeur par défaut

1

Description

Spécifie l'ordre de saut de ligne pour l'interface série IPMI.

cfgIpmiSerialInputNewLineSequence (lecture/écriture)

Valeurs valides

0 (<ENTRÉE>)

1 (NULL)

Valeur par défaut

1

Description

Spécifie l'ordre de saisie de saut ligne pour l'interface série IPMI.

---

cfgSmartCard

Ce groupe spécifie les propriétés utilisées pour prendre en charge l'accès à l'iDRAC au moyen d'une carte à puce.

cfgSmartCardLogonEnable (lecture/écriture)

Valeurs valides

0 (désactivé)

1 (activé)

2 (Activé avec la RACADM à distance)

Valeur par défaut

0

Description

Active, désactive ou active avec la prise en charge de la RACADM à distance pour l'accès à l'iDRAC au moyen d'une carte à puce.

cfgSmartCardCRLEnable (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

0

Description

Active ou désactive la liste de révocation de certificat (CRL)

---

cfgNetTuning

Ce groupe permet aux utilisateurs de configurer les paramètres d'interface réseau avancés pour le NIC du RAC. Une fois configurés, les paramètres mis à jour peuvent prendre jusqu'à une minute pour devenir actifs.

△ **PRÉCAUTION : Soyez extrêmement prudent lorsque vous modifiez les propriétés dans ce groupe. Une modification inappropriée des propriétés de ce groupe peut rendre le NIC du RAC inopérable.**

cfgNetTuningNicAutoneg (lecture/écriture)

Valeurs valides

1 (VRAI)

0 (FAUX)

Valeur par défaut

1

Description

Active la négociation automatique de la vitesse du lien physique et du duplex. Lorsqu'elle est activée, l'autonégociation a la priorité sur les valeurs définies dans les objets **cfgNetTuningNic100MB** et **cfgNetTuningNicFullDuplex**.

cfgNetTuningNic100MB (lecture/écriture)

Valeurs valides

0 (10 Mb)

1 (100 Mb)

Valeur par défaut

1

Description

Spécifie la vitesse à utiliser pour le NIC du RAC. Cette propriété n'est pas utilisée si **cfgNetTuningNicAutoNeg** est défini sur **1** (activé).

cfgNetTuningNicFullDuplex (lecture/écriture)

Valeurs valides

0 (demi-duplex)

1 (duplex intégral)

Valeur par défaut

1

Description

Spécifie le paramètre duplex pour le NIC du RAC. Cette propriété n'est pas utilisée si **cfgNetTuningNicAutoNeg** est défini sur **1** (activé).

cfgNetTuningNicMtu (lecture/écriture)

Valeurs valides

576 – 1 500

Valeur par défaut

1 500

Description

La taille en octets de l'unité de transmission maximale utilisée par le NIC de l'iDRAC.

Retour á la page du sommaire

Retour á la page du sommaire

Interfaces RACADM prises en charge

Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.1

Le tableau suivant présente les sous-commandes RACADM et leur prise en charge d'interface correspondante.

Tableau C-1. Prise en charge d'interface de sous-commande RACADM

Sous-commande	Telnet/SSH/Série	RACADM locale	RACADM distant
arp	✔	✘	✔
clearasrscreen	✔	✔	✔
clrraclog	✔	✔	✔
clrsel	✔	✔	✔
coredump	✔	✘	✔
coredumpdelete	✔	✔	✔
fwupdate	✔	✔	✔
getconfig	✔	✔	✔
getniccfg	✔	✔	✔
getraclog	✔	✔	✔
getractime	✔	✔	✔
getsel	✔	✔	✔
getssninfo	✔	✔	✔
getsvctag	✔	✔	✔
getsysinfo	✔	✔	✔
gettracelog	✔	✔	✔
help	✔	✔	✔
ifconfig	✔	✘	✔
netstat	✔	✘	✔
ping	✔	✘	✔
racdump	✔	✘	✔
racreset	✔	✔	✔
racresetcfg	✔	✔	✔
serveraction	✔	✔	✔
setniccfg	✔	✔	✔
sslcertdownload	✘	✔	✔
sslcertupload	✘	✔	✔
sslcertview	✔	✔	✔
sslcsrgen	✘	✔	✔
sslkeyupload	✘	✔	✔
testemail	✔	✔	✔
testtrap	✔	✔	✔
vmdisconnect	✔	✔	✔
vmkey	✔	✔	✔
usercertupload	✘	✔	✔
usercertview	✔	✔	✔
localConRedirDisable	✘	✔	✘
✔ = Prise en charge ; ✘ = Non prise en charge			

Retour á la page du sommaire

Retour á la page du sommaire

Présentation d'iDRAC6

Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.1

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™.

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

Vous pouvez configurer l'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 blocage du système, l'iDRAC6 peut consigner des données d'événement et capturer une image de l'écran lorsqu'il détecte un blocage 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 l'iDRAC6. Une fois l'iDRAC6 configuré sur le réseau, il est accessible sur l'adresse IP qui lui a été attribuée via 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).

Fonctions de gestion d'iDRAC6 Express

L'iDRAC6 Express fournit les fonctions de gestion suivantes :

- Enregistrement de système de noms de domaine dynamique (DDNS)
- Gestion et surveillance à distance du système à l'aide d'une interface Web et de la ligne de commande SM-CLP sur une connexion série Telnet ou SSH
- 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 standard ou étendu
- Surveillance : permet d'accéder aux informations sur le système et à la condition des composants
- Accès aux journaux système : permet d'accéder au journal d'événements système, au journal iDRAC6 et à l'écran du dernier blocage du système fermé subitement ou sans réponse qui est indépendant de l'état du système d'exploitation
- Intégration du logiciel Dell OpenManage™ : vous permet de lancer l'interface Web iDRAC6 à partir de Dell OpenManage Server Administrator ou d'IT Assistant
- Alerte iDRAC6 : avertit des problèmes potentiels du nud géré au moyen d'un message électronique ou d'une interruption SNMP
- Gestion de l'alimentation à distance : fournit des fonctionnalités de gestion de l'alimentation à distance, comme l'arrêt et la réinitialisation, à partir d'une console de gestion
- Prise en charge d'interface de gestion de plateforme intelligente (IPMI)
- Cryptage SSL (Secure Sockets Layer) : permet une gestion sécurisée du système à distance via l'interface Web
- Gestion de la sécurité de niveau mot de passe : empêche tout accès non autorisé à un système distant.
- Autorisation basée sur le rôle : permet d'attribuer des droits pour diverses tâches de gestion de systèmes
- Prise en charge IPv6 : ajoute la prise en charge IPv6 pour accéder à l'interface Web iDRAC6 à l'aide d'une adresse IPv6, spécifie l'adresse IPv6 pour le NIC iDRAC6 et spécifie un numéro de destination pour configurer une destination d'alerte SNMP IPv6.
- Prise en charge WS-MAN : Assure une gestion accessible par réseau en utilisant le protocole WS-MAN (Web Services for Management).
- Prise en charge SM-CLP : ajoute la prise en charge du protocole SM-CLP (Server Management-Command Line Protocol), qui fournit des standards pour les implémentations de CLI de gestion de système.
- Restauration et récupération du micrologiciel : vous permet de démarrer à partir de l'image de micrologiciel de votre choix ou de la restaurer.

Pour plus d'informations sur iDRAC6 Express, consultez le *Manuel du propriétaire* à l'adresse **support.dell.com\manuals**.

---

iDRAC6 Enterprise et vFlash Media

Ajoute la prise en charge RACADM, KVM virtuel, des fonctionnalités de support virtuel, un NIC dédié et un Flash virtuel (avec la carte Dell vFlash Media en option). Le disque Flash virtuel vous permet de stocker des images d'amorçage d'urgence et les outils de diagnostic sur la carte vFlash Media. Pour plus d'informations sur iDRAC6 Enterprise et vFlash Media, consultez le *Manuel du propriétaire* à l'adresse **support.dell.com\manuals**.

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

Tableau 1-1. Liste de fonctionnalités iDRAC6

Fonctionnalité	BMC	iDRAC6 Express	iDRAC6 Enterprise	vFlash Media

Prise en charge de l'interface et des normes				
IPMI 2.0	✔	✔	✔	✔
GUI Web	✘	✔	✔	✔
SNMP	✘	✔	✔	✔
WSMAN	✘	✔	✔	✔
SMASH-CLP	✘	✔	✔	✔
Ligne de commande RACADM	✘	✘	✔	✔
Conductibilité				
Modes réseau Partagé/Basculement	✔	✔	✔	✔
IPv4	✔	✔	✔	✔
Marquage VLAN	✔	✔	✔	✔
IPv6	✘	✔	✔	✔
DNS dynamique	✘	✔	✔	✔
NIC dédié	✘	✘	✔	✔
Sécurité et authentification				
Autorité basée sur le rôle	✔	✔	✔	✔
Utilisateurs locaux	✔	✔	✔	✔
Active Directory	✘	✔	✔	✔
Authentification bifactorielle	✘	✔	✔	✔
Ouverture de session individuelle	✘	✔	✔	✔
Cryptage SSL	✔	✔	✔	✔
Gestion et conversion distantes				
Mise à jour de micrologiciels distante	✔ [1]	✔	✔	✔
Contrôle de l'alimentation du serveur	✔ [1]	✔	✔	✔
Série sur le LAN (avec proxy)	✔	✔	✔	✔
Série sur le LAN (sans proxy)	✘	✔	✔	✔
Plafonnement de l'alimentation	✘	✔	✔	✔
Capture d'écran de la dernière panne	✘	✔	✔	✔
Capture d'amorçage	✘	✔	✔	✔
Média virtuel	✘	✘	✔	✔
Console virtuelle	✘	✘	✔	✔
Partage de la console virtuelle	✘	✘	✔	✔
Disque flash virtuel	✘	✘	✘	✔
Analyse				
Surveillance et alertes des capteurs	✔ [1]	✔	✔	✔
Surveillance 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.	✘	✔	✔	✔
Journal de suivi	✘	✔	✔	✔
[1] : La fonctionnalité est disponible uniquement via IPMI et non via une GUI Web				
✔ = Pris en charge ; ✘ = Non pris en charge				

L'iDRAC6 dispose des fonctionnalités de sécurité suivantes :

- Authentification des utilisateurs via Active Directory (en option) ou via les ID d'utilisateur et les mots de passe stockés sur le matériel
- Autorité basée sur le rôle 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 prenant en charge le cryptage 128 bits et 40 bits (dans les pays où le cryptage 128 bits n'est pas accepté) à l'aide de 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.

- Secure Shell (SSH) qui utilise une couche de transport cryptée pour une sécurité plus élevée
- Nombre maximal 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 sur iDRAC6
- Authentification par carte à puce

Plates-formes prises en charge

Pour connaître les dernières plates-formes prises en charge, consultez le fichier « Lisez-moi » d'iDRAC6 et la *matrice de prise en charge des logiciels Dell* disponibles à l'adresse **support.dell.com\manuals** et sur le DVD *Dell Systems Management Tools and Documentation* fourni avec votre système.

Systèmes d'exploitation pris en charge

Pour accéder aux dernières informations, consultez le fichier « Lisez-moi » d'iDRAC6 et la *matrice de prise en charge des logiciels Dell* disponibles à l'adresse **support.dell.com\manuals** et sur le DVD *Dell Systems Management Tools and Documentation* fourni avec votre système.

Navigateurs Web pris en charge

Pour accéder aux dernières informations, consultez le fichier « Lisez-moi » d'iDRAC6 et la *matrice de prise en charge des logiciels Dell* disponibles à l'adresse **support.dell.com\manuals** et sur le DVD *Dell Systems Management Tools and Documentation* fourni avec votre système.

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.

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
BIC iDRAC6	- 10 Mbits/s/100 Mbits/s/Ethernet - Prise en charge de DHCP - Interruptions SNMP et notifications d'événements par e-mail - Prise en charge de l'environnement de commande SM-CLP (Telnet ou SSH) pour les opérations telles que la configuration iDRAC6, le démarrage système, la réinitialisation, la mise sous tension et les commandes d'arrêt - 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 iDRAC6.

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

Numéro de port	Fonction
22*	SSH
23*	Telnet
80*	HTTP
443*	HTTPS
623	RMCP/RMCP+
5900*	Clavier/Souris de la redirection de console, Service de média virtuel, Service de média virtuel sécurisé, Vidéo de la redirection de console
* Port configurable	

Tableau 1-4. Ports de client iDRAC6

Numéro de port	Fonction
25	SMTP
53	DNS
68	Adresse IP DHCP
69	TFTP
162	interruption SNMP
636	LDAPS
3269	LDAPS pour le catalogue global (GC)

Autres documents utiles

En plus de ce *Guide d'utilisation*, les documents suivants fournissent des informations supplémentaires sur la configuration et l'utilisation d'iDRAC6 dans votre système : Ces documents sont disponibles sur le site Web du support de Dell à l'adresse **support.dell.com\manuals**.

- L'aide en ligne d'iDRAC6 fournit des informations détaillées sur l'utilisation de l'interface Web.
- Le *Guide d'utilisation de Dell Unified Server Configurator* fournit des informations sur le matériel iDRAC et la configuration des services système.
- Le *Guide d'utilisation de Dell OpenManage IT Assistant* fournit des informations relatives à l'utilisation d'IT Assistant.
- Pour installer un iDRAC6, consultez votre *Manuel du propriétaire*.
- Le *Guide d'utilisation de Dell OpenManage Server Administrator* donne des informations sur l'installation et l'utilisation de Server Administrator.
- Pour connaître les dernières plates-formes, les derniers systèmes d'exploitation et navigateurs Web pris en charge, consultez le fichier « Lisez-moi » d'iDRAC6 et la *matrice de prise en charge des logiciels Dell*.
- Le *Guide d'utilisation des progiciels Dell Update Package* fournit des informations sur l'obtention et l'utilisation des progiciels Dell Update Package dans le contexte de la stratégie de mise à jour de votre système.
- Consultez le *Guide d'utilisation des utilitaires de contrôleur BMC Dell OpenManage* pour des informations sur iDRAC6 et l'interface IPMI.

En outre, la documentation système suivante fournit des informations supplémentaires sur le système sur lequel iDRAC6 est installé :

- les instructions de sécurité fournies avec votre système contiennent d'importantes informations se rapportant à la sécurité et aux réglementations. Pour obtenir des informations supplémentaires sur la réglementation, voir la page d'accueil Regulatory Compliance (conformité à la réglementation) à l'adresse **www.dell.com/regulatory_compliance**. Les informations sur la garantie se trouvent dans ce document ou dans un document distinct.
- Les *Instructions d'installation en rack*, fournies avec le rack, indiquent comment installer le système en rack.
- Le *Guide de mise en route* présente les caractéristiques du système, les procédures de configuration et les spécifications techniques.
- Le document *Hardware Owner's Manual* (Manuel du propriétaire) présente les caractéristiques du système et contient des informations de dépannage et des instructions d'installation ou de remplacement des composants.
- La documentation relative aux logiciels de gestion du système contient des informations sur les fonctionnalités, l'installation et l'utilisation de base de ces logiciels, ainsi que sur la configuration requise.
- 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 installer et configurer ces options.
- Des mises à jour sont parfois fournies avec le système. Elles décrivent les modifications apportées au système, aux logiciels ou à la documentation.

  REMARQUE : Lisez toujours ces mises à jour en premier, car elles remplacent souvent les informations contenues dans les autres documents.

- Si des notes de version ou des fichiers lisez-moi (readme) sont fournis, ils contiennent des mises à jour de dernière minute apportées au système ou à la documentation ou bien des informations techniques destinées aux utilisateurs expérimentés ou aux techniciens.

Retour á la page du sommaire

Retour á la page du sommaire

Démarrage de l'iDRAC6

Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.1

L'iDRAC6 vous permet de surveiller, dépanner et réparer à distance un système Dell, même lorsque celui-ci est en panne. L'iDRAC6 est doté d'une grande richesse de fonctionnalités incluant la redirection de console, le média virtuel, le KVM virtuel, l'authentification par carte à puce et l'ouverture de session individuelle.

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

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

Pour configurer l'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 de support de Dell à l'adresse **support.dell.com \ manuals** pour des instructions précises sur la réalisation de cette procédure.

1. Configurez les propriétés, les paramètres réseau et les utilisateurs de l'iDRAC6 : vous pouvez configurer l'iDRAC6 à l'aide de l'utilitaire de configuration de l'iDRAC6, de l'interface Web ou de la RACADM.
2. Si vous utilisez un système Windows, configurez Microsoft® Active Directory® pour accéder à l'iDRAC6 afin de pouvoir ajouter et contrôler les privilèges d'utilisateur de l'iDRAC6 de vos utilisateurs existants dans votre logiciel Active Directory.
3. 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 redirection de console et le média virtuel.
5. Configurez les paramètres de sécurité.
6. Configurez les alertes pour une gestion efficace des systèmes.
7. Configurez les paramètres de l'interface de gestion de plateforme intelligente de iDRAC6 (IPMI) pour utiliser les outils IPMI standardisés pour gérer les systèmes sur votre réseau.

Retour á la page du sommaire

Retour á la page du sommaire

Installation de base de l'iDRAC6

Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.1

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

Avant de commencer

Rassemblez les éléments suivants, fournis avec votre système, avant d'installer et de configurer le logiciel de l'iDRAC6 :

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

Installation de la carte iDRAC6 Express/Enterprise

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

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

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

Configuration du système pour utiliser un iDRAC6

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

Pour exécuter l'utilitaire de configuration iDRAC6 :

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

   Si le système d'exploitation commence à se charger alors que vous n'avez pas encore appuyé sur <Ctrl><E>, laissez-le terminer, puis redémarrez et réessayez.
3. Configurez le LOM.
   a. À l'aide des touches de direction, sélectionnez Paramètres LAN, puis appuyez sur <Entrée>. La page Sélection de NIC est affichée.
   b. À l'aide des touches de direction, 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 l'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.
      - **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 complètement fonctionnelle lorsque 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 est défectueux, 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 complètement fonctionnelle lorsque 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 transmettre toutes les 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 complètement fonctionnelle lorsque le système d'exploitation hôte est configuré pour le regroupement de NIC. Le périphérique d'accès à distance reçoit des données via les NIC 1, NIC 2, NIC 3 et NIC 4, mais transmet des données seulement via le NIC 1. Si le NIC 1 échoue, le périphérique d'accès à distance rebascule l'intégralité de la transmission des données sur le NIC 2. Si le NIC 2 échoue, le périphérique d'accès à distance rebascule l'intégralité de la transmission des

données sur le NIC 3. Si le NIC 3 échoue, le périphérique d'accès à distance rebascule l'intégralité de la transmission des données sur le NIC 4. Si le NIC 4 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. Il se peut que cette option ne soit pas disponible sur iDRAC6 Enterprise.

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 Ethernet**, **Masque de sous-réseau** et **Passerelle par défaut**.
   e. Appuyez sur <Échap>.
5. Appuyez sur <Échap>.
6. Sélectionnez **Enregistrer les modifications 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 logiciels de l'iDRAC6, voir « Installation du logiciel sur le système géré ».

Installation du logiciel iDRAC6

Pour installer le logiciel iDRAC6 :

1. Installez le logiciel sur le système géré. Consultez « Installation du logiciel sur le système géré ».
2. Installez le logiciel sur la station de gestion. Consultez « Installation du logiciel sur le système géré ».

Configuration de l'iDRAC6

Pour configurer l'iDRAC6 :

1. Sélectionnez l'un des outils de configuration suivants :
   - Interface Web : (voir « Configuration de l'iDRAC6 via l'interface Web »).
   - CLI RACADM : (voir « Utilisation de l'interface de ligne de commande SM-CLP iDRAC6 »).
   - Console Telnet : (voir « Utilisation d'une console Telnet »).

   REMARQUE : L'utilisation simultanée de plusieurs outils de configuration iDRAC6 peut provoquer des résultats inattendus.
2. Configurez les paramètres réseau iDRAC6. Consultez « Configuration des paramètres réseau de l'iDRAC6 ».
3. Ajout et configuration d'utilisateurs iDRAC6 Consultez « Ajout et configuration d'utilisateurs iDRAC6 ».
4. Configurez le navigateur Web pour accéder à l'interface Web. Consultez « Configuration d'un navigateur Web pris en charge ».
5. Désactivez l'option de redémarrage automatique de Microsoft® Windows®. Consultez « Désactivation de l'option Redémarrage automatique de Windows ».
6. Mettez à jour le micrologiciel iDRAC6. Consultez « Mise à jour du micrologiciel iDRAC6 ».

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 le DRAC 6 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, consultez votre *Guide d'installation rapide* 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 voir l'écran de la dernière panne du système ou utiliser la fonctionnalité **Récupération automatique**.

Pour plus d'informations sur l'écran de la dernière panne, voir « Affichage de l'écran de la dernière panne système ».

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 logiciels de gestion des systèmes, dont Dell OpenManage Server Administrator
- Docs : contient la documentation pour les logiciels de gestion de systèmes, les périphériques et les contrôleurs RAID
- SERVICE : contient les outils nécessaires pour configurer le système ainsi que les tout derniers outils de diagnostic et pilotes optimisés par Dell pour votre système

Pour plus d'informations, consultez le *Guide d'utilisation de Server Administrator*, le *Guide d'utilisation d'IT Assistant* et le *Guide d'utilisation d'Unified Server Configurator* disponibles sur le site Web du support de Dell à l'adresse **support.dell.com\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 où vous voulez installer les composants de Management Station.
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. Accédez au 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 lancé 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 :

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

Mise à jour du micrologiciel iDRAC6

Utilisez l'une des méthodes suivantes pour mettre le micrologiciel de votre iDRAC6.

- Interface Web : (voir « Mise à jour du micrologiciel iDRAC6 via l'interface Web »).
- CLI RACADM : (voir « Mise à jour du micrologiciel iDRAC6 via RACADM »).
- Progiciels Dell Update : (voir « Mise à jour du micrologiciel iDRAC6 à l'aide des progiciels de mise à jour Dell pour les systèmes d'exploitation Windows et Linux pris en charge »).

Avant de commencer

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

1. Installez et activez les pilotes IPMI et de nuds gérés 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 sur un système sous SUSE® Linux Enterprise Server (version 10) pour Intel® EM64T, démarrez le **service.**
4. Débranchez et démontez le média virtuel.

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

5. Assurez-vous que USB est activé.

Téléchargement du micrologiciel iDRAC6

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

Le package du micrologiciel iDRAC6 se compose des éléments 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 via l'interface Web

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

Mise à jour du micrologiciel iDRAC6 via RACADM

Vous pouvez mettre à jour le micrologiciel iDRAC6 à l'aide de l'outil CLI RACADM. 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 sur le site Web de 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 de l'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.

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

Téléchargez et exécutez les progiciels de mise à jour Dell pour les systèmes d'exploitation Windows et Linux pris en charge sur le site Web Dell à l'adresse **support.dell.com**. Pour plus d'informations, reportez-vous au *Guide de l'utilisateur Dell OpenManage System Administrator*, disponible sur le site de support 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 peuvent être ignorées. Ces messages sont dus à la réinitialisation des périphériques USB au cours de la mise à jour du micrologiciel et sont inoffensifs.

Suppression de la mémoire cache du navigateur

Après la mise à niveau du micrologiciel, supprimez la mémoire cache du navigateur Web.

Consultez l'aide en ligne de votre navigateur Web pour plus d'informations.

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**, cliquez sur **Paramètres réseau**.
5. Si la case **Utiliser un serveur proxy** est cochée, sélectionner la case **Ne pas utiliser de serveur proxy pour les adresses locales**.
6. Cliquez deux fois sur **OK**.

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 redémarrez le navigateur Web pour rétablir une connexion à l'interface Web iDRAC6.

Navigateurs Web 32 bits et 64 bits

L'interface Web iDRAC6 n'est pas prise en charge sur les navigateurs 64 bits. Si vous ouvrez un navigateur 64 bits, accédez à la page Redirection de console et essayez d'installer le plug-in, la procédure d'installation échoue. Si cette erreur n'a pas été reconnue et que vous répétez cette procédure, la page Redirection de console se charge bien que l'installation du plug-in ait échoué pendant votre première tentative. Ce problème se produit parce que le navigateur Web enregistre les informations du plug-in dans le répertoire du profil même si la procédure d'installation du plug-in a échoué. Pour résoudre ce problème, installez et exécutez un navigateur 32 bits pris en charge et connectez-vous à l'iDRAC6.

Affichage de versions localisées de l'interface Web

Windows

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

- 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 redirection de console sur un client Red Hat® Enterprise Linux® (version 4) avec une GUI en chinois simplifié, le menu et le titre du visualiseur 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 résoudre 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**>. L'entrée suivant 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. Accédez au 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 l'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 de l'iDRAC6, voir « Configuration avancée d'iDRAC6 ».

Retour á la page du sommaire

Retour á la page du sommaire

Configuration de l'iDRAC6 via l'interface Web

Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.1

L'iDRAC6 intègre une interface Web qui vous permet de configurer les propriétés et les utilisateurs d'iDRAC6, d'effectuer les tâches de gestion à distance et de dépanner un système (géré) distant 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 de la gestion du serveur-protocole de ligne de commande (SM-CLP).

Les commandes RACADM locales sont exécutées à partir du serveur géré.

Les commandes SM-CLP/Telnet RACADM sont exécutées dans un environnement accessible à distance via une connexion Telnet ou SSH. Pour de plus amples renseignements sur la SM-CLP, consultez « Utilisation de l'interface de ligne de commande SM-CLP iDRAC6 » Pour de plus amples renseignements sur la RACAD, consultez « Présentation de la sous-commande RACADM » et « Définitions des groupes et des objets de la base de données des propriétés iDRAC6 ».

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 plus d'informations, voir « Navigateurs 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, vous devez activer la IPv4 :

   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, vous devez activer la IPv6 :

   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 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 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 par défaut et le mot de passe pour un utilisateur iDRAC6 sont **root** et **calvin**, respectivement.

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

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

     Les noms Active Directory peuvent être entrés 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\jean_dupont` ou `JEAN_DUPONT@DELL.COM`.
2. Dans le champ **Mot de passe**, tapez votre mot de passe utilisateur iDRAC ou Active Directory. La différence entre majuscules et minuscules est prise en compte.
3. Depuis la boîte déroulante **Domaine**, sélectionnez *Cet iDRAC* pour ouvrir une session en tant qu'utilisateur iDRAC6, ou sélectionnez tout domaine disponible pour vous connecter 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 de l'utilisateur, sélectionnez *Cet iDRAC* depuis 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, la session peut rester ouverte jusqu'à ce qu'elle expire. Nous vous conseillons vivement 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 pour Internet Explorer à partir du site Web de support de Microsoft, à l'adresse : **support.microsoft.com**.

Configuration de iDRAC6 NIC

Cette section suppose qu'iDRAC6 a déjà été configuré et est accessible sur le réseau. Voir « Configuration de l'iDRAC6 » 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 privilège de **configuration iDRAC** pour effectuer les étapes suivantes.

REMARQUE : La plupart des serveurs DHCP requièrent un serveur pour stocker un jeton d'identification 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 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 de l'arbre maximal (STP) activé, assurez d'activer également le PortFast ou une technologie similaire comme suit :

- Slur es ports pour l'interrupteur branché au iDRAC6
- Sur les ports connectés au poste de gestion ayant une session iDRAC KVM ouverte.

REMARQUE : Il se peut que vous receviez le message suivant si le système s'arrête durant POST : Strike the F1 key to continue, F2 to run the system setup program (Appuyez sur la touche F1 pour continuer, F2 pour lancer le programme de configuration du système). Une des raisons possibles de cette erreur est le cas d'une tempête du réseau qui cause la perte de communication avec l'iDRAC6. Une fois que la tempête du réseau s'est calmée, redémarrez le système.

1. Cliquez sur **Accès à distance→ Configuration→ Réseau.**
2. Sur la page **Réseau** , vous pouvez entrer les paramètres de la carte d'interface réseau, les paramètres courants du iDRAC, les paramètres IPv4 IPv6, IPMI et VLAN. Voir Tableau 4-1, Tableau 4-2, Tableau 4-3, Tableau 4-4, Tableau 4-5 et Tableau 4-6 pour les descriptions de ces paramètres.
3. Après avoir entré les paramètres requis, cliquez sur **Appliquer**.

4. Cliquez sur le bouton approprié pour continuer. Reportez-vous au Tableau 4-7.

Tableau 4-1. Paramètres de la carte Interface réseau

Paramètre	Description
Sélection de NIC	Configure le mode courant sur les quatre modes possibles : · Réservé (iDRAC NIC) **REMARQUE :** Cette option n'est offerte que pour iDRAC6 Enterprise. · Partagé (LOM1) · Partagé avec reprise de support optique à lecture laser 2 (LOM2) · Partagé avec reprise de support optique à lecture laser 2 (LOM) **REMARQUE :** Il se peut que cette option ne soit pas disponible sur iDRAC6 Enterprise. **REMARQUE :** L'iDRAC6 ne communique pas localement via le même port physique si **Sélection de NIC** est définie sur les modes **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.
MAC Address (Adresse Mac)	Affiche l'adresse de contrôle de l'accès aux médias (MAC) qui identifie de manière unique chaque nud d'un réseau.
Activer le NIC	Lorsqu'il est coché, ce paramètre indique que le NIC est activé et active les commandes restantes de ce groupe. Lorsqu'un NIC est désactivé, toutes les communications avec iDRAC via le réseau sont bloquées. La valeur par défaut est **Marche**.
Négociation automatique	Si défini à **MARCHE (On)**, affiche la vitesse du réseau et le mode en communiquant avec le routeur ou le concentrateur le plus près. Si défini à **ARRÊT (Off)**, vous permet de définir la vitesse du réseau et le mode duplex manuellement (Off). Si la **Sélection NIC** n'est *pas* définie à **Réservée**, la négociation automatique est toujours activée (**On**).
Vitesse du réseau	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	Permet d'activer 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**.

Tableau 4-2. Paramètres iDRAC courant

Paramètre	Description
Enregistrer iDRAC sur DNS	Enregistre le nom iDRAC6 sur le serveur DNS. La valeur par défaut est **Désactivé**.
Nom iDRAC DNS	Affiche le nom iDRAC6 uniquement lorsque l'option **Enregistrer iDRAC sur DNS** est sélectionnée. 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.
Utiliser DHCP pour le nom de domaine DNS	Utilise le nom de domaine DNS par défaut. Si la case n'est pas cochée et que l'option **Enregistrer iDRAC sur DNS** est sélectionnée, changez le nom de domaine DNS dans le champ **Nom de domaine DNS**. La valeur par défaut est **Désactivé**. **REMARQUE :** Pour cocher la case **Utiliser DHCP pour le nom de domaine DNS**, cochez également la case **Utiliser DHCP (pour l'adresse IP du NIC)**.
Nom de domaine DNS	Le champ du **nom de domaine DNS** par défaut est vide. Lorsque la case **Utiliser DHCP pour le nom de domaine DNS** est cochée, cette option est grisée et le champ ne peut pas être modifié.

Tableau 4-3. Paramètres IPv4

Paramètre	Description
Activé	Si le NIC est activé, celui-ci sélectionne le support de protocole IPv4 et définit les autres champs de cette section à Activé.
Utiliser DHCP (pour l'adresse IP du NIC)	Demande à iDRAC6 d'obtenir une adresse IP pour le NIC sur le serveur de protocole de configuration dynamique d'hôte (DHCP). La valeur par défaut est **Désactivé**.
Adresse IP	Spécifie l'adresse IP du NIC iDRAC6.
Masque de sous-réseau	Vous permet de saisir ou de modifier une adresse IP statique pour le NIC d'iDRAC6. Pour modifier ce paramètre, désélectionnez la case Utiliser DHCP (pour l'adresse IP du NIC).

défaut	L'adresse d'un routeur ou d'un interrupteur. La valeur est sous forme séparée par un point telle que 192.168.0.1.
Utiliser DHCP pour obtenir des adresses de serveur DNS	Activez DHCP pour obtenir les adresses de serveur DNS en cochant la case **Utiliser DHCP pour obtenir des adresses de serveur DNS**. Si vous n'utilisez pas DHCP pour obtenir les adresses de serveur DNS, indiquez les adresses IP dans les champs **Serveur DNS statique préféré** et **Autre serveur DNS statique**. La valeur par défaut est **Désactivé**. **REMARQUE :** Lorsque la case **Utiliser DHCP pour obtenir des adresses de serveur DNS** est cochée, les adresses IP ne peuvent pas être entrées dans les champs **Serveur DNS statique préféré** et **Autre serveur DNS statique**.
Serveur DNS préféré	Adresse IP du serveur DNS.
Serveur DNS secondaire	Adresse IP secondaire

Tableau 4-4. Paramètres IPv6

Paramètre	Description
Activé	Si la case à cocher est sélectionnée, IPv6 est activé. Si la case à cocher est désélectionnée, IPv6 est désactivé. Désactivé est sélectionné par défaut.
Auto Config	En cochant cette case vous permettez à l'iDRAC6 d'obtenir l'adresse IPv6 pour l'interface réseau d'iDRAC6 depuis le serveur de protocole de configuration dynamique d'hôte (DHCPv6). L'activation de la **Configuration automatique** désactive et supprime les valeurs de l'adresse IP 1, la longueur du préfixe et la passerelle IP.
Adresse IP 1	Indique l'adresse IPv6 de l'interface réseau d'iDRAC. Pour changer ce paramètre, vous devez tout d'abord désactiver **Configuration automatique** en désélectionnant la case à cocher correspondante.
Longueur du préfixe	Configure la longueur du préfixe de l'adresse IPv6. Il peut s'agir de toute valeur comprise entre 1 et 128. Pour changer ce paramètre, vous devez tout d'abord désactiver **Configuration automatique** en désélectionnant la case à cocher correspondante.
Passerelle IP	Configure la passerelle statique pour l'interface réseau d'iDRAC. Pour changer ce paramètre, vous devez tout d'abord désactiver **Configuration automatique** en désélectionnant la case à cocher correspondante.
Adresse locale du lien	Spécifie l'adresse IPv6 du NIC iDRAC6.
Adresse IP 2	Spécifie l'adresse IPv6 du NIC iDRAC6 supplémentaire en cas de disponibilité.
Utiliser DHCP pour obtenir des adresses de serveur DNS	Activez DHCP pour obtenir les adresses de serveur DNS en cochant la case **Utiliser DHCP pour obtenir des adresses de serveur DNS**. Si vous n'utilisez pas DHCP pour obtenir les adresses de serveur DNS, indiquez les adresses IP dans les champs **Serveur DNS statique préféré** et **Autre serveur DNS statique**. La valeur par défaut est Désactivé. Cochez la copie de vérification REMARQUE : Lorsque la case **Utiliser DHCP pour obtenir des adresses de serveur DNS** est cochée, les adresses IP ne peuvent pas être entrées dans les champs **Serveur DNS préféré** et **Autre serveur DNS**.
Serveur DNS préféré	Configure l'adresse IPv6 statique du serveur DNS préféré. Pour changer ce paramètre, vous devez tout d'abord décocher **Utiliser DHCP pour obtenir des adresses de serveur DNS**.
Serveur DNS secondaire	Configure l'adresse IPv6 statique du serveur DNS secondaire. Pour changer ce paramètre, vous devez tout d'abord décocher **Utiliser DHCP pour obtenir des adresses de serveur DNS**.

Tableau 4-5. Paramètres IPMI

Paramètre	Description
Activer IPMI sur le réseau local	Lorsque ce paramètre est coché, 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 blanc.

Tableau 4-6. Paramètres VLAN

Paramètre	Description
Activer l'ID du VLAN	Si cette option est activée, seule la circulation ID du LAN virtuel (VLAN) est acceptée.
ID du VLAN	Champ ID du VLAN des champs 802.1g. Entrez une valeur valide pour l'ID du VLAN (doit être un numéro entre 1 et 4094).
Priorité	Champ Priorité des champs 802.1g. Entrez un numéro entre 0 et 7 pour définir la priorité de l'ID du VLAN.

Tableau 4-7. Boutons de la page Configuration réseau

Bouton	Description
Imprimer	Imprime les valeurs de **Configuration réseau** qui apparaissent à l'écran.
Actualiser	Recharge la page **Configuration réseau**.

Paramètres avancés	Ouvre la page **Sécurité réseau** pour permettre à l'utilisateur d'entrer les attributs de la plage IP et les attributs de blocage IP.
Appliquer les modifications	Enregistre les nouveaux paramètres définis sur la page Configuration réseau. **REMARQUE :** Les modifications des paramètres de l'adresse IP du NIC ferment toutes les sessions utilisateur et forcent les utilisateurs à se reconnecter à l'interface Web d'iDRAC6 avec les paramètres d'adresse IP mis à jour. Toutes les autres modifications nécessitent la réinitialisation du NIC, qui peut provoquer une perte brève de connectivité.

Configuration du filtrage IP et du blocage IP

REMARQUE : Vous devez disposer du privilège de **configuration iDRAC** pour effectuer les étapes suivantes.

1. Cliquez sur **Accès à distance**→ **Configuration** , puis 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**. Une fois les paramètres configurés, cliquez sur **Appliquer**.
3. Cliquez sur le bouton approprié pour continuer. Reportez-vous au Tableau 4-9.

Tableau 4-8. Paramètres de la page Sécurité réseau

Paramètres	Description
Plage IP activée	Active la fonctionnalité de vérification de la plage IP, qui définit une plage d'adresses IP pouvant accéder à iDRAC. La valeur par défaut est **Désactivé**.
Adresse de la plage IP	Détermine le format binaire d'adresse IP autorisé, en fonction des 1 dans le masque de sous-réseau. Cette valeur correspond à l'opérateur 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 avec un iDRAC6. Les ouvertures de session à partir des adresses IP qui sont situées à l'extérieur de cette plage échoueront. 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 avec l'iDRAC6.
Masque de sous-réseau de la plage IP	Définit les positions des bits de fort poids 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 de 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 prédéfinie. 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 de rejeter les tentatives d'ouverture de session à partir de cette adresse. L'adresse par défaut est **10**.
Plage d'échecs avant blocage IP	Détermine la période en secondes pendant laquelle doivent se produire des échecs du nombre d'échecs avant blocage IP pour déclencher la période de pénalité avant blocage IP. L'adresse par défaut est **3600**.
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. L'adresse par défaut est **3600.**

Tableau 4-9. Boutons de la page Sécurité réseau

Bouton	Description
Imprimer	Imprime les valeurs de **Sécurité réseau** qui apparaissent à l'écran.
Actualiser	Recharge la page **Sécurité réseau**.
Appliquer les modifications	Enregistre les nouveaux paramètres que vous avez créés sur la page **Sécurité réseau**.
Retourner à la page Configuration réseau	Retoune à la page **Configuration réseau**.

Configuration des événements sur plate-forme

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 événements sur plateforme [PET] et/ou e-mail).

Les événements sur plateforme filtrables sont répertoriés dans le Tableau 4-10.

Tableau 4-10. Filtres d'événements sur plateforme

Index	Événement sur plateforme

1	Assertion Ventilateur critique
2	Assertion Avertissement batterie
3	Assertion batterie critique
4	Assertion Tension critique
5	Assertion Avertissement température
6	Assertion Température critique
7	Assertion Intrusion critique
8	Dégradation de la redondance des ventilateurs
9	Perte de la redondance des ventilateurs.
10	Assertion Avertissement de processeur
11	Assertion Processeur critique
12	Processeur absent
13	Assertion Avertissement concernant le bloc d'alimentation
14	Assertion Bloc d'alimentation critique
15	Bloc d'alimentation absent
16	Assertion Journal des événements critique
17	Assertion Surveillance critique
18	Assertion Avertissement concernant le bloc d'alimentation système
19	Assertion Bloc d'alimentation système critique

.

Lorsqu'un événement sur plate-forme se produit (par exemple, une assertion d'avertissement de 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 plate-forme (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'événement sur plate-forme est aussi configuré pour effectuer une action (tel qu'un redémarrage du système), l'action est effectuée.

Configuration des filtres d'événements sur plate-forme (PEF)

REMARQUE : Configurez vos filtres d'événements sur plate-forme avant de configurer les interruptions d'événement sur plate-forme 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. Consultez « Accès à l'interface Web ».
2. Cliquez sur **Système**→**Gestion d'alerte**→ **Événements sur plate-forme**.
3. Dans le premier tableau, cochez la case **Permettre les alertes des filtres d'événements sur plate-forme** , puis cliquez sur **Appliquer les modifications**.

   REMARQUE : Activer Alertes des filtres d'événements sur plate-forme doit être activé pour qu'une alerte soit envoyée à une destination configurée valide (PET ou e-mail).

4. Dans le tableau suivant, **Liste des filtres d'événements sur plate-forme**, cliquez sur le filtre à configurer.
5. À la page **Définir les événements sur plate-forme**, sélectionnez l'action appropriée **Éteindre** ou sélectionnez **Aucun**.
6. Sélectionnez ou désélectionnez **Générer une alerte** pour activer ou désactiver cette action.

   REMARQUE : Générer une alerte doit être activé pour qu'une alerte soit envoyée à une destination configurée valide (PET ou e-mail).

7. Cliquez sur **Appliquer les modifications**.

   Vous êtes de retour à la page **Événements sur plate-forme** où les modifications que vous avez appliquées sont affichées dans la **Liste des filtres d'événements sur plate-forme.**

8. Répétez les étapes 4 à 7 pour configurer d'autres filtres d'événements sur plate-forme.

Configuration des interruptions d'événement sur plate-forme (PET)

REMARQUE : Vous devez avoir le droit de **configurer iDRAC** pour ajouter, activer et désactiver une alerte SNMP. Les options suivantes ne sont pas disponibles si vous ne disposez pas de l'autorisation de **configuration iDRAC**.

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

2. Assurez-vous d'avoir bien suivi les procédures dans « Configuration des filtres d'événements sur plate-forme (PEF) ».

3. Cliquez sur **Système→ Gestion des alertes → Paramètres des interruptions**.

4. Dans la **Liste de destination IPv4** ou la **Liste de destination IPv6**, cliquez sur un numéro de destination pour configurer votre destination d'une alerte SNMP IPv4 ou IPv6.

5. À la page **Définir une destination d'une alerte d'événement sur plate- forme**, sélectionnez ou désélectionnez **Activer la destination**. Une case cochée indique que l'adresse IP est activée pour recevoir des alertes. Une case décochée signifie que l'adresse IP est désactivée pour ne pas recevoir des alertes.

6. Entrez une adresse IP valide de destination d'interruption d'événement et cliquez sur **Appliquer les modifications**.

7. Cliquez sur **Envoyer l'interruption-test** pour tester l'alerte configurée ou cliquez sur **Retourner à la page Destination d'événement sur plate-forme**.

   REMARQUE : Votre compte d'utilisateur doit avoir la fonction **Tester les alertes** afin d'envoyer une interruption-test. Voir Tableau 6-6, « Droits de groupes iDRAC » pour de plus amples renseignements.

   À la page **Destinations des alertes d'événement sur plate-forme**, les modifications que vous avez appliquées sont affichées dans la **Liste de destinations IPv4 ou IPv6.**

8. Dans le champ **Chaîne de la communauté**, entrez le nom de la communauté SNMP d'iDRAC approprié. Cliquez sur **Appliquer les modifications**.

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

9. Répétez les étapes 4 à 7 pour configurer les autres numéros de destination IPv4 ou IPv6.

Configuration des alertes par e-mail

REMARQUE : Les alertes par e-mail acceptent 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 bien suivi les procédures dans « Configuration des filtres d'événements sur plate-forme (PEF) ».

3. Cliquez sur **Système→ Gestion d'alerte→ Paramètres d'une alerte par e- mail**.

4. Dans le tableau sous **Adresses e-mail de destination**, cliquez sur le **Numéro d'alerte par e-mail** pour lequel vous souhaitez configurer une adresse de destination.

5. À la page **Définir une alerte par e-mail**, sélectionnez ou désélectionnez **Activer une alerte par e-mail**. Une case cochée indique que l'adresse e-mail est activée pour recevoir des alertes. Une case décochée signifie que l'adresse e-mail est désactivée pour ne pas recevoir des alertes.

6. Dans le champ **Adresse e-mail de destination**, tapez une adresse e-mail valide.

7. Dans le champ **Description de l'e-mail**, tapez une courte description à afficher dans l'e-mail.

8. Cliquez sur **Appliquer les modifications**.

9. Si vous voulez tester l'alerte par e-mail configurée, cliquez sur **Envoyer un e-mail-test**. Sinon, cliquez sur **Retourner à la page Destination d'une alerte par e-mail**.

10. Cliquez sur **Retourner à la page Destination d'une alerte par e-mail** et entrez une adresse IP SMTP valide dans le champ **Adresse IP du serveur SMTP (e-mail)**.

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

11. Cliquez sur **Appliquer les modifications**.

12. Répétez les étapes 4 à 9 pour configurer des destinations d'alertes par e- mail supplémentaires.

Configuration d'IPMI

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 **Accès distant**.

   b. Cliquez sur l'onglet **Configuration**, puis sur **Réseau**.

   c. Sur la page **Configuration réseau** sous **Paramètres LAN IPMI**, sélectionnez **Activer IPMI sur le LAN** puis cliquez sur **Appliquer les changements**.

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

   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 les modifications**.

   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 **Accès distant**.

   b. Dans l'onglet **Configuration**, cliquez sur **Communication série sur LAN**.

   c. Sur la page **Configuration de la communication série sur LAN**, sélectionnez **Activer 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 les modifications**.

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

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

   g. Cliquez sur **Appliquer les modifications**.

4. Configurez IPMI série.

   a. Dans l'onglet **Configuration**, cliquez sur **Série**.

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

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

   c. Configurez le débit en bauds IPMI série.

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

   d. Configurez la limite du niveau de privilège du canal.

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

   e. Cliquez sur **Appliquer les modifications**.

   f. Assurez-vous que MUX série est correctement configuré 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.
      - Allez à **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.

Si IPMI série est 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, consultez la spécification d'IPMI 2.0. Pour de plus amples renseignements sur les commandes en mode terminal, consultez le *Guide d'utilisation des utilitaires du contrôleur de gestion de la carte mère Dell OpenManage* à **support.dell.com\manuals**\.

Configuration des utilisateurs de l'iDRAC6

Voir « Ajout et configuration d'utilisateurs iDRAC6 » 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 au SSL via l'interface Web
- Création d'une RSC
- Téléversement d'un certificat de serveur
- Affichage d'un certificat de serveur

Secure Sockets Layer (SSL)

L'iDRAC6 utilise Web Server, un serveur 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 à 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 compatible SSL peut effectuer les tâches suivantes :

- S'authentifier sur un client compatible 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. L'iDRAC6 applique la norme de cryptage SSL à 128 bits qui est la forme la plus fiable de cryptage généralement disponible pour les navigateurs Internet en Amérique du Nord.

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 Web Server 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 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 de dépistage et d'identification fiables et d'autres critères de sécurité importants. Thawte et VeriSign sont des exemples de CA. Une fois que l'autorité de certification reçoit une RSC, elle la contrôle et vérifie les informations qu'elle contient. Si le postulant remplit les normes de sécurité de l' autorité de certification , cette dernière lui envoie 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'autorité de certification approuve la RSC et qu'elle envoie le certificat, téléversez ce dernier sur le micrologiciel iDRAC6. Les informations de la RSC enregistrées sur le micrologiciel d'iDRAC6 doivent correspondre aux informations du certificat.

Accès au SSL via l'interface Web

1. Cliquez sur **Accès à distance**→ **Configuration**.
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 autorité de certification. Les informations de la RSC sont stockées dans le micrologiciel iDRAC6.

- Téléverser un certificat du serveur.
- Visualiser un certificateur du serveur.

Le Tableau 4-11 décrit les options de la page **SSL** ci-dessus.

Tableau 4-11.

Champ	Description
Requête de signature de certificat (RSC)	Cette option vous permet de générer une RSC à envoyer à une autorité de certification pour demander un certificat Web sécurisé. **REMARQUE :** Chaque nouvelle CSR supplante la CSR qui se trouve déjà sur le micrologiciel. Pour qu'une CA accepte votre CSR, la CSR du micrologiciel doit correspondre au certificat renvoyé par la CA.
Téléverser le 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 l'iDRAC6. **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 l'iDRAC6.
Afficher le certificat de serveur	Cette option vous permet de visualiser un certificat de serveur existant.

Options de la page SSL

Génération d'une requête de signature de certificat

REMARQUE : La nouvelle RSC remplace toujours les données de RSC stockées sur le micrologiciel. Avant qu'iDRAC ne puisse accepter votre RSC signée, la RSC figurant dans le micrologiciel devrait correspondre au certificat renvoyée par l'autorité de certification.

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)**, entrez une valeur pour chaque attribut RSC. Le Tableau 4-12 décrit les attributs de la RSC.
3. Cliquez sur **Générer** pour créer la RSC et la télécharger sur votre ordinateur local.
4. Cliquez sur le bouton approprié pour continuer. Reportez-vous au Tableau 4-13.

Tableau 4-12. Générer des attributs de requête de signature de certificat (RSC)

Champ	Description
Nom commun	Le nom exact à certifier (normalement, le nom de domaine du iDRAC, par exemple, **www.compagniexyz.com**). Les caractères alphanumériques, les tirets, les traits de soulignement, les espaces et les points sont valides.
Nom de la société	Le nom associé à cette société (par exemple, Compagnie XYZ). Seuls les caractères alphanumériques, les tirets, les traits de soulignement, les points et les espaces sont valides.
Service de la société	Nom associé au service, comme un département (par exemple, Informatique). Seuls les caractères alphanumériques, les tirets, les traits de soulignement, les points et les espaces sont valides.
Ville	La ville ou autre lieu où se trouve l'entité à certifier (par exemple, Round Rock). Seuls les caractères alphanumériques et les espaces sont valides. Ne séparez pas les mots par des traits de soulignement ou d'autres caractères.
Nom de l'état	L'état ou la province où se trouve l'entité qui fait la demande de certification (par exemple, Texas). Seuls les caractères alphanumériques et les espaces sont valides. N'utilisez pas d'abréviations.
Code du pays	Le nom du pays où se trouve l'entité qui fait la demande de certification.
E-mail	L'adresse e-mail associée à la CSR. Tapez l'adresse e-mail de l'entreprise ou toute autre adresse e-mail associée à la RSC. Ce champ est optionnel.

Tableau 4-13. Boutons de la page Générer une requête de signature de certificat (CSR)

Bouton	Description
Imprimer	Imprime les valeurs de **Générer une requête de signature de certificat** qui apparaissent à l'écran.
Actualiser	Recharge la page **Générer une requête de signature de certificat**.
Générer	Génère une RSC et invite l'utilisateur à l'enregistrer dans un répertoire spécifié.
Retour au menu principal SSL	Renvoie l'utilisateur à la page **SSL**.

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 d'accès au fichier**, tapez le chemin du certificat dans le champ **Valeur** ou cliquez sur **Parcourir** pour accéder au fichier du certificat.

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

3. Cliquez sur **Appliquer**.

4. Cliquez sur le bouton approprié de la page pour continuer. Reportez-vous au Tableau 4-14.

Tableau 4-14. Boutons de la page Téléversement d'un certificat

Bouton	Description
Imprimer	Imprime la page **Téléversement d'un certificat**.
Retour au menu principal SSL	Retourne à la page **Menu principal SSL**.
Appliquer	Appliquez le certificat au micrologiciel d'iDRAC6.

Affichage d'un certificat de serveur

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

   La page **Visualisation d'un certificat de serveur** affiche le certificat de serveur que vous avez téléversé vers l'iDRAC.

   Le Tableau 4-15 décrit les champs et les descriptions associées énumérés dans le tableau **Certificat**.

2. Cliquez sur le bouton approprié pour continuer. Reportez-vous au Tableau 4-16.

Tableau 4-15. Informations relatives au certificat

Champ	Description
Numéro de série	Numéro de série du certificat
Informations sur le sujet	Attributs du certificat entrés par le demandeur
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

Tableau 4-16. Boutons de la page Afficher le certificat de serveur

Bouton	Description
Imprimer	Imprime les valeurs de **Afficher le certificat de serveur** qui apparaissent à l'écran.
Actualiser	Recharge la page **Afficher le certificat de serveur**.
Retour au menu principal SSL	Vous renvoie à la page **SSL**.

Configuration et gestion des certificats Active Directory

La page vous permet de configurer et gérer les paramètres de la fonctionnalité Active Directory.

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

REMARQUE : Avant de configurer ou d'utiliser la fonctionnalité Active Directory, vous devez vous assurer que le serveur Active Directory est configuré pour communiquer avec iDRAC6.

REMARQUE : Pour de plus amples renseignements sur la configuration d'Active Directory et la manière de la configurer avec Schéma détaillé ou Schéma standard, consultez « Utilisation d'iDRAC6 avec Microsoft Active Directory ».

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

1. Cliquez sur **Accès à distance**→ **Configuration**.
2. Cliquez sur **Active Directory** pour ouvrir la page **Configuration et gestion d'Active Directory**.

   Tableau 4-17 énumère les options de la page **Configuration et gestion d'Active Directory**.
3. Cliquez sur le bouton approprié pour continuer. Reportez-vous au Tableau 4-18.

Tableau 4-17. Options de la page Configuration et gestion d'Active Directory

Attribut	Description
Paramètres communs	
Active Directory Activé	Spécifie l'activation ou la désactivation d'Active Directory.
Ouverture de session individuelle activée	Spécifie si l'ouverture de session individuelle est activée ou désactivée. Si elle est activée, vous pouvez ouvrir une session iDRAC6 sans entrer vos références d'authentification d'utilisateur de domaine, par exemple le nom d'utilisateur et le mot de passe. Les valeurs sont **Oui** et **Non**.
Sélection de schéma	Spécifie l'utilisation d'un schéma standard ou étendu dans Active Directory. **REMARQUE :** Dans cette version, les fonctionnalités TFA (Two Factor Authentication [authentification bifactorielle]) s'articulant autour de la carte à puce et SSO (single sign-on [ouverture de session individuelle]) ne sont pas prises en charge si Active Directory est configuré pour 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 doit choisir pour ouvrir une session. Si elle n'est pas configurée, les utilisateurs d'Active Directory sont toujours en mesure d'ouvrir une session en entrant le nom d'utilisateur dans le format de nom_d'utilisateur@nom_domaine, nom_domaine/nom d'utilisateur.
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.
L'adresse du serveur du contrôleur de domaines 1-3 (FQDN ou IP)	Spécifie le nom de domaine complet qualifié (FQDN) du contrôleur de domaine ou de l'adresse IP. Au moins une des 3 adresses doit être configurée. Le DRAC tente de se connecter à chacune des adresses configurées une par une jusqu'à ce qu'une connexion soit établie. Si le schéma détaillé est sélectionné, il s'agira des adresses des contrôleurs de domaine dans lesquelles l'objet de l'iDRAC et les objets d'association sont situés. Si le schéma standard est sélectionné, il s'agit des adresses des contrôleurs de domaine dans lesquelles les comptes d'utilisateur et les groupes de rôles sont situés.
Validation de certificat activée	iDRAC utilise toujours le protocole allégé d'accès annuaire (LDAP) sur un protocole sécurité de cryptage (SSL) tout en se connectant à Active Directory. Par défaut, iDRAC utilise le certificat de l'autorité de certification chargé dans iDRAC pour valider le certificat de serveur SSL des contrôleurs de domaine durant l'établissement de liaison du protocole SSL et fournit une sécurité accrue. La validation du certificat peut être désactivée aux fins de test ou bien l'administrateur du système choisit de se fier aux contrôleurs de domaine dans la limite de sécurité sans valider les certificats SSL. Cette option spécifie l'activation ou la désactivation de la validation des certificats.
Certificat CA d'Active Directory	
Certificat	Le certificat de l'autorité de certificat qui signe l'ensemble des certificats de serveur SSL des contrôleurs de domaine.
Paramètres du schéma détaillé	**Nom iDRAC :** Spécifie le nom qui identifie uniquement l'iDRAC dans Active Directory. Cette valeur est NULL par défaut. **Nom de domaine iDRAC :** Le nom du DNS (chaîne) du domaine où se trouve l'objet iDRAC de l' Active Directory. Cette valeur est NULL par défaut. Ces paramètres s'affichent uniquement si l'iDRAC a été configuré en vue d'une utilisation avec un schéma Active Directory étendu.
Paramètres du schéma standard	**Adresse du serveur du catalogue global 1-3 (FQDN ou IP)** : Spécifie le nom complet de domaine qualifié (FQDN) ou l'adresse IP du ou des serveurs du catalogue global. Au moins une des 3 adresses doit être configurée. Le DRAC tente de se connecter à chacune des adresses configurées une par une jusqu'à ce qu'une connexion soit établie. Le serveur du catalogue global est exigé pour le schéma standard uniquement lorsque les comptes d'utilisateur et les groupes de rôles se trouvent dans différents domaines. **Groupes de rôles :** Spécifie la liste des groupes de rôles associé au iDRAC6. **Nom du groupe** : nom qui identifie le groupe de rôles dans l'Active Directory associé à la carte iDRAC6. **Domaine du groupe** : spécifie le domaine du groupe. **Privilège du groupe** : spécifie le niveau de privilège du groupe. Ces paramètres s'affichent uniquement si l'iDRAC a été configuré en vue d'une utilisation avec un schéma Active Directory standard.

Tableau 4-18. Boutons de la page Configuration et gestion d'Active Directory

Bouton	Définition
Imprimer	Imprime les valeurs qui sont affichées à la page Configuration et gestion de l'Active Directory.
Actualiser	Rafraîchit la page Configuration et gestion d'Active Directory.
Configurer Active Directory	Permet la configuration d'Active Directory. Voir « Utilisation d'iDRAC6 avec Microsoft Active Directory » pour obtenir des informations détaillées sur la configuration.
Paramètres de test	Permet de tester la configuration d'Active Directory à l'aide des paramètres spécifiés. Voir la section « Utilisation d'iDRAC6 avec Microsoft Active Directory » pour obtenir des informations détaillées sur l'utilisation de l'option **Paramètres de test**.

Configuration des services iDRAC6

REMARQUE : Pour modifier ces paramètres, vous devez avoir le droit de **configurer l'iDRAC**.

1. Cliquez sur **Accès distant**→ **Configuration**. Puis, cliquez sur l'onglet **Services** pour afficher la page de configuration des **Services**.
2. Configurez les services suivants, si nécessaire :
   - Configuration locale — voir Tableau 4-19
   - Web Server : voir Tableau 4-20 pour accéder aux paramètres Web Server
   - SSH : voir Tableau 4-21 pour accéder aux paramètres SSH
   - Telnet : voir Tableau 4-22 pour accéder aux paramètres Telnet
   - RACADM à distance — voir Tableau 4-23 pour accéder aux paramètres RACADM à distance.
   - SNMP : voir Tableau 4-24 pour accéder aux paramètres SNMP
   - Agent de récupération de système automatique (ASR) — voir Tableau 4-25 pour accéder aux paramètres Agent ASR.
3. Cliquez sur **Appliquer**.
4. Cliquez sur le bouton approprié pour continuer. Reportez-vous au Tableau 4-26.

Tableau 4-19. 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 RACADM	Désactive la configuration locale d'iDRAC à l'aide de l'option RACADM.

Tableau 4-20. Paramètres du serveur Web

Paramètre	Description
Activé	Active ou désactive le serveur Web iDRAC. Lorsqu'elle est cochée, cette case indique que Web Server est activé. **Activé** est sélectionné par défaut.
Nombre maximal de sessions	Nombre maximal de sessions simultanées 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 du **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 aux paramètres du délai d'expiration prennent immédiatement effet et mettent fin à la session d'interface Web. Le serveur Web est également réinitialisé. Veuillez attendre quelques minutes avant d'ouvrir une nouvelle session d'interface Web. La place du délai d'inactivité est de 60 à 10 800 secondes. La valeur par défaut est de 1 800 secondes.
Numéro de port HTTP	Port sur lequel iDRAC6 écoute une connexion au navigateur. L'adresse par défaut est **80**.
Numéro de port HTTPS	Port sur lequel iDRAC6 écoute une connexion au navigateur sécurisée. L'adresse par défaut est **443**.

Tableau 4-21. Paramètres SSH

Paramètre	Description
Activé	Active ou désactive SSH. Lorsqu'elle est cochée, cette case indique que SSH est activé.
Délai	Délai d'attente Secure Shell, en secondes. La plage du délai d'expiration est comprise entre 60 et 1 920 secondes. Saisissez 0 seconde pour

d'attente	désactiver la fonctionnalité Délai d'expiration. L'adresse par défaut est **300**.
Numéro de port	Port sur lequel iDRAC6 écoute une connexion SSH. L'adresse par défaut est **22**.

Tableau 4-22. Paramètres Telnet

Paramètre	Description
Activé	Active ou désactive Telnet. Lorsqu'il est coché, Telnet est activé.
Délai d'attente	Délai d'expiration en cas d'inactivité de la commande 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. L'adresse par défaut est **300**.
Numéro de port	Port sur lequel iDRAC6 écoute une connexion Telnet. L'adresse par défaut est **23**.

Tableau 4-23. Paramètres RACADM distante

Paramètre	Description
Activé	Active ou désactive la RACADM distante. Lorsqu'il est coché, la RACADM distante est activée.
Sessions actives	Nombre de sessions ouvertes sur le système.

Tableau 4-24. Paramètres SNMP

Paramètre	Description
Activé	Active ou désactive SNMP. Lorsqu'il est coché, SNMP est activé.
Nom de la communauté SNMP	Active ou désactive le nom de la communauté SNMP. Lorsque coché, le nom de la communauté SNMP est activé. Nom de communauté qui contient l'adresse IP pour la destination de l'alerte SNMP. Le nom de la communauté peut contenir jusqu'à 31 caractères de long autre qu'un blanc. La valeur par défaut est **public**.

Tableau 4-25. Paramètre de l'agent de récupération de système automatique

Paramètre	Description
Activé	Active ou désactive l'agent de récupération de système automatique. Lorsque cette option est cochée, l'agent de récupération de système automatique est activé.

Tableau 4-26. Boutons de la page Services

Bouton	Description
Imprimer	Imprime la page **Services**.
Actualiser	Actualise la page **Services**.
Appliquer les modifications	Applique les paramètres de la page **Services**.

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

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 d'iDRAC6.

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

1. Ouvrez l'interface Web d'iDRAC6 et ouvrez une session sur le système à distance.
2. Cliquez sur **Accès à distance**, puis cliquez sur l'onglet **Mise à jour**.
3. À la page **Téléversement/Restauration (Étape 1 de 3)** , cliquez sur **Parcourir** ou tapez le chemin vers l'image de micrologiciel que vous avez téléchargée depuis **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 du micrologiciel est **firmimg.d6**.

4. Cliquez sur **Téléverser**.

   Le fichier va se téléverser sur l'iDRAC6. Ce processus peut prendre plusieurs minutes.

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

   ```
   File upload in progress... (Téléversement du fichier en cours...)
   ```

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

   - Si le fichier image s'est téléversé avec succès et a passé tous les points de vérification, le nom du fichier image s'affiche. Si l'image du micrologiciel a été téléversée, les versions courantes 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 s'affiche et la mise à jour retourne à la page **Téléversement/Restauration (Étape 1 de 3)**. Vous pouvez réessayer de mettre à jour iDRAC6 ou cliquer sur **Annuler** pour faire revenir l'iDRAC6 au mode de fonctionnement normal.

6. Dans le cas d'une image du micrologiciel, la fonction **Préserver 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. Vous ne pourrez pas vous connecter à l'interface Web iDRAC6. Vous devrez reconfigurer les paramètres LAN à l'aide de l'utilitaire de configuration d'iDRAC6 durant le BIOS POST.

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

8. La page **Mise à jour (Étape 3 de 3)** affiche l'état de la mise à jour. La progression de l'opération de 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, l'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 s'affiche si une erreur se produit.

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

Restauration du micrologiciel d'iDRAC6

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

1. Ouvrez l'interface Web d'iDRAC6 et ouvrez une session sur le système à distance.

   Cliquez sur **Système→Accès à distance**, puis cliquez sur l'onglet **Mise à jour**.

2. À la page **Téléversement/Restauration (Étape 1 de 3)**, cliquez sur **Restaurer**. La version courante et la version restaurée du micrologiciel s'affichent à la page **État (Étape 2 de 3)**.

   Préserver 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 sent rétablis. Dans les paramètres par défaut, le LAN est activé. Vous ne pourrez pas vous connecter à l'interface Web iDRAC6. Vous devrez reconfigurer les paramètres LAN à l'aide de l'utilitaire de configuration d'iDRAC6 durant BIOS POST 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 3/3)**, vous verrez l'état de la 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, l'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 s'affiche si une erreur se produit.

Retour á la page du sommaire

Retour á la page du sommaire

Configuration avancée d'iDRAC6

Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.1

Contenant des informations sur la configuration avancée d'iDRAC6, cette section est recommandée aux utilisateurs ayant des connaissances avancées de 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 plus d'informations, voir « Installation de base de l'iDRAC6 ».

Configuration de l'iDRAC6 pour la visualisation de la sortie série à distance sur SSH/Telnet

Vous pouvez configurer l'iDRAC6 de manière à rediriger la console série à distance en procédant de la manière suivante :

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

1. Allumez ou redémarrez votre 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 **Communication série** en appuyant sur <Entrée>.
4. Définissez l'écran **Communication série** comme suit :

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

   REMARQUE : Vous pouvez définir communication série sur **Activé avec redirection série via com1** si le champ d'adresse du port série, périphérique2 série, est également défini sur com1.

   adresse du port série....périphérique1 série = com1, périphérique2 série = com2

   connecteur série externe....périphérique1 série

   débit de la ligne de secours....115200

   type de terminal distant....vt100/vt220

   redirection après démarrage....Activé)

   Sélectionnez ensuite **Enregistrer les modifications**.

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

Configuration des paramètres de l'iDRAC6 pour activer SSH/Telnet

Configurez ensuite les paramètres de l'iDRAC6 pour activer ssh/telnet, via RACADM ou l'interface Web de l'iDRAC6.

Pour configurer les paramètres de l'iDRAC6 afin d'activer ssh/telnet via 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 ».

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

1. Développez l'arborescence du **système** et cliquez sur **Accès distant**.
2. Cliquez sur l'onglet **Configuration**, 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 de la console texte via Telnet ou SSH

Lorsque vous avez ouvert une session sur l'iDRAC6 avec le logiciel du terminal de votre station de gestion via 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 de l'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 réduire cette valeur avec la commande :

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

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

Utilisation d'une console Telnet

Exécution de Telnet via Microsoft® 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 sur 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 hotfix 824810 sur le site Web de 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 **www.microsoft.com/downloads/** et recherchez « *Windows Services for UNIX 3.5* ».

Activation de Microsoft Telnet pour la redirection de console 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 redirection de console du BIOS est configurée pour l'émulation VT100/VT220. Si vous avez ce problème, mettez à jour l'affichage en choisissant le mode ANSI pour la redirection de console du BIOS. Pour effectuer cette procédure dans le menu de configuration du BIOS, sélectionnez **Redirection de console** → **Type de terminal distant** → **ANSI**.

REMARQUE : Lorsque vous configurez la fenêtre d'émulation VT100 du client, vous devez définir la fenêtre ou l'application qui affiche la console redirigée sur 25 lignes et 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 l'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 de l'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 arrière> peut avoir des résultats inattendus. Par exemple, la session peut renvoyer en écho ^h. Toutefois, la plupart des clients Microsoft et Linux telnet peuvent être configurés pour utiliser la touche <Retour arrière>.

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

1. Ouvrez une fenêtre d'invite de commande (si nécessaire).
2. Si vous n'exécutez pas encore 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 :

   ```
   Backspace will be sent as delete. (Retour arrière sera envoyé en tant que supprimer.)
   ```

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

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 cur 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 plus grande sécurité. L'iDRAC6 prend en charge la version 2 de SSH avec authentification par mot de passe. SSH est activé sur l'iDRAC6 lorsque vous installez ou mettez à jour le 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 publie un message d'erreur. Le texte du message dépend du client et n'est pas contrôlé par l'iDRAC6.

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

Seules quatre sessions SSH sont prises en charge à la fois. Le délai d'expiration de la session est contrôlé par la propriété cfgSsnMgtSshIdleTimeout comme décrit dans la section « Définitions des groupes et des objets de la base de données des propriétés iDRAC6 ».

Pour activer SSH sur l'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 plus d'informations sur les propriétés cfgSerialSshEnable et cfgRacTuneSshPort, voir « Définitions des groupes et des objets de la base de données des propriétés iDRAC6 ».

La mise en uvre SSH de l'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 • RIJNDAEL256-CBC • AES192-CBC • RIJNDAEL192-CBC

	• AES128-CBC • RIJNDAEL128-CBC • BLOWFISH-128-CBC • 3DES-192-CBC • ARCFOUR-128
Intégrité du message	• HMAC-SHA1-160 • HMAC-SHA1-96 • HMAC-MD5-128 • HMAC-MD5-96
Authentification	• Mot de passe

REMARQUE : SSHv1 n'est pas pris en charge.

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

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

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

Modifiez le fichier **/etc/grub.conf** de la manière suivante :

1. Localisez les sections relatives aux paramètres généraux dans le fichier et ajoutez les deux 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.

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 generated by anaconda
#
# Note that you do not have to rerun grub after making changes
# to this file
# NOTICE:  You do not have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /, e.g.
#          root (hd0,0)
#          kernel /boot/vmlinuz-version ro root=/dev/sdal
#          initrd /boot/initrd-version.img
#
#boot=/dev/sda
default=0
timeout=10
#splashimage=(hd0,2)/grub/splash.xpm.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'affichera pas sur la redirection de console du RAC. Pour désactiver l'interface graphique, commentez la ligne commençant par splashimage.

2. Pour activer plusieurs options GRUB afin de démarrer les sessions de console via la connexion en série 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 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  This file describes how the INIT process should set up
#          the system in a certain run-level.
#
# Author:  Miquel van Smoorenburg
#          Modified for RHS Linux by Marc Ewing and Donnie Barnes
#
# Default runlevel. The runlevels used by RHS are:
#   0 - halt (Do NOT set initdefault to this)
#   1 - Single user mode
#   2 - Multiuser, without NFS (The same as 3, if you do not have
#       networking)
#   3 - Full multiuser mode
#   4 - unused
#   5 - X11
#   6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:

# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit

l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6

# Things to run in every runlevel.
ud::once:/sbin/update

# Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

# When our UPS tells us power has failed, assume we have a few
# minutes of power left. Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have power installed and your
# UPS is connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"
# If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"

# Run gettys in standard runlevels
co:2345:respawn:/sbin/agetty -h -L 57600 ttyS1 ansi
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# Run xdm in runlevel 5
# xdm is now a separate service
x:5:respawn:/etc/X11/prefdm -nodaemon
```

Modifiez le fichier **/etc/securetty** 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
```

Configuration de l'iDRAC6 pour la connexion série

Vous pouvez utiliser l'une des interfaces suivantes pour vous connecter à l'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.

Configurez le **BIOS** pour activer la connexion série :

1. Allumez ou redémarrez votre 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 **Communication série** en appuyant sur <Entrée>.
4. Définissez l'écran **Communication série** comme suit :

   connecteur série externe....périphérique d'accès à distance

   Sélectionnez ensuite **Enregistrer les modifications**.

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

Connectez ensuite votre câble DB-9 ou null modem de la station de gestion au serveur de nud géré. Consultez « Connexion d'un DB-9 ou d'un câble null modem pour console série ».

Assurez-vous ensuite que votre logiciel d'émulation du terminal de gestion est configuré pour la connexion série. Consultez « Configuration du logiciel d'émulation de terminal de la station de gestion ».

Configurez ensuite les paramètres de l'iDRAC6 pour activer ssh/telnet, via RACADM ou l'interface Web de l'iDRAC6.

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

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

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

1. Développez l'arborescence du **système** et cliquez sur **Accès distant**.
2. Cliquez sur l'onglet **Configuration**, 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 de vos paramètres précédents, une demande 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 fonctions telles que RACADM. Par exemple, pour imprimer le journal des événements système, entrez la commande RACADM suivante :

```
racadm getsel
```

Configuration d'iDRAC pour le mode de base de connexion directe et le mode terminal de connexion directe

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

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

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

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

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

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

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

1. Développez l'arborescence du **système** et cliquez sur **Accès distant**.
2. Cliquez sur l'onglet **Configuration**, puis sur **Série**.
3. Sélectionnez **Activé** dans la section **série RAC**.

   Pour le mode de base de connexion directe :

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

   Pour le mode terminal de connexion directe :

   Dans la section **série IPMI**, faites passer le menu déroulant **Paramètres du mode de connexion** à **Mode terminal de connexion directe**.
4. Cliquez sur **Appliquer les modifications**. Pour plus d'informations sur les modes de base de connexion directe et terminal de connexion directe, voir « Configuration des modes série et terminal ».

Le mode de base de connexion directe 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
```

Le mode terminal de connexion directe permet de publier des commandes ASCII sur l'iDRAC6. Par exemple, pour activer/désactiver le serveur via le mode terminal de connexion directe :

1. Connectez-vous à l'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 :

   ```
   [SYS]
   ```

   ```
   [OK]
   ```
3. Tapez la commande suivante pour vous assurer que l'ouverture de session a réussi :

   ```
   [SYS TMODE]
   ```

   Les éléments suivants s'affichent :

   ```
   [OK TMODE]
   ```
4. Pour désactiver le serveur (le serveur se désactive immédiatement), tapez la commande suivante :

   ```
   [SYS POWER OFF]
   ```
5. Pour activer le serveur (le serveur s'active immédiatement) :

   ```
   [SYS POWER ON]
   ```

Basculement entre le mode Communication d'interface série RAC et Redirection de console

série

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

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

1. Allumez ou redémarrez votre 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 **Communication série** en appuyant sur <Entrée>.
4. Définissez l'écran **Communication série** comme suit :

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

   REMARQUE : Vous pouvez définir le champ **communication série** sur **Activé avec la redirection série via com1** si le **périphérique2 série** du **champ adresse de port address** est également défini sur com1.

   adresse du port série -- périphérique1 série = com1, périphérique2 série = com2

   connecteur série externe -- périphérique2 série

   débit de la ligne de secours....115200

   type de terminal à distance....vt100/vt220

   redirection après démarrage....Activé

   Sélectionnez ensuite **Enregistrer les modifications**.

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

Connectez le câble modem null 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 d'amorçage du serveur géré, les écrans 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 suivants de la station de gestion : Débit en bauds :115200 ; données : 8 bits ; parité : aucune ; arrêt : 1 bit et contrôle du débit : aucun.

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

```
<Échap> + <Maj> <9>
```

La séquence de touches ci-dessus vous achemine à l'invite « Connexion iDRAC » (si le RAC est défini sur le mode « RAC série ») ou au mode « Connexion série » où les commandes de terminal peuvent être émises (si le RAC est défini sur le mode « Terminal de connexion directe série IPMI »).

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

```
<Échap> + <Maj> <q>
```

Connexion d'un DB-9 ou d'un câble null modem pour console série

Pour accéder au système géré en utilisant une console texte série, vous devez connecter un câble de modem null DB-9 au port COM du système géré. Pour que la connexion fonctionne avec un câble null modem, les paramètres de communication de série correspondants doivent être définis dans la configuration CMOS. Certains des câbles DB-9 n'ont pas le brochage ou 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 aussi être utilisé pour la redirection de console texte du BIOS.

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

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

Votre 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 sont légèrement différentes mais doivent avoir les mêmes paramètres de base. Suivez les informations dans « Paramètres de Minicom requis pour l'émulation de console série » 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, Dell vous conseille d'utiliser une fenêtre Xterm plutôt que la console fournie par défaut par 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 **Serial Port Setup** (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/Parité/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 sont 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 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 redirection de console 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 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/Parité/Bits	57600 8N1
Contrôle du débit matériel	Oui
Contrôle du débit logiciel	Non
Émulation de terminal	ANSI
Paramètres de la numérotation du modem et des paramètres	Effacez les paramètres **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 redirection de console série

HyperTerminal est l'utilitaire d'accès au port série de Microsoft Windows. Pour définir correctement la taille de l'écran de la console, 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 Hilgraeve HyperTerminal. Cependant, la version comprise ne fournit pas beaucoup de fonctions requises pendant la redirection de console. À la place, vous pouvez utiliser tout logiciel d'émulation de terminal qui prend en charge le mode d'émulation VT100/VT220 ou ANSI. Un exemple d'émulateur de terminal complet VT100/VT220 ou ANSI qui prend en charge la redirection de console sur votre système est Hilgraeve HyperTerminal Private Edition 6.3. En outre, l'utilisation de la fenêtre de ligne de commande pour effectuer une redirection de console série Telnet risque d'afficher des caractères parasites.

Pour configurer HyperTerminal pour la redirection de console série :

1. Lancez le programme HyperTerminal.

2. Tapez le nom de la nouvelle connexion et cliquez sur **OK**.

3. À côté de **Connexion en utilisant** : sélectionnez le port COM de la station de gestion (COM2, par exemple) auquel vous avez connecté le câble modem null DB-9 et cliquez sur **OK**.

4. Configurez les paramètres du port COM comme indiqué dans le Tableau 5-7.

5. Cliquez sur **OK**.

6. Cliquez sur **Fichier→ Propriétés**, puis sur l'onglet **Paramètres**.

7. Définissez l'**ID du terminal Telnet** : sur **ANSI**.

8. Cliquez sur **Configuration du terminal** et choisissez **26** pour **Lignes de l'écran**.

9. Réglez **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	57600
Bits de données	8
Parité	None (Aucun)

Bits d'arrêt	1
Contrôle du débit	Matériel

Configuration des modes série et terminal

Configuration du mode série IPMI et iDRAC6

1. Développez l'arborescence du **système** et cliquez sur **Accès distant**.
2. Cliquez sur l'onglet **Configuration**, puis sur **Série**.
3. Configurez les paramètres série IPMI.

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

   Voir Tableau 5-9 pour une description des paramètres série de l'iDRAC6.
5. Cliquez sur **Appliquer les modifications**.
6. Cliquez sur le bouton approprié de la page **Configuration série** pour continuer. Consultez Tableau 5-10 pour obtenir une description des paramètres de la page Configuration série.

Tableau 5-8. Paramètres série IPMI

Paramètre	Description
Paramètres du mode de connexion	• Mode de base de connexion directe : mode de base série IPMI • Mode de base de connexion directe : mode de base série IPMI
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**.
Contrôle du flux	• Aucun : contrôle du débit matériel désactivé • RTS/CTS : contrôle du débit matériel activé
Limite du niveau de privilège du canal	• Administrateur • Opérateur • Utilisateur

Tableau 5-9. Paramètres série de l'iDRAC6

Paramètre	Description
Activé	Active ou désactive la console série de l'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 redirection de console. Coché = Activé ; Décoché = Désactivé
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. La valeur maximum et par défaut est de 8 192 caractères.
Commande d'ouverture de session	Ligne de commande de l'iDRAC6 à exécuter lors d'une ouverture de session valide.

Tableau 5-10. Paramètres de la page Configuration série

Bouton	Description
Imprimer	Imprime la page **Configuration série**.

Actualiser	Actualise la page **Configuration série**.
Appliquer les modifications	Appliquer les modifications série IPMI et iDRAC6.
Paramètres du mode terminal	Ouvre la page **Paramètres du mode terminal**.

Configuration du mode terminal

1. Développez l'arborescence du **système** et cliquez sur **Accès distant**.
2. Cliquez sur l'onglet **Configuration**, puis sur **Série**.
3. Sur la page **Série**, cliquez sur **Paramètres du mode terminal**.
4. Configurez les paramètres du mode terminal.

   Voir Tableau 5-11 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 Tableau 5-12 pour une description des boutons de la page Paramètres du mode terminal.

Tableau 5-11. 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 : • **iDRAC émet un caractère <retarr.><sp><retarr.> lorsque <retarr.> ou <suppr.> est reçu**. • **iDRAC émet un caractère <suppr.> lorsque <retarr.> ou <suppr.> est reçu**.
Contrôle d'écho	Active ou désactive l'écho.
Contrôle de la négociation	Active ou désactive la négociation.
Nouvelle séquence linéaire	Sélectionnez **Aucun**, **<CR-LF>**, **<NULL>**, **<CR>**, **<LF-CR>** ou **<LF>**.
Saisie d'une nouvelle séquence linéaire	Sélectionnez **<CR>** ou **<NULL>**.

Tableau 5-12. Boutons de la page Paramètres du mode terminal

Bouton	Description
Imprimer	Imprime la page **Paramètres du mode terminal**.
Actualiser	Actualise la page **Paramètres du mode terminal**.
Renvoyer à la configuration du port série	Retourne à la page **Configuration du port série**.
Appliquer les modifications	Applique les modifications apportées aux paramètres du mode terminal.

Configuration des paramètres réseau de l'iDRAC6

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

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

- Interface Web : voir « Configuration de iDRAC6 NIC ».
- CLI RACADM : voir « cfgLanNetworking ».
- Utilitaire de configuration de l'iDRAC6 : consultez la section « Configuration du système pour utiliser un iDRAC6 ».

REMARQUE : Pour déployer l'iDRAC6 dans un environnement Linux, voir « Installation de la RACADM ».

Accès à l'iDRAC6 via un réseau

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

- Une interface Web
- la RACADM
- Console Telnet
- SSH
- IPMI

Le Tableau 5-13 décrit chaque interface iDRAC6.

Tableau 5-13. Interfaces iDRAC6

Interface	Description
Une interface Web	Fournit un accès à distance à l'iDRAC6 à l'aide d'une interface utilisateur graphique. L'interface Web est intégrée au micrologiciel de l'iDRAC6 et accessible via l'interface NIC d'un navigateur Web pris en charge sur la station de gestion. Pour une liste des navigateurs Web pris en charge, voir « Navigateurs Web pris en charge ».
RACADM	Fournit un accès à distance à l'iDRAC6 à l'aide d'une interface de ligne de commande. RACADM utilise l'adresse IP de l'iDRAC6 IP pour exécuter les commandes RACADM. **REMARQUE :** La capacité d'accès à distance de racadm est prise en charge uniquement sur les stations de gestion. Pour plus d'informations, consultez « Utilisation de la RACADM à distance ». **REMARQUE :** Lors de l'utilisation des fonctionnalités distantes de RACADM, vous devez disposer d'un accès en écriture sur les dossiers sur lesquels vous utilisez les sous-commandes RACADM impliquant des opérations sur des fichiers, comme par exemple : `racadm getconfig -f <nom de fichier>` ou : `sous-commandes racadm sslcertupload -t 1 -f c:\cert\cert.txt`
Console Telnet	Donne accès à l'iDRAC6 et permet la prise en charge des commandes série et RACADM y compris les commandes **powerdown**, **powerup**, **powercycle** et **hardreset**. **REMARQUE :** Telnet est un protocole non sécurisé qui transmet toutes les données, y compris les mots de passe, en texte simple. Lors de la transmission d'informations critiques, utilisez l'interface SSH.
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 l'iDRAC6 aux fonctionnalités de gestion de base du système distant. L'interface inclut IPMI sur LAN, IPMI sur communication série et Communication série sur LAN. Pour plus d'informations, voir le Guide d'utilisation *Dell OpenManage Baseboard Management Controller Utilities* à l'adresse **support.dell.com\manuals**.

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

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

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

- Lancez Server Administrator.
- Dans l'arborescence 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 fonction d'accès RACADM à distance. Pour plus d'informations sur la configuration de votre iDRAC6 et une liste des documents connexes, voir « Installation de base de l'iDRAC6 ».

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 distante ou d'une station de gestion. 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 IP.

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

```
Security Alert: Certificate is invalid - Name on Certificate is invalid or does not match site name
```

```
Continuing execution. Use -S option for racadm to stop the execution on certificate-related errors.

(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.)
```

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

```
Security Alert: Certificate is invalid - Name on Certificate is invalid or does not match site name

Racadm not continuing execution of the command.

ERROR: Unable to connect to iDRAC6 at specified IP address

(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 l'iDRAC6 à l'adresse  IP spécifiée.)
```

REMARQUE : La capacité d'accès à distance de RACADM est prise en charge uniquement sur les stations de gestion. Consultez la *Matrice de prise en charge des logiciels des systèmes Del*l située sur le **site Web de support de Dell** à l'adresse **support.dell.com\manuals** pour plus d'informations.

REMARQUE : Lorsque vous utilisez la capacité d'accès à distance de RACADM, vous devez posséder des droits d'écriture sur les dossiers sur lesquels vous utilisez les sous-commandes RACADM impliquant des opérations sur des fichiers, par exemple :

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

ou

sous-commandes racadm sslcertupload -t 1 -f c:\cert\cert.txt
```

Synopsis de la RACADM

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

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

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

Options de la RACADM

Le Tableau 5-14 énumère les options de la commande RACADM.

Tableau 5-14. Options de la commande racadm

Option	Description
-**r <*racIpAddr*>** **-r <*racIpAddr*>:<***numéro de port***>**	Spécifie l'adresse IP distante du contrôleur. Utilisez <*numéro de port*> lorsque le numéro de port iDRAC6 n'est pas le port par défaut (443)
-**i**	Ordonne à 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 devrait contrôler les erreurs de certificat invalide. RACADM interrompt l'exécution de la commande avec un message d'erreur si elle détecte un certificat invalide.

Activation et désactivation de la fonctionnalité à distance de RACADM

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

Par défaut, la fonctionnalité de 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 fonctionnalité de capacité d'accès à distance, tapez :

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

Sous-commandes RACADM

Le Tableau 5-15 fournit une description de chaque sous-commande RACADM que vous pouvez exécuter dans la RACADM. Pour obtenir une liste détaillée des sous-commandes RACADM, y compris la syntaxe et les entrées valides, voir « Présentation de la sous-commande RACADM ».

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

```
racadm help
```

Tableau 5-15. 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 de la dernière panne (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.
config	Configure l'iDRAC6.
getconfig	Affiche les propriétés de configuration iDRAC6 actuelles.
coredump	Affiche le dernier vidage de mémoire de l'iDRAC6.
coredumpdelete	Supprime le vidage de mémoire stocké sur l'iDRAC6.
fwupdate	Exécute ou affiche l'état 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 de l'iDRAC6 avec le contenu actuel du tableau de routage.
setniccfg	Définit la configuration IP du contrôleur.
getniccfg	Affiche la configuration IP actuelle du contrôleur.
getsvctag	Affiche les numéros de service.
racdump	Vide les informations de condition et d'état de l'iDRAC6 pour le débogage.
racreset	Réinitialise l'iDRAC6.
racresetcfg	Restaure la configuration par défaut de l'iDRAC6.
serveraction	Effectue des opérations de gestion de l'alimentation sur le système géré.
getraclog	Affiche le journal de l'iDRAC6.
clrsel	Efface toutes les entrées du journal des événements système.
gettracelog	Affiche le journal de suivi de l'iDRAC6. Si elle est utilisée avec -i, la commande affiche le nombre d'entrées du journal de suivi de l'iDRAC6.
sslcsrgen	Génère et télécharge la CSR SSL.
sslcertupload	Téléverse un certificat d'autorité de certification ou un certificat de serveur sur iDRAC6.
sslcertdownload	Télécharge un certificat de CA.
sslcertview	Affiche un certificat d'autorité de certification ou un certificat de serveur dans l'iDRAC6.
sslkeyupload	Contraint l'iDRAC6 à envoyer un e-mail test sur le NIC de l'iDRAC6 pour vérifier la configuration de l'e-mail.
testtrap	Contraint l'iDRAC6 à envoyer une interruption SNMP sur le NIC d'iDRAC6 pour vérifier la configuration de l'interruption.
vmdisconnect	Force la déconnexion du média virtuel.
vmkey	Restaure la valeur par défaut de la taille du disque flash virtuel (256 Mo).

Questions fréquemment posées sur les messages d'erreur de la RACADM

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

ERROR: Unable to connect to RAC at specified IP address (ERREUR : Impossible de se connecter au RAC à l'adresse IP spécifiée.)

Qu'est-ce que ce message signifie ?

Vous devez attendre que l'iDRAC6 soit entièrement réinitialisé avant d'envoyer 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 RACADM locale : problèmes de syntaxe, d'erreurs typographiques et de noms incorrects.
- Messages d'erreur 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 bascule ma carte iDRAC6 entre les modes Dédié et Partagé pendant la réponse ping, je ne reçois aucune réponse.

Effacez la table ARP sur votre système.

Configuration de plusieurs contrôleurs iDRAC6

À l'aide de RACADM, vous pouvez configurer un ou plusieurs iDRAC6 avec des propriétés identiques. Lorsque vous effectuez une requête sur une carte iDRAC6 spécifique à l'aide de son numéro de groupe et du numéro de l'objet, RACADM crée le fichier de configuration **racadm.cfg** à partir des informations collectées. En exportant le fichier vers un ou plusieurs 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 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 RACADM locale et distante.

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

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 le contrôleur iDRAC6 cible qui a été configuré.

   À l'invite de commande, tapez :

   ```
   racadm racreset
   ```

La sous-commande **getconfig -f racadm.cfg** nécessite 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 les autres 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 corrompre ainsi la base de données RACADM.

Création d'un fichier de configuration iDRAC6

Le fichier de configuration de l'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 l'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 : Voir « getconfig » pour des informations sur la commande **getconfig**.

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 l'iDRAC6.

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

- Si l'analyseur rencontre un groupe indexé, c'est la valeur de l'objet ancré qui différencie les différents index.

  L'analyseur lit tous les index du contrôleur iDRAC6 pour ce groupe-là. Les objets présents dans ce groupe sont de simples modifications lorsque iDRAC6 est configuré. Si un objet modifié représente un nouvel index, l'index est créé sur l'iDRAC6 au cours de la configuration.

- Vous ne pouvez pas spécifier l'index de votre choix dans un fichier **.cfg**.

  Les index peuvent être créés et supprimés, ainsi le groupe peut devenir fragmenté avec des index utilisés et non utilisés. Si un index est présent, il est modifié. Si un index n'est pas présent, le premier index disponible est utilisé. Cette méthode permet une certaine flexibilité lors de l'ajout d'entrées indexées lorsque vous n'avez pas besoin de faire des correspondances d'index exactes entre tous les RAC gérés. De nouveaux utilisateurs sont ajoutés au premier index disponible. Un fichier **.cfg** qui analyse et s'exécute correctement sur un iDRAC6 peut ne pas s'exécuter correctement sur un autre si tous les index sont remplis et qu'un nouvel utilisateur doit être ajouté.

- Utilisez la sous-commande **racresetcfg** pour configurer plusieurs iDRAC6 avec des propriétés identiques.

  Utilisez la sous-commande **racresetcfg** pour réinitialiser l'iDRAC6 à ses paramètres initiaux par défaut et exécutez ensuite la `commande racadm config -f <nom de fichier>.cfg`. Le fichier **.cfg** doit inclure tous les objets, utilisateurs, index et autres paramètres requis.

PRÉCAUTION : Utilisez la sous-commande racresetcfg pour réinitialiser la base de données et les paramètres de carte d'interface réseau iDRAC6 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 rétablis.

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 :

  ```
  #

  # This is a comment (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 « Définitions des groupes et des objets de la base de données des propriétés iDRAC6 ».

  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 caractères de valeur 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.

Consultez l'exemple de la puce précédente.

- L'analyseur **.cfg** ignore une entrée d'objet d'index.

  L'utilisateur *ne peut pas* spécifier quel index est utilisé. Si l'index existe déjà, il est utilisé ou la nouvelle entrée est créée dans le premier index disponible pour ce groupe.

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

REMARQUE : Vous pouvez créer un groupe indexé manuellement en utilisant la commande suivante :
`racadm config -g <nom de groupe> -o <objet ancré> -i <index 1-16> <nom d'ancre unique>`

- La ligne d'un groupe indexé *ne peut pas* être supprimée d'un fichier **.cfg**.

  L'utilisateur doit supprimer un objet indexé manuellement en utilisant la commande suivante :

  `racadm config -g <nom de groupe> -o <nom d'objet> -i <index 1-16> ""`

REMARQUE : Une chaîne de caractères nulle (identifiée par deux caractères "") ordonne à l'iDRAC6 de supprimer l'index du groupe spécifié.

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

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

- 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]

  cfgUserAdminUserName=<NOM_D'UTILISATEUR>
  ```

  Si vous tapez `racadm getconfig -f <monexample>.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 d'iDRAC6 dans le fichier de configuration, supprimez toutes les entrées **<***variable***>**=**valeur** inutiles. Seul le nom du groupe variable actuel avec « [» et «] » reste avec les deux entrées **<***variable***>**= **valeur** correspondant au changement d'adresse IP.

Par exemple :

```
#

# Object Group "cfgLanNetworking" (Groupe d'objet « cfgLanNetworking »)

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.10.110

cfgNicGateway=10.35.10.1
```

Ce fichier est mis à jour comme suit :

```
#

# Object Group "cfgLanNetworking" (Groupe d'objet « cfgLanNetworking »)

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.9.143

# comment, the rest of this line is ignored (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 nécessaires. En outre, vous pouvez utiliser la même commande **getconfig** utilisée dans l'exemple précédent pour confirmer la mise à jour.

Utilisez ce fichier pour télécharger des modifications générales 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 du 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 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 iDRAC6, voir « Configuration du système pour utiliser un iDRAC6 ».

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

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

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

Le Tableau 5-16 fournit une description de chaque mode.

Tableau 5-16. Configurations NIC d'iDRAC6

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

Questions fréquemment posées concernant la sécurité réseau

Lorsque j'accède à l'interface Web de l'iDRAC6, un message de sécurité s'affiche ; il m'informe que le nom d'hôte du certificat SSL ne correspond pas au nom d'hôte de l'iDRAC6.

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

Pour résoudre ce problème de sécurité, téléversez un certificat de serveur d'iDRAC6 émis sur l'adresse IP ou le nom iDRAC de l'iDRAC6. Lors de la création d'une requête de signature de certificat (RSC) utilisée pour délivrer le certificat, assurez-vous que le nom commun (CN) de la RSC correspond à l'adresse IP

(**si le certificat est émis à IP**) de l'iDRAC6 (par exemple, 192.168.0.120) ou le nom de DNS iDRAC6 (**si le certificat est émis au nom enregistré d'iDRAC**).

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

1. Dans l'arborescence du **système**, cliquez sur **Accès distant**.
2. Cliquez sur l'onglet **Configuration** puis sur **Réseau**.
3. Dans le tableau **Paramètres communs** :
   a. Cochez la case **Enregistrer iDRAC sur DNS**.
   b. Dans le champ **Nom IDRAC DNS**, entrez le nom d'iDRAC6.
4. Cliquez sur **Appliquer les modifications**.

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

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

Lorsque vous réinitialisez le serveur Web d'un 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 :

- Quand 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**
- Quand l'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 ayant un maximum de 31 caractères.

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

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

Retour á la page du sommaire

Retour á la page du sommaire

Ajout et configuration d'utilisateurs iDRAC6

Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.1

Pour gérer votre système avec l'iDRAC6 et maintenir la sécurité du système, créez des utilisateurs exclusifs et octroyez-leur des droits d'administration spécifiques (*autorisation 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 l'iDRAC6 et maintenir la sécurité du système, créez des utilisateurs exclusifs et octroyez-leur des droits d'administration spécifiques (*autorisation basée sur les rôles*).

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

REMARQUE : Vous devez disposer du privilège de **configuration d'utilisateur** pour configurer un utilisateur iDRAC.

1. Cliquez sur **Accès distant**→ **Configuration**→ **Utilisateurs**.

   La page Utilisateurs affiche les informations suivantes sur les utilisateurs iDRAC : **ID d'utilisateur, État (activé/désactivé), Nom d'utilisateur, Privilège RAC**, **Privilège IPMI LAN**, **Privilège IPMI série** et état **Série sur LAN (activé/désactivé)**. Le Tableau 6-1 décrit les états et les autorisations d'utilisateur pour configurer les utilisateurs iDRAC.

   REMARQUE : Utilisateur-1 est réservé pour l'utilisateur anonyme IPMI et n'est pas configurable.

2. Dans la colonne **ID d'utilisateur**, cliquez sur un ID d'utilisateur.

   Dans la page **Menu principal de l'utilisateur**, vous pouvez configurer un utilisateur, consulter un certificat d'utilisateur, envoyer un certificat d'une autorité de certification (CA) de confiance ou consulter un certificat CA de confiance.

   Si vous sélectionnez **Configurer l'utilisateur** et cliquez sur **Suivant**, la page **Configuration de l'utilisateur** apparaît. Passez à l'étape 4.

   Si vous sélectionnez les options sous **Configuration de la carte à puce**, consultez le Tableau 6-2.

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 existant. Le Tableau 6-3 décrit les **Paramètres généraux de l'utilisateur**.
   - Les privilèges d'utilisateur IPMI. 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 modifications**.

5. Cliquez sur le bouton approprié pour continuer. Reportez-vous au Tableau 6-7.

Tableau 6-1. États et droits des utilisateurs

Paramètre	Description
ID d'utilisateur	Affiche la liste séquentielle des numéros d'identification des utilisateurs. Chaque champ sous **ID d'utilisateur** contient l'un des 16 numéros d'utilisateur prédéfinis. Ce champ ne peut pas être modifié.
État	Affiche l'état de connexion de l'utilisateur : Activé ou Désactivé. Désactivé est la valeur par défaut. **REMARQUE :** L'utilisateur 2 est activé par défaut.
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. **REMARQUE :** Les noms d'utilisateur iDRAC6 ne peuvent pas comporter les caractères **/** (barre oblique) ou **.** (point).

	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.
Privilège du RAC	Définit le groupe (niveau de privilège) auquel l'utilisateur est affecté (Administrateur, Opérateur, Lecture seule ou Aucun).
Privilège LAN IPMI	Affiche le niveau de privilège LAN IPMI auquel l'utilisateur est affecté (Administrateur, Opérateur, Lecture seule ou Aucun).
Privilège série IPMI	Affiche le niveau de privilège de port série IPMI auquel l'utilisateur est affecté (Administrateur, Opérateur, Lecture seule ou Aucun).
Série sur LAN	Permet/interdit à l'utilisateur d'utiliser les communications série sur LAN IPMI.

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

Option	Description
Consulter le Certificat de l'utilisateur	Affiche la page Certificat de l'utilisateur qui a été téléchargée sur l'iDRAC.
Télécharger le Certificat CA de confiance	Vous permet de télécharger le certificat CA de confiance sur l'iDRAC et de l'importer dans le profil de l'utilisateur.
Consulter le certificat CA de confiance	Affiche le certificat CA de confiance qui a été téléchargé sur l'iDRAC. Le certificat CA de confiance est émis par la CA qui est autorisée à délivrer des certificats aux utilisateurs.

Tableau 6-3. Paramètres généraux de l'utilisateur

ID d'utilisateur	L'un des 16 numéros d'utilisateur prédéfinis.
Activer l'utilisateur	Lorsqu'elle est cochée, cette propriété indique que l'accès de l'utilisateur à iDRAC6 est activé. Lorsqu'elle est décochée, l'accès utilisateur est désactivé.
Nom d'utilisateur	Un nom d'utilisateur comportant jusqu'à 16 caractères.
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** de 20 caractères maximum. Les caractères ne sont pas affichés.
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 maximum de l'utilisateur accordé sur le LAN	Spécifie le privilège maximum de l'utilisateur sur le canal IPMI LAN sur l'un des groupes d'utilisateurs suivants : **Administrateur**, **Opérateur**, **Utilisateur** ou **Aucun**.
Privilège maximum de l'utilisateur accordé sur le port série	Spécifie le privilège maximum de l'utilisateur sur le canal IPMI série sur l'un des groupes d'utilisateurs suivants : **Administrateur**, **Opérateur**, **Utilisateur** ou **Aucun**.
Activer la connexion série sur le réseau local	Permet à l'utilisateur d'utiliser les communications série sur le LAN IPMI. Lorsque cette option est sélectionnée, ce privilège est activé.

Tableau 6-5. Privilèges utilisateur iDRAC

Propriété	Description
Rôles	Spécifie le privilège maximum de l'utilisateur iDRAC sur l'un des suivants : **Administrateur**, **Opérateur**, **Lecture seule** ou **Aucun**. Voir Tableau 6-6 pour connaître les **Droits d'accès du groupe iDRAC**.
Ouvrir une session iDRAC	Permet à l'utilisateur d'ouvrir une session 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.
Effacer les journaux	Permet à l'utilisateur d'effacer les journaux iDRAC.
Exécuter les commandes de contrôle du serveur	Permet à l'utilisateur d'exécuter des commandes Server Control.
Accéder à la redirection de console	Permet à l'utilisateur d'exécuter la redirection de console.
Accéder au média virtuel	Permet à l'utilisateur d'exécuter et d'utiliser le média virtuel.
Tester les alertes	Permet à l'utilisateur d'envoyer des alertes de test (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 Groupe iDRAC

Groupe d'utilisateurs	Droits accordés
Administrateur	**Ouverture de session iDRAC**, **Configuration d'iDRAC**, **Configuration des utilisateurs**, **Effacement des journaux**, **Exécution des commandes de contrôle du serveur**, **Accès à la redirection de console**, **Accès au média virtuel**, **Test des alertes**, **Exécution des commandes de diagnostic**
Opérateur	Sélectionne parmi les autorisations suivantes : **Ouverture de session iDRAC**, **Configuration d'iDRAC**, **Configuration des utilisateurs**, **Effacement des journaux**, **Exécution des commandes d'action du serveur**, **Accès à la redirection de console**, **Accès au média virtuel**, **Test des alertes**, **Exécution des commandes de diagnostic**
Lecture seule	**Ouvrir une session iDRAC**
None (Aucun)	Aucun droit attribué

Tableau 6-7. Boutons de la page Configuration de l'utilisateur

Bouton	Action
Imprimer	Imprime les valeurs de **Configuration utilisateur** qui apparaissent à l'écran.
Actualiser	Recharge la page **Configuration utilisateur**.
Retour à la page Utilisateurs	Retourne à la **page Utilisateurs**.
Appliquer les modifications	Enregistre les nouveaux paramètres définis pour la configuration utilisateur.

Utilisation de l'utilitaire 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 seul ou plusieurs utilisateurs iDRAC6 peuvent être configurés via 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 ce fichier séquentiel sur chaque système géré.
- Créez le fichier de configuration de l'iDRAC6 comme décrit dans « Présentation de la sous-commande RACADM » et exécutez la sous-commande **racadm config** sur chaque système géré avec le 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 et le mot de passe calvin. La sous-commande **racresetcfg** restaure les paramètres d'origine de l'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 alors perdue.

REMARQUE : Les utilisateurs peuvent être activés et désactivés à tout moment. Par conséquent, un utilisateur peut avoir un nombre 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 consulter ou modifier le fichier **monfichier.cfg** qui contient tous les paramètres de configuration de l'iDRAC6.

Plusieurs paramètres et ID d'objets 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 pas 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 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 :
   - Privilège iDRAC
   - Privilège LAN IPMI
   - Privilège série IPMI
   - Privilège série sur LAN
4. Activez l'utilisateur.

Exemple

L'exemple suivant décrit comment ajouter un nouvel utilisateur appelé « Jean » avec un mot de passe « 123456 » et des privilèges d'ouverture de session au RAC.

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i 2 jean

racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 123456

racadm config -g cfgUserAdmin -i 2 -o cfgUserAdminPrivilege 0x00000001

racadm config -g cfgUserAdmin -i 2 -o 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 jean

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 RAC :

```
racadm config -g cfgUserAdmin -o cfgUserAdminUserName -i <index> ""
```

Une chaîne de guillemets nulle ("") donne l'ordre à iDRAC6 de supprimer la configuration utilisateur à l'index indiqué et de restaurer les valeurs d'usine par défaut de la configuration utilisateur.

Activation d'un utilisateur iDRAC6 avec des droits

Pour activer un utilisateur avec des droits administratifs spécifiques (autorité basé sur les rôles), localisez tout d'abord un index utilisateur disponible en effectuant les étapes dans « Avant de commencer ». Tapez ensuite les lignes de commande suivantes en incluant le nouveau nom d'utilisateur et le nouveau mot de passe.

REMARQUE : Voir Tableau B-2 pour une liste des valeurs de masque binaire valides correspondant à des privilèges d'utilisateur spécifiques. La valeur de privilège par défaut est 0, qui indique que l'utilisateur n'a aucun privilège activé.

```
racadm config -g cfgUserAdmin -o cfgUserAdminPrivilege -i <index> <valeur de masque binaire du privilège d'utilisateur>
```

Retour á la page du sommaire

Retour á la page du sommaire

Utilisation d'iDRAC6 avec Microsoft Active Directory

Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.1

Un service d'annuaire permet de maintenir une base de données commune rassemblant toutes les informations nécessaires au contrôle des utilisateurs, des ordinateurs, des imprimantes, etc. d'un réseau. Si votre société utilise le logiciel de service Microsoft® Active Directory®, vous pouvez le configurer pour accéder à l'iDRAC6, ce qui vous permet d'ajouter et de contrôler les privilèges utilisateur iDRAC6 pour les utilisateurs existants dans votre logiciel Active Directory.

REMARQUE : L'utilisation d'Active Directory pour reconnaître les utilisateurs de l'iDRAC6 est prise en charge sur les systèmes d'exploitation Microsoft Windows® 2000, Windows Server® 2003 et Windows Server 2008.

La Tableau 7-1 affiche les neuf privilèges utilisateur Active Directory iDRAC6.

Tableau 7-1. Privilèges utilisateur iDRAC6

Droits	Description
Ouvrir une session iDRAC	Permet à l'utilisateur d'ouvrir une session iDRAC6.
Configurer iDRAC	Permet à l'utilisateur de configurer l'iDRAC6.
Configurer les utilisateurs	Permet à l'utilisateur de permettre à des utilisateurs spécifiques d'accéder au système.
Effacer les 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 redirection de console	Permet à l'utilisateur d'exécuter la redirection de console.
Accéder au média virtuel	Permet à l'utilisateur d'exécuter et d'utiliser le média virtuel.
Tester les alertes	Permet à l'utilisateur d'envoyer des alertes de test (e-mail et PET) à un utilisateur spécifique.
Exécuter des commandes de diagnostic	Permet à l'utilisateur d'exécuter des commandes de diagnostic.

Pré requis pour l'activation de l'authentification Active Directory pour l'iDRAC6.

Pour utiliser la fonctionnalité d'authentification d'Active Directory de l'iDRAC6, vous devez déjà avoir déployé une infrastructure Active Directory. Consultez le site Web Microsoft pour des informations sur la configuration d'une infrastructure Active Directory si vous n'en avez pas déjà une.

L'iDRAC6 utilise l'infrastructure à clé publique (PKI) standard pour s'authentifier en toute sécurité sur Active Directory et vous aurez donc également besoin d'une PKI intégrée dans l'infrastructure Active Directory. Consultez le site Web Microsoft pour plus d'informations sur la configuration de PKI.

Pour vous authentifier correctement sur tous les contrôleurs de domaine, vous devrez également activer le protocole Secure Socket Layer (SSL) sur tous les contrôleurs de domaine auxquels se connecte l'iDRAC6. Pour des informations plus spécifiques, consultez « Activation de SSL sur un contrôleur de domaine ».

Mécanismes d'authentification Active Directory pris en charge

Vous pouvez utiliser Active Directory pour définir l'accès de l'utilisateur sur l'iDRAC6 au moyen de deux méthodes : vous pouvez utiliser la solution *schéma étendu* que Dell a personnalisée pour y ajouter des objets Active Directory définis par Dell ou vous pouvez utiliser la solution *schéma standard* qui utilise uniquement les objets du groupe Active Directory. Reportez-vous aux sections suivantes pour plus d'informations sur ces solutions.

Lorsque vous utilisez Active Directory pour configurer l'accès à l'iDRAC6, vous devez choisir la solution de schéma étendu ou 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 nécessaire 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.

Extension du schéma Active Directory

Important : l'extension de schéma de ce produit est différente de celle des générations précédentes des produits de gestion à distance Dell. Vous devez étendre le nouveau schéma et installer le nouveau snap-in Utilisateurs et ordinateurs d'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 d'Active Directory n'a aucun impact sur les versions précédentes de ce produit.

L'extendeur de schéma et l'extension snap-in MMC Utilisateurs et ordinateurs d'Active Directory sont disponibles sur le DVD *Dell Systems Management Tools and Documentation*. Pour plus d'informations, voir « Extension du schéma Active Directory » et « Installation de l'extension Dell sur le snap-in Utilisateurs et ordinateurs d'Active Directory ». Pour plus d'informations sur l'extension du schéma pour l'iDRAC6 et l'installation du snap-in MMC Utilisateurs et ordinateurs d'Active Directory, consultez le *Guide d'installation et de sécurité de Dell OpenManage* disponible à l'adresse **support.dell.com\manuals**.

REMARQUE : Lorsque vous créez des objets Association iDRAC ou des objets Périphérique iDRAC, assurez-vous de sélectionner **Objet avancé Gestion à distance Dell**.

Extensions de schéma Active Directory

Les données d'Active Directory constituent une base de données distribuée d'attributs et de classes. Le schéma d'Active Directory inclut les règles qui déterminent le type de données peuvent être ajoutées ou incluses dans la base de données. La classe d'utilisateur est un exemple de classe qui est conservée dans la base de données. 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 uniques pour répondre aux besoins spécifiques à 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 d'Active Directory existant peut être défini par un ID unique. Pour que les ID soient uniques dans toute l'industrie, Microsoft maintient une base de données d'identificateurs 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 avec d'autres. Pour étendre le schéma de Microsoft Active Directory, Dell a reçu des OID uniques, des extensions de noms uniques et des ID d'attributs uniques liés pour les attributs et les classes ajoutés au service d'annuaire.

L'extension de Dell est : dell

L'OID de base de Dell est : 1.2.840.113556.1.8000.1280

La plage des ID de liens du RAC est : 12070 à 12079

Présentation des extensions de schéma de l'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 de l'iDRAC et de périphériques iDRAC sur le réseau, sans ajouter trop de complexité.

Aperçu des objets Active Directory

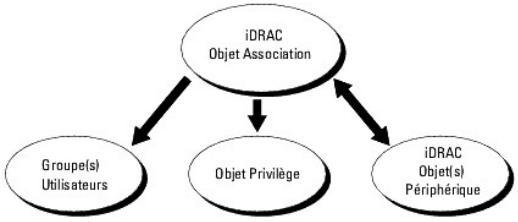
Pour chacun des iDRAC physiques présents sur le réseau que vous voulez intégrer à Active Directory en vue de l'authentification et de l'autorisation, vous devez créer au moins un objet Association et un objet Périphérique iDRAC. Vous pouvez créer plusieurs objets Association et chaque objet Association peut être lié à autant d'utilisateurs, de groupes d'utilisateurs ou d'objets Périphérique iDRAC que vous le souhaitez. 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 l'administrateur de contrôler les privilèges de chaque utilisateur sur des iDRAC spécifiques.

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



Vous pouvez créer autant d'objets Association que vous le voulez. 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 en gérer 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 objet Privilège par objet Association. L'objet Association connecte les *Utilisateurs* qui ont des *Privilèges* sur les contrôleurs iDRAC.

L'extension Dell sur le snap-in Utilisateurs et ordinateurs d'Active Directory 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.

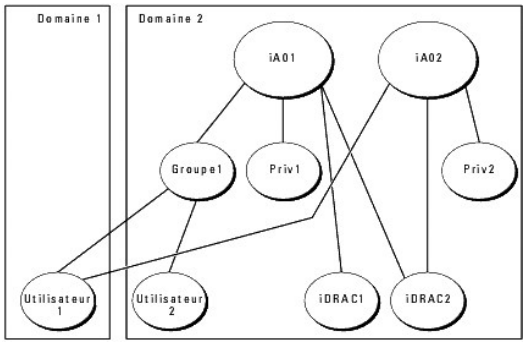
Les utilisateurs, groupes d'utilisateurs ou groupes d'utilisateurs imbriqués depuis tout domaine peuvent être ajoutés dans l'objet Association. Les solutions de schéma étendu prennent en charge tout groupe d'utilisateurs et toute imbrication de groupes d'utilisateurs à travers plusieurs domaines autorisés 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 l'iDRAC2 via les deux objets associés. Par conséquent, Utilisateur1 a accumulé des privilèges résultant de l'association de l'ensemble des privilèges pour les objets Priv1 et Priv2 sur l'iDRAC2.

Par exemple, Priv1 possède les privilèges Ouvrir une session, Média virtuel et Effacer les journaux et Privr2 a les privilèges Ouvrir une session iDRAC, Configurer l'iDRAC et Tester les alertes. Par conséquent, Utilisateur1 a maintenant l'ensemble des privilèges : Ouvrir une session iDRAC, Média virtuel, Effacer les journaux, Configurer l'iDRAC et Tester les alertes, 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 maximum 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 l'iDRAC2. Utilisateur1 possède seulement les privilèges Priv1 sur l'iDRAC. Utilisateur2 possède les privilèges Priv1 sur l'iDRAC1 et l'iDRAC2. En outre, cette figure illustre que l'utilisateur1 peut être dans un domaine différent et être un membre d'un groupe imbriqué.

Configuration du schéma étendu d'Active Directory pour accéder à iDRAC

Pour pouvoir utiliser Active Directory pour accéder à l'iDRAC6, configurez le logiciel Active Directory et l'iDRAC6 en effectuant les étapes suivantes dans l'ordre :

1. Étendez le schéma Active Directory (voir « Extension du schéma Active Directory »).
2. Étendez le snap-in Utilisateurs et ordinateurs Active Directory (voir « Installation de l'extension Dell sur le snap-in Utilisateurs et ordinateurs Active Directory »).
3. Ajoutez des utilisateurs iDRAC6 et leurs privilèges à Active Directory (voir « Ajout d'utilisateurs iDRAC et de leurs privilèges à Active Directory »).

4. Activez SSL sur chacun de vos contrôleurs de domaine (voir « Activation de SSL sur un contrôleur de domaine »).

5. Configurez les propriétés Active Directory de iDRAC6 via l'interface Web de l'iDRAC6 ou RACADM (voir « Configuration d'Active Directory avec le schéma étendu en utilisant l'interface Web iDRAC6. » ou « Configuration d'Active Directory avec le schéma étendu via RACADM »).

En étendant le schéma Active Directory, vous ajoutez une unité d'organisation 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) contrôleur 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, l'unité organisationnelle Dell ne sera pas ajoutée au schéma.

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

- *Lecteur DVD* **:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\LDIF_Files**
- <Lecteur **DVD >:\SYSMGMT\ManagementStation\support\OMActiveDirectory_Tools\Remote_Management_Advanced\Schema Extender**

Pour utiliser les fichiers LDIF, reportez-vous aux 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 ».

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 saisissez l'avertissement, puis cliquez sur **Suivant**.
3. Sélectionnez **Utiliser les références d'ouverture de session actuelles** ou saisissez un nom d'utilisateur et un mot de passe ayant des droits d'administrateur de schéma.
4. Cliquez sur **Suivant** pour exécuter Dell Schema Extender.
5. Cliquez sur **Terminer**.

   Le schéma est étendu. Pour vérifier l'extension de schéma, utilisez la console de gestion de Microsoft (MMC) et le snap-in du schéma Active Directory pour vérifier ce qui suit :

   - Classes (voir Tableau 7-2 à Tableau 7-7)
   - Attributs (Tableau 7-8)

Consultez votre documentation Microsoft pour des informations supplémentaires sur l'utilisation de 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 attribué (OID)
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 l'iDRAC d'envoyer des requêtes LDAP (Lightweight Directory Access Protocol) à Active Directory.
Type de classe	Classe structurelle
SuperClasses	dellProduct

Attributs	**dellSchemaVersion** **dellRacType**

Tableau 7-4. delliDRACAssociationObject Class

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** **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 (Aucun)
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	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/Identificateur d'objet de syntaxe	Valeur unique
dellPrivilegeMember Liste des objets dellPrivilege qui appartiennent à cet attribut.	1.2.840.113556.1.8000.1280.1.1.2.1 Nom distingué (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellProductMembers	1.2.840.113556.1.8000.1280.1.1.2.2	FALSE

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. Numéro de lien : 12070	Nom distingué (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
dellIsLoginUser TRUE si l'utilisateur a les droits Ouvrir une session sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.3 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsCardConfigAdmin TRUE si l'utilisateur a les droits Configuration de carte sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.4 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsUserConfigAdmin TRUE si l'utilisateur a les droits Configuration d'utilisateur sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.5 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsLogClearAdmin TRUE si l'utilisateur a les droits Effacement de journal sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.6 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsServerResetUser TRUE si l'utilisateur a les droits Réinitialisation de serveur sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.7 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsConsoleRedirectUser TRUE si l'utilisateur a les droits Redirection de console sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.8 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsVirtualMediaUser TRUE si l'utilisateur a les droits Média virtuel sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.9 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsTestAlertUser TRUE si l'utilisateur a les droits Tests d'alerte utilisateur sur le périphérique.	1.2.840.113556.1.8000.1280.1.1.2.10 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellIsDebugCommandAdmin 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 Booléen (LDAPTYPE_BOOLEAN 1.3.6.1.4.1.1466.115.121.1.7)	TRUE
dellSchemaVersion La version de schéma courante est utilisée pour mettre à jour le schéma.	1.2.840.113556.1.8000.1280.1.1.2.12 Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellRacType Cet attribut est le type courant de RAC 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 Case Ignore String (LDAPTYPE_CASEIGNORESTRING 1.2.840.113556.1.4.905)	TRUE
dellAssociationMembers Liste des dellAssociationObjectMembers appartenant à ce produit. Cet attribut est le lien vers l'arrière vers l'attribut dellProductMembers. ID de lien : 12071	1.2.840.113556.1.8000.1280.1.1.2.14 Nom distingué (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE

Installation de l'extension Dell sur le snap-in Utilisateurs et ordinateurs Active Directory

Lorsque vous étendez le schéma dans Active Directory, vous devez également étendre le snap-in Utilisateurs et ordinateurs d'Active Directory pour que l'administrateur puisse gérer les périphériques iDRAC, les utilisateurs et les groupes d'utilisateurs, les associations de iDRAC et les privilèges de iDRAC.

Lorsque vous installez votre logiciel Systems Management à l'aide du DVD *Dell Systems Management Tools and Documentation*, vous pouvez installer le snap-in en sélectionnant l'option **Extension Dell du snap-in Utilisateurs et ordinateurs d'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. Pour les systèmes d'exploitation Windows 64 bits, le programme d'installation du Snap-in se trouve sous **<lecteur DVD>:\SYSMGMT\ManagementStation\support\OMActiveDirectory_SnapIn64**

Pour des informations supplémentaires sur le snap-in Utilisateurs et ordinateurs d'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 visualiser l'objet iDRAC Dell dans le conteneur.

Pour plus d'informations, voir la section « Ouverture du snap-in Utilisateurs et ordinateurs Active Directory ».

Ouverture du snap-in Utilisateurs et ordinateurs Active Directory

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

1. Si vous êtes connecté au 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, la version appropriée du pack administrateur Microsoft doit être installée sur votre système local. Pour installer ce pack administrateur, cliquez sur **Démarrer**→ **Exécuter**, entrez `MMC` et appuyez sur **Entrée**.

   La console 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** et cliquez sur **OK**.

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

Le snap-in Utilisateurs et ordinateurs d'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, procédez comme suit :

- Créer un objet de périphérique iDRAC
- Créer un objet Privilège
- Créer un objet Association
- Configuration d'un objet Association

Création d'un objet de périphérique iDRAC

1. Dans la fenêtre **Racine de la console** MMC, effectuez un clic droit sur un conteneur.

2. Sélectionnez **Nouveau**→ **Objet avancé Gestion à distance Dell**.

   La fenêtre **Nouvel objet** s'affiche.

3. Tapez un nom pour le nouvel objet. Ce nom doit être identique au nom de iDRAC saisi à l'étape A de « Configuration d'Active Directory avec le schéma étendu en utilisant l'interface Web iDRAC6. ».

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, effectuez un clic droit sur un conteneur.

2. Sélectionnez **Nouveau**→ **Objet avancé Gestion à distance Dell**.

   La fenêtre **Nouvel objet** s'affiche.

3. Tapez un nom pour le nouvel objet.

4. Sélectionnez **Objet Privilège**.

5. Cliquez sur **OK**.

6. Effectuez un clic droit sur l'objet Privilège que vous avez créé et sélectionnez **Propriétés**.

7. Cliquez sur l'onglet **Privilèges de gestion avancée** 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, effectuez un clic droit sur un conteneur.
2. Sélectionnez **Nouveau→ Objet avancé Gestion à distance Dell**.

   Cela ouvre la fenêtre **Nouvel objet**.
3. Tapez un nom pour le nouvel objet.
4. Sélectionnez **Objet Association**.
5. Sélectionnez l'étendue de **l'objet Association**.
6. Cliquez sur **OK**.

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. Effectuez un clic droit sur **l'objet Association** et sélectionnez **Propriétés**.
2. Sélectionnez l'onglet **Utilisateurs** et cliquez sur **Ajouter**.
3. Tapez le nom de l'utilisateur ou du groupe d'utilisateurs et cliquez sur **OK**.

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

Ajout de privilèges

1. Sélectionnez l'onglet **Objet Privilèges** et cliquez sur **Ajouter**.
2. Tapez 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 d'Active Directory avec le schéma étendu en utilisant l'interface Web iDRAC6.

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

2. Connectez-vous à l'interface Web iDRAC6.
3. Développez l'arborescence du **système** et cliquez sur **Accès distant**.
4. Cliquez sur l'onglet **Configuration** et sélectionnez **Active Directory**.
5. Allez à la fin de l'écran **Configuration et gestion d'Active Directory**, et cliquez sur **Configurer Active Directory**.

   L'écran **Étape 1/4 Configuration et gestion d'Active Directory** apparaît.
6. Sous **Paramètres du certificat**, cochez la case **Activer la validation des certificats** si vous voulez valider le certificat SSL de vos serveurs Active Directory ; sinon, passez à l'étape 9.
7. Sous **Téléverser le certificat CA d'Active Directory**, entrez le chemin de fichier du certificat ou naviguez pour trouver le fichier du certificat.

   REMARQUE : Vous devez entrer le chemin de fichier absolu, y compris le chemin et le nom de fichier complets et l'extension du fichier.
8. Cliquez sur **Téléverser**.

   Les informations concernant le certificat CA d'Active Directory que vous avez téléversé apparaissent.
9. Sous **Téléverser le keytab Kerberos**, entrez le chemin du fichier keytab ou naviguez pour accéder au fichier. Cliquez sur **Téléverser**. Le keytab Kerberos sera téléversé dans l'iDRAC6.
10. Cliquez sur **Suivant** pour passer à l'**Étape 2/4 Configuration et gestion d'Active Directory**.
11. Cliquez sur **Activer Active Directory**.

PRÉCAUTION : Dans cette version, les fonctionnalités TFA (Two Factor Authentication [Authentification bifactorielle]) basée sur la carte à puce et SSO (single sign-on [ouverture de session individuelle]) ne sont pas prises en charge si Active Directory est configuré pour le schéma étendu.

12. Cliquez sur **Ajouter** pour saisir le nom de domaine utilisateur.
13. Entrez le nom de domaine utilisateur dans l'invite, puis cliquez sur **OK**. Notez que cette étape est facultative. 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 entrer le nom d'utilisateur.
14. Tapez le **Délai d'attente** en secondes pour spécifier le temps que l'iDRAC6 doit attendre avant d'obtenir une réponse d'Active Directory. La valeur par défaut est 120 secondes.
15. Entrez l'Adresse du serveur du contrôleur de domaine. Vous pouvez entrer jusqu'à trois serveurs Active Directory pour la procédure d'ouverture de session, mais vous devez configurer au moins un serveur en entrant l'adresse IP ou le nom de domaine pleinement qualifié (FQDN). l'iDRAC6 tente de se connecter à chaque serveur configuré jusqu'à ce qu'une connexion soit établie.

    REMARQUE : Le FQDN ou l'adresse IP que vous spécifiez dans ce champ doit correspondre au champ Sujet ou Nom alternatif du sujet de votre certificat du contrôleur de domaine si la validation des certificats est activée.
16. Cliquez sur **Suivant** pour passer à l'**Étape 3/4 Configuration et gestion d'Active Directory**.
17. Sous **Sélection du schéma**, cliquez sur **Schéma étendu.**
18. Cliquez sur **Suivant** pour passer à l'**Étape 4/4 Configuration et gestion d'Active Directory**.
19. Sous **Paramètres du schéma étendu**, entrez le nom de l'iDRAC et son nom de domaine pour configurer l'objet du périphérique iDRAC. Le nom de domaine de l'iDRAC est le domaine dans lequel l'objet DRAC est créé.
20. Cliquez sur **Terminer** pour enregistrer les paramètres du schéma étendu d'Active Directory.

    Le serveur Web de l'iDRAC vous renvoie automatiquement à l'écran **Configuration et gestion d'Active Directory**.
21. Cliquez sur **Paramètres de test** pour vérifier les paramètres du schéma étendu d'Active Directory.
22. Tapez vos nom d'utilisateur et mot de passe Active Directory.

    Les résultats du test et le journal du test sont affichés. Pour plus d'informations, voir « Test de vos configurations ».

    REMARQUE : Vous devez posséder un serveur DNS correctement configuré sur iDRAC pour prendre en charge l'ouverture de session Active Directory. Naviguez vers la page **Accès distant**→ **Configuration**→ **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 d'Active Directory avec le schéma étendu via RACADM

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

1. Ouvrez une invite de commande et entrez 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 cfgDomainController1 <nom de domaine pleinement qualifié ou adresse IP du contrôleur de domaine>
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgDomainController2 <nom de domaine pleinement qualifié ou adresse IP du contrôleur de domaine>
   ```

   ```
   racadm config -g cfgActiveDirectory -o cfgDomainController3 <nom de domaine pleinement qualifié ou adresse IP du contrôleur de domaine>
   ```

   REMARQUE : Au moins l'une des 3 adresses doit être configurée. Le iDRAC tente de se connecter à chacune des adresses configurées une par une jusqu'à ce qu'une connexion soit établie. Lorsque l'option de schéma étendu est sélectionnée, ces adresses sont les adresses FQDN ou IP des contrôleurs de domaine où se trouve le 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 Sujet ou Nom alternatif du sujet de votre certificat du contrôleur de domaine si la validation des certificats est activée.

   PRÉCAUTION : Dans cette version, les fonctionnalités TFA (Two Factor Authentication [Authentification bifactorielle]) basée sur la carte à puce et SSO (single sign-on [ouverture de session individuelle]) ne sont pas prises en charge si Active Directory est configuré pour le schéma étendu.

   Pour désactiver la validation des certificats durant la négociation SSL, entrez la commande RACADM suivante :

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

   Dans ce cas, il n'est pas nécessaire de téléverser un certificat CA.

   Pour faire respecter la validation des certificats durant la négociation SSL, entrez la commande RACADM suivante :

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

   Dans ce cas, vous devez téléverser un certificat CA en utilisant la commande RACADM suivante :

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

   ```
   racadm sslcertupload -t 0x2 -f <certificat CA racine ADS>
   ```

   L'utilisation de la commande RACADM suivante peut être facultative. Pour plus d'informations, voir « Importation du certificat SSL du micrologiciel iDRAC6 ».

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

2. Si DHCP est activé sur l'iDRAC et que vous voulez utiliser le nom DNS fourni par le serveur DHCP, entrez la commande RACADM suivante :

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

3. Si DHCP est désactivé sur l'iDRAC ou que vous voulez entrer manuellement les adresses IP DNS, entrez 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>
   ```

4. Si vous voulez configurer une liste de domaines utilisateur afin que vous ayez seulement besoin d'entrer le nom d'utilisateur durant l'ouverture de session sur l'interface Web iDRAC6, entrez 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.

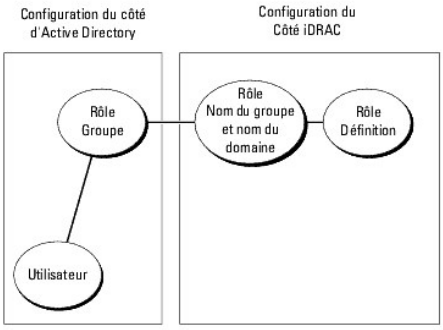
   Voir « Utilisation d'Active Directory pour ouvrir une session iDRAC6 » pour plus de détails sur les domaines utilisateur.

5. 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 la 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 de l'iDRAC avec Microsoft Active Directory et le schéma standard



Du côté d'Active Directory, un objet de groupe standard est utilisé comme groupe de rôles. Un utilisateur ayant accès à l'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 niveau des rôles et des privilèges est défini sur chaque iDRAC6 et non pas dans Active Directory. Vous pouvez configurer et définir un maximum de cinq groupes de rôles sur chaque iDRAC. Le Tableau 7-9 affiche les privilèges par défaut des groupes de rôles.

Tableau 7-9. Privilèges par défaut des groupes de rôles

Groupes de rôles	Niveau de privilège par défaut	Droits accordés	Masque binaire
Groupe de rôles 1	Administrateur	**Ouverture de session iDRAC**, **Configuration d'iDRAC**, **Configuration des utilisateurs**, **Effacement des journaux**, **Exécution des commandes de contrôle du serveur**, **Accès à la redirection de console**, **Accès au média virtuel**, **Test des alertes**, **Exécution des commandes de diagnostic**	0x000001ff
Groupe de rôles 2	Opérateur	**Ouverture de session iDRAC**, **Configuration de iDRAC**, **Exécution des commandes de contrôle du serveur**, **Accès à la redirection de console**, **Accès au média virtuel, Test des alertes, Exécution des commandes de diagnosti**c	0x000000f9
Groupe de rôles 3	Lecture seule	Ouvrir une session iDRAC	0x00000001
Groupe de rôles 4	None (Aucun)	Aucun droit attribué	0x00000000
Groupe de rôles 5	None (Aucun)	Aucun droit attribué	0x00000000

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

Scénario de domaine unique et scénario à plusieurs domaines

Si tous les utilisateurs et groupes de rôles connectés 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 de domaine unique, tous les types de groupes sont pris en charge.

Si tous les utilisateurs et groupes de rôles connectés, 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 les groupes imbriqués, le cas échéant, doivent être des types de groupes universels.

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

Vous devez effectuer les étapes suivantes pour configurer Active Directory pour qu'un utilisateur Active Directory puisse accéder à l'iDRAC6 :

1. Sur un serveur Active Directory (contrôleur de domaine), ouvrez le **snap- in Utilisateurs et ordinateurs d'Active Directory**.
2. Créez un groupe ou sélectionnez un groupe existant. Le nom du groupe et le nom de ce domaine doivent être configurés sur iDRAC6 soit avec l'interface Web, soit RACADM (voir « Configuration d'Active Directory avec le schéma étendu en utilisant l'interface Web iDRAC6 » ou « Configuration d'Active Directory avec le schéma standard via RACADM »).
3. Ajoutez l'utilisateur Active Directory comme membre du groupe Active Directory pour qu'il puisse accéder à iDRAC.

Configuration d'Active Directory avec le schéma étendu en utilisant l'interface Web iDRAC6

1. Ouvrez une fenêtre d'un navigateur Web pris en charge.
2. Connectez-vous à l'interface Web iDRAC6.
3. Développez l'arborescence du **système** et cliquez sur **Accès distant**.
4. Cliquez sur l'onglet **Configuration** et sélectionnez **Active Directory**.
5. Allez à la fin de l'écran **Configuration et gestion d'Active Directory**, et cliquez sur **Configurer Active Directory**.

   L'écran **Étape 1/4 Configuration et gestion d'Active Directory** apparaît.
6. Sous **Paramètres du certificat**, cochez la case **Activer la validation des certificats** si vous voulez valider le certificat SSL de vos serveurs Active Directory ; sinon, passez à l'étape 9**.**
7. Sous **Téléverser le certificat CA d'Active Directory**, entrez le chemin de fichier du certificat ou naviguez pour trouver le fichier du certificat.

   REMARQUE : Vous devez entrer le chemin de fichier absolu, y compris le chemin et le nom de fichier complets et l'extension du fichier.
8. Cliquez sur **Téléverser**.

   Les informations concernant le certificat CA d'Active Directory valide s'affichent.
9. Sous **Téléverser le keytab Kerberos**, entrez le chemin du fichier keytab ou naviguez pour accéder au fichier. Cliquez sur **Téléverser**. Le keytab Kerberos est téléversé dans l'iDRAC6.
10. Cliquez sur **Suivant** pour passer à l'**Étape 2/4 Configuration et gestion d'Active Directory**.
11. Sélectionnez **Activer Active Directory**.
12. Sélectionnez **Activer l'ouverture de session individuelle** si vous souhaitez ouvrir une session iDRAC6 sans entrer vos références d'authentification utilisateur de domaine, par exemple le nom d'utilisateur et le mot de passe.
13. Cliquez sur **Ajouter** pour saisir le nom de domaine utilisateur.
14. Entrez le nom de domaine utilisateur dans l'invite, puis cliquez sur **OK**.
15. Tapez le **Délai d'attente** en secondes pour spécifier le temps que l'iDRAC6 doit attendre avant d'obtenir une réponse d'Active Directory. La valeur par défaut est 120 secondes.
16. Entrez l'Adresse du serveur du contrôleur de domaine. Vous pouvez entrer jusqu'à trois serveurs Active Directory pour la procédure d'ouverture de session, mais vous devez configurer au moins un serveur en entrant l'adresse IP ou le nom de domaine pleinement qualifié (FQDN). iDRAC6 tente de se connecter à chaque serveur configuré jusqu'à ce qu'une connexion soit établie.

    REMARQUE : Le FQDN ou l'adresse IP que vous spécifiez dans ce champ doit correspondre au champ Sujet ou Nom alternatif du sujet de votre certificat du contrôleur de domaine si la validation des certificats est activée.
17. Cliquez sur **Suivant** pour passer à l'**Étape 3/4 Configuration et gestion d'Active Directory**.
18. Sous **Sélection du schéma**, cliquez sur **Schéma standard.**
19. Cliquez sur **Suivant** pour passer à l'**Étape 4a/4** de l'**écran Configuration et gestion d'Active Directory**.
20. Sous **Paramètres du schéma standard,** entrez l'adresse du serveur de catalogue global pour spécifier son emplacement dans Active Directory. Vous devez configurer l'emplacement d'au moins un serveur de catalogue global.

    REMARQUE : Le FQDN ou l'adresse IP que vous spécifiez dans ce champ doit correspondre au champ Sujet ou Nom alternatif du sujet de votre certificat du contrôleur de domaine si la validation des certificats est activée.

    REMARQUE : Le serveur de catalogue global n'est requis que pour le schéma standard pour le cas où les comptes 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.
21. Sous **Groupes de rôles**, cliquez sur un **Groupe de rôles**.

    L'écran de l'**Étape 4b/4** s'affiche.
22. 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.

23. Spécifiez le **Domaine du groupe de rôles** qui est le domaine du groupe de rôles.

24. Spécifier les **Privilèges du groupe de rôles** en sélectionnant le **Niveau des privilèges du groupe de rôles**. Par exemple, si vous sélectionnez **Administrateur**, tous les privilèges sont sélectionnés pour ce niveau de droits.

25. Cliquez sur **Appliquer** pour enregistrer les paramètres du groupe de rôles.

    Le serveur Web de l'iDRAC6 vous renvoie automatiquement à l'écran de l'**Étape 4a/4 Configuration et gestion d'Active Directory où vos paramètres sont affichés.**

26. Répétez étape 20 les étapes étape 25 pour configurer des groupes de rôles supplémentaires

27. Cliquez sur **Terminer** pour revenir à l'écran **Configuration et gestion d'Active Directory**.

28. Cliquez sur les **Paramètres de test** pour vérifier les paramètres du schéma standard d'Active Directory.

29. Tapez vos nom d'utilisateur et mot de passe iDRAC6.

    Les résultats du test et le journal du test sont affichés. Pour plus d'informations, voir « Test de vos configurations ».

REMARQUE : Vous devez posséder un serveur DNS correctement configuré sur iDRAC pour prendre en charge l'ouverture de session Active Directory. Naviguez vers la page **Accès distant**→ **Configuration**→ **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 d'Active Directory avec le schéma standard via RACADM

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

1. Ouvrez une invite de commande et entrez 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 commun 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 utilisateurs spécifiques>

   REMARQUE : Pour les valeurs numériques Masque binaire, voir Tableau B-2.

   racadm config -g cfgActiveDirectory -o cfgDomainController1 <nom de domaine pleinement qualifié ou adresse IP du contrôleur de domaine>

   racadm config -g cfgActiveDirectory -o cfgDomainController2 <nom de domaine pleinement qualifié ou adresse IP du contrôleur de domaine>

   racadm config -g cfgActiveDirectory -o cfgDomainController3 <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 Sujet ou Nom alternatif du sujet de votre certificat du contrôleur de domaine si la validation des certificats est activée.

   REMARQUE : Entrez le FQDN du contrôleur de domaine, *et non* le FQDN du domaine uniquement. Par exemple, entrez `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.

   racadm config -g cfgActiveDirectory -o cfgGlobal Catalog1 <nom de domaine pleinement qualifié ou adresse IP du contrôleur de domaine>

   racadm config -g cfgActiveDirectory -o cfgGlobal Catalog1 <nom de domaine pleinement qualifié ou adresse IP du contrôleur de domaine>

   racadm config -g cfgActiveDirectory -o cfgGlobal 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 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 Sujet ou Nom alternatif du sujet de votre certificat du contrôleur de domaine si la validation des certificats est activée.

Pour désactiver la validation des certificats durant la négociation SSL, entrez la commande RACADM suivante :

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

Dans ce cas, aucun certificat CA ne doit être téléversé.

Pour faire respecter la validation des certificats durant la négociation SSL, entrez la commande RACADM suivante :

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

Dans ce cas, vous devez également téléverser le certificat CA en utilisant la commande RACADM suivante :

```
racadm sslcertupload -t 0x2 -f <certificat CA racine ADS>
```

L'utilisation de la commande RACADM suivante peut être facultative. Pour plus d'informations, voir « Importation du certificat SSL du micrologiciel iDRAC6 ».

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

2. Si DHCP est activé sur l'iDRAC6 et que vous voulez utiliser le nom DNS fourni par le serveur DHCP, entrez les commandes RACADM suivantes :

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

3. Si DHCP est désactivé sur l'iDRAC6 ou que vous voulez entrer manuellement les adresses IP DNS, entrez 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 du DNS secondaire>
   ```

4. Si vous voulez configurer une liste de domaines utilisateur afin que vous ayez seulement besoin d'entrer le nom d'utilisateur durant l'ouverture de session sur l'interface Web, entrez la commande suivante :

   ```
   racadm config -g cfgUserDomain -o cfgUserDomainName -i <index>
   ```

   Jusqu'à 40 domaines utilisateur peuvent être configurés avec des numéros d'index compris entre 1 et 40.

   Voir « Utilisation d'Active Directory pour ouvrir une session iDRAC6 » pour plus de détails 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 l'écran. Il vous sera demandé d'entrer un nom d'utilisateur de test (par exemple, nomd'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 peut prendre un certain temps. Un journal de test détaillé s'affichera au bas de l'écran 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, voir « Questions fréquemment posées concernant Active Directory ».

Si vous devez apporter des modifications à vos paramètres, cliquez sur l'onglet **Active Directory**, puis modifiez la configuration pas-à-pas.

Activation de SSL sur un contrôleur de domaine

Lorsque l'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 moment, le contrôleur de domaine doit publier un certificat signé par l'autorité de certification (CA), dont le certificat racine est également téléversé sur l'iDRAC. En d'autres termes, pour que l'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 la CA du domaine.

Si vous utilisez la CA 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.

1. Activez SSL sur chacun de vos contrôleurs de domaine en installant le certificat SSL pour chaque contrôleur.
   a. Cliquez sur **Démarrer**→ **Outils d'administration**→ **Règle de sécurité du domaine**.
   b. Développez le dossier **Règles de clé publique**, effectuez un clic droit sur **Paramètres de demande automatique de certificat** et cliquez sur **Demande automatique de certificat**.
   c. Dans l'**Assistant Configuration de demandes automatiques de certificats**, cliquez sur **Suivant** et sélectionnez **Contrôleur de domaine**.
   d. Cliquez sur **Suivant** et cliquez sur **Terminer**.

Exportation du certificat d'autorité de certification racine du contrôleur de domaine sur l'iDRAC

REMARQUE : Si votre système exécute Windows 2000, les étapes suivantes peuvent varier.

REMARQUE : Si vous utilisez un CA autonome, les étapes suivantes peuvent varier.

1. Localisez le contrôleur de domaine qui exécute le service CA 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 composant logiciel enfichable**.
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 effectuez un clic droit sur le certificat CA 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 à 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 à l'étape 14 sur l'iDRAC.

    Pour téléverser le certificat à l'aide de la RACADM, voir « Configuration d'Active Directory avec le schéma étendu en utilisant l'interface Web iDRAC6. » ou « Configuration d'Active Directory avec le schéma standard via RACADM ».

    Pour téléverser le certificat à l'aide de l'interface Web, voir « Configuration d'Active Directory avec le schéma étendu en utilisant l'interface Web iDRAC6. » ou « Configuration d'Active Directory avec le schéma étendu en utilisant l'interface Web iDRAC6 ».

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 iDRAC sur le contrôleur de domaine d'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 sécurisées 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 CA connue et le certificat de cette CA est déjà dans la liste des autorités de certification racines de confiance du contrôleur de domaine, vous n'avez pas besoin d'effectuer les étapes décrites dans cette section.

Le certificat SSL iDRAC est le même que celui utilisé pour le serveur Web iDRAC. Tous les contrôleurs iDRAC sont livrés avec un certificat auto-signé par défaut.

Pour téléverser le certificat SSL iDRAC, exécutez la commande RACADM suivante :

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

1. Sur le contrôleur de domaine, ouvrez une fenêtre **Console MMC** et sélectionnez **Certificats**→ **Autorités de certification racines de confiance**.
2. Effectuez un clic droit sur **Certificats**, sélectionnez **Toutes les tâches** et cliquez sur **Importer**.
3. Cliquez sur **Suivant** et naviguez pour sélectionner le fichier de certificat SSL.

4. Installez le certificat SSL de l'iDRAC dans l'**Autorité de certification racine de confiance** de chaque contrôleur de domaine.

   Si vous avez installé votre propre certificat, assurez-vous que la CA 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 sélectionnez un magasin de votre choix.

6. Cliquez sur **Terminer** et cliquez sur **OK**.

Utilisation d'Active Directory pour ouvrir une session iDRAC6

Vous pouvez utiliser Active Directory pour ouvrir une session iDRAC6 via une des méthodes suivantes :

- Une interface Web
- RACADM distant
- La console série ou telnet.

La syntaxe d'ouverture de session est la même pour les trois méthodes :

<nom d'utilisateur@domaine>

ou

*<domaine>**<nom d'utilisateur>* ou *<domaine>*/*<nom d'utilisateur>*

où *nom d'utilisateur* est une chaîne de caractères 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, l'écran d'ouverture de session Web listera 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 d'entrer 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 « Utilisation d'Active Directory pour ouvrir une session iDRAC6 ».

Vous pouvez également ouvrir une session de l'iDRAC6 à l'aide de la carte à puce. Pour plus d'informations, voir « Ouverture de session sur l'iDRAC6 avec la carte à puce ».

REMARQUE : Le serveur Windows 2008 Active Directory prend uniquement en charge la chaîne de caractères <nom_d'utilisateur@<nom_de_domaine> avec 256 caractères maximum.

Utilisation d'une connexion directe Active Directory

Vous pouvez activer l'iDRAC6 pour utiliser Kerberos, un protocole d'authentification réseau, afin de permettre l'ouverture de session individuelle. Pour plus d'informations sur la configuration d'iDRAC6 pour utiliser la fonctionnalité d'ouverture de session individuelle d'Active Directory, voir « Activation de l'authentification Kerberos ».

Configuration d'iDRAC6 pour utiliser une ouverture de session individuelle

1. Cliquez sur **Accès distant**→ onglet **Configuration**→ sous-onglet **Active Directory**→ sélectionnez **Configurer Active Directory**.

2. Dans l'écran **Étape 2/4 Configuration et gestion d'Active Directory**, sélectionnez **Activer l'ouverture de session individuelle**. L'option **Activer l'ouverture de session individuelle** est activée uniquement si vous avez sélectionné l'option **Activer Active Directory**.

   L'option **Activer l'ouverture de session individuelle** vous permet d'ouvrir une session iDRAC6 directement après vous êtes connecté à votre station de travail sans entrer vos références d'authentification utilisateur de domaine, par exemple le nom d'utilisateur et le mot de passe. Pour ouvrir une session iDRAC6 à l'aide de cette fonctionnalité, vous devez impérativement être déjà connecté à votre système via un compte utilisateur Active Directory valide. En outre, vous devez déjà avoir configuré le compte utilisateur pour ouvrir une session iDRAC6 à l'aide des références d'Active Directory. L'iDRAC6 utilise les références d'Active Directory mises en cache pour vous connecter.

   Pour activer l'ouverture de session individuelle à l'aide de la ligne de commande, exécutez la commande racadm :

   ```
   racadm -g cfgActiveDirectory -o cfgADSSOEnable 1
   ```

Ouverture d'une session iDRAC6 via l'ouverture de session individuelle

1. Connectez-vous à votre station de travail à l'aide de votre compte réseau.

2. Pour accéder à la page Web d'iDRAC6, tapez :

   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 de l'iDRAC6 et *numéro de port* le numéro de port HTTPS.

   La page d'ouverture de session individuelle de l'iDRAC6 s'affiche.

3. Cliquez sur **Login** (Connexion).

L'iDRAC6 vous connecte à l'aide de vos références mises en cache dans le système d'exploitation lorsque vous vous connectez via votre compte Active Directory valide.

Questions fréquemment posées concernant Active Directory

Mon ouverture de session sur 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 droits d'administrateur depuis l'interface Web. Cliquez sur **Accès distant**→ **Configuration**→ **Active Directory**. Allez à la fin de l'écran **Configuration et gestion d'Active Directory** et cliquez sur **Paramètres de tes**t. Entrez un nom d'utilisateur et mot de passe de test, puis cliquez sur **Démarrer le test**. L'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. Cliquez sur l'onglet **Active Directory** pour revenir à l'écran **Configuration et gestion d'Active Directory**. Allez à la fin de l'écran 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 certificats, mais je ne suis pas parvenu à ouvrir une session via Active Directory. J'ai exécuté les diagnostics depuis l'interface utilisateur et les résultats du test affichent le message d'erreur suivant :

ERROR: Can't contact LDAP server, error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed: Please check the correct Certificate Authority (CA) certificate has been uploaded to iDRAC. Please also check if the iDRAC date is within the valid period of the certificates and if the Domain Controller Address configured in iDRAC matches the subject of the Directory Server Certificate.

(ERREUR : impossible de contacter le serveur LDAP, erreur : 14090086:SSL routines :SSL3_GET_SERVER_CERTIFICATE : échec de la vérification du certificat : veuillez vérifier que le certificat de l'autorité de certification (CA) correct a été téléversé sur l'iDRAC. Veuillez également vérifier que la date de l'iDRAC est comprise dans la période de validité des certificats et si l'adresse du contrôleur de domaine configurée dans l'iDRAC correspond au sujet du certificat de serveur d'annuaires.)

Quel peut être le problème et comment le résoudre ?

Si la validation de certificats est activée, l'iDRAC6 utilise le certificat CA téléversé pour vérifier le certificat du serveur d'annuaires lorsque l'iDRAC6 établit une connexion SSL avec le serveur d'annuaires. Les raisons les plus courantes de l'échec de la validation de certificat sont :

1. La date de l'iDRAC6 n'est pas comprise dans la période de validité du certificat de serveur ou du Certificat CA. Vérifiez l'heure de l'iDRAC6 et la période de validité de votre certificat.

2. Les adresses du contrôleur de domaine configurées dans l'iDRAC6 ne correspondent pas au sujet ou au nom alternatif du sujet du certificat de serveur d'annuaires. 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 pas celui du domaine, par exemple, nomdeserveur.exemple.com au lieu de exemple.com.

J'utilise une adresse IP pour une adresse de contrôleur de domaine, et je ne suis pas parvenu à valider le certificat. Quel est le problème ?

Vérifiez le champ Sujet ou Nom alternatif du sujet 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 Sujet ou Nom alternatif du sujet 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 que la ou les *adresses du contrôleur de domaine* dans l'iDRAC6 afin de correspondre au sujet ou au nom alternatif du sujet du certificat de serveur.

2. Publier à nouveau le certificat de serveur de telle sorte à utiliser une adresse IP dans le champ Sujet ou Nom alternatif du sujet afin que celui-ci corresponde à l'adresse IP configurée dans l'iDRAC6.

3. Désactiver la validation des certificats si vous choisissez de faire confiance à ce contrôleur de domaine sans validation de certificats durant la négociation SSL.

J'utilise un schéma étendu dans un environnement à plusieurs domaines. Comment puis-je configurer la ou les adresses du contrôleur de domaine ?

Utilisez le nom d'hôte (FQDN) ou l'adresse IP du ou des contrôleurs de domaine servant le domaine dans lequel l'objet iDRAC6 réside.

Dois-je configurer la ou les adresses du catalogue global ?

Si vous utilisez un schéma étendu, il n'est pas nécessaire de configurer l'adresse du catalogue global.

Si vous utilisez le schéma standard, et que les utilisateurs et groupes de rôles proviennent de domaines différents, vous devez configurer la ou les adresses du catalogue global. Dans ce cas, seul le groupe universel peut être utilisé.

Si vous utilisez le schéma standard, et que les utilisateurs et groupes de rôles proviennent du même domaine, il n'est pas nécessaire de configurer la ou les adresses du catalogue global.

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 globales sont configurées, l'iDRAC6 continue d'interroger le catalogue global. Si des privilèges supplémentaires sont récupérés du catalogue global, ces privilèges sont accumulés.

L'iDRAC6 utilise-t-il toujours LDAP sur SSL ?

Oui. Tous les transports se font via le port sécurisé 636 et/ou 3269.

Durant la *configuration du test*, l'iDRAC6 effectue une connexion LDAP CONNECT uniquement pour aider à l'isolation du problème, mais il n'effectue pas de LDAP BIND sur une connexion non sécurisée.

Pourquoi l'iDRAC6 active-t-il la validation des certificats par défaut ?

L'iDRAC6 renforce la sécurité afin d'assurer l'identité du contrôleur de domaines auquel l'iDRAC6 se connecte. À défaut de la validation des certificats, un pirate pourrait usurper un contrôleur de domaine et détourner une connexion SSL. Si vous choisissez de faire confiance à tous les contrôleurs de domaine de votre connexion sécurisée sans validation des certificats, vous pouvez la désactiver via la GUI ou la ligne de commande.

L'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 iDRAC6 via Active Directory ?

Vous pouvez diagnostiquer le problème en cliquant sur Paramètres de test au bas de l'écran Configuration et Management d'Active Directory dans l'interface Web de l'iDRAC6. Corrigez ensuite le problème spécifique indiqué par les résultats du test. Pour plus d'informations, voir « Test de vos configurations ».

La plupart des problèmes fréquemment rencontrés sont expliqués dans cette section. Toutefois, en général, vous devriez 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 dans l'iDRAC6 à l'aide de vos références locales.

   Lorsque vous avez ouvert une session :

   a. Vérifiez que vous avez coché la case **Activer Active Directory** dans l'écran **Configuration et gestion d'Active Directory** de l'iDRAC6.

   b. Vérifiez que le paramètre DNS est correct sur l'écran Configuration réseau iDRAC6.

   c. Assurez-vous que vous avez téléversé le bon certificat CA racine d'Active Directory vers l'iDRAC6 si vous avez activé la validation de certificat. Assurez-vous que l'heure de l'iDRAC6 est comprise dans la période de validité du certificat CA.

   d. Si vous utilisez le schéma étendu, assurez-vous que le Nom iDRAC6 et le Nom de domaine iDRAC6 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.

Retour á la page du sommaire

Retour á la page du sommaire

Configuration de l'authentification par carte à puce

Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.1

L'iDRAC6 prend en charge la fonctionnalité d'authentification bifactorielle (TFA) en activant **l'ouverture de session 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, l'authentification bifactorielle offre un niveau accru de sécurité en exigeant que les utilisateurs fournissent deux facteurs d'authentification : ce qu'ils ont et ce qu'ils savent. Le premier est une carte à puce et un périphérique physique et le second est un code secret tel qu'un mot de passe ou code PIN.

L'authentification bifactorielle exige des utilisateurs qu'ils vérifient leur identité en fournissant *les deux* facteurs.

Configuration de l'ouverture de session par carte à puce sur l'iDRAC6

Pour activer la fonctionnalité Ouverture de session par carte à puce sur l'iDRAC6 à partir de l'interface Web, accédez à **Accès distant**→ **Configuration**→ **Carte à puce et sélectionnez Activer**.

Si vous sélectionnez :

- **Activer** ou **Activer 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.

  Lorsque vous sélectionnez **Activer**, toutes les interfaces hors bande de l'interface de ligne de commande (CLI), telles que telnet, SSH, série, RACADM distante, et IPMI sur LAN, sont désactivées. Ceci s'explique par le fait que ces services prennent en charge uniquement l'authentification monofactorielle.

  Lorsque vous sélectionnez **Activer avec la RACADM distante**, toutes les interfaces hors bande de la CLI, à l'exception de la RACADM distante, sont désactivées.

  REMARQUE : Dell recommande à l'administrateur de l'iDRAC6 d'utiliser le paramètre **Activer avec la RACADM distante** uniquement pour accéder à l'interface utilisateur Web de l'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, Dell recommande d'utiliser le paramètre **Activé** pour l'ouverture de session par carte à puce. De même, assurez-vous que la configuration des utilisateurs locaux de l'iDRAC6 et/ou la configuration Active Directory a été achevée avant d'activer la fonctionnalité **Ouverture de session par carte à puce**.

- **Désactiver** la configuration de la carte à puce (par défaut). Cette sélection désactive la fonctionnalité TFA Ouverture de session par carte à puce. Dès lors, à la prochaine ouverture de session sur la GUI de l'iDRAC6, vous êtes invité à saisir un nom d'utilisateur et un mot de passe d'ouverture de session Microsoft® Active Directory® ou local. Ceci se présente sous la forme d'une invite d'ouverture de session par défaut dans l'interface Web.
- **Activer le contrôle CRL pour l'ouverture de session par carte à puce**. Le certificat iDRAC de l'utilisateur qui est téléchargé depuis le serveur de distribution de la liste de révocation de certificat (CRL), est contrôlé pour vérifier sa révocation dans la CRL.

  REMARQUE : Les serveurs de distribution CRL sont répertoriés dans les certificats de la carte à puce des utilisateurs.

Configuration des utilisateurs d'iDRAC6 local pour l'ouverture de session par carte à puce

Vous pouvez configurer les utilisateurs de l'iDRAC6 local pour qu'ils ouvrent une session sur l'iDRAC6 au moyen de la carte à puce. Cliquez sur **Accès distant**→ **Configuration**→ **Utilisateurs**.

Toutefois, pour que l'utilisateur puisse ouvrir une session sur l'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 (CA) de confiance sur l'iDRAC6.

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 sur l'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 CA 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 ouvrir une session de l'iDRAC6, le nom d'utilisateur que vous configurez dans l'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 publié pour l'utilisateur, « exempleutilisateur@domaine.com », le nom d'utilisateur doit être configuré comme « exempleutilisateur ».

Configuration des utilisateurs Active Directory pour l'ouverture de session par carte à puce

Pour configurer les utilisateurs Active Directory pour qu'ils ouvrent une session sur l'iDRAC6 au moyen de la carte à puce, l'administrateur de l'iDRAC6 doit configurer le serveur DNS, téléverser le certificat CA Active Directory sur l'iDRAC6 et activer l'ouverture de session Active Directory. Voir « Utilisation d'iDRAC6 avec Microsoft Active Directory » pour plus d'informations sur la configuration des utilisateurs Active Directory.

REMARQUE : Si l'utilisateur de la carte à puce figure dans Active Directory, un mot de passe Active Directory est exigé ainsi que le code PIN de la carte à puce.

Vous pouvez configurer Active Directory depuis **Accès distant**→ **Configuration**→ **Active Directory**.

Configuration de la carte à puce

REMARQUE : Pour modifier ces paramètres, vous devez avoir le droit de **configurer iDRAC**.

1. Développez l'arborescence du **système** et cliquez sur **Accès distant**.
2. Cliquez sur l'onglet **Configuration**, puis sur **Carte à puce**.
3. 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**.
4. Cliquez sur **Appliquer les modifications**.

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 (GUI) 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. • **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 l'ouverture de session par carte à puce désactive toutes les interfaces hors bande de la CLI, y compris SSH, Telnet, série, la RACADM distante et IPMI sur LAN. • **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. **REMARQUE :** L'ouverture de session par carte à puce vous impose de reconfigurer les utilisateurs de l'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 utilisateur Active Directory pour cet utilisateur. Vous pouvez configurer le certificat utilisateur dans la page **Utilisateurs**→ **Menu principal des utilisateurs**.
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 que l'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. Pour que la fonctionnalité CRL puisse être utilisée, une adresse IP DNS valide doit être configurée sur l'iDRAC6 dans sa configuration réseau. Vous pouvez configurer l'adresse IP DNS dans l'iDRAC6 sous **Accès distant**→ **Configuration**→ **Réseau**. L'utilisateur n'est pas en mesure d'ouvrir une session si : • Le certificat utilisateur est répertorié comme révoqué dans le fichier CRL. • L'iDRAC6 n'est pas en mesure de communiquer avec le serveur de distribution CRL. • L'iDRAC6 n'est pas en mesure de télécharger la CRL. **REMARQUE :** Vous devez configurer correctement l'adresse IP du serveur DNS dans la page **Configuration**→ **Réseau** pour que ce contrôle réussisse.

Ouverture de session sur l'iDRAC6 avec la carte à puce

L'interface Web de l'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 de l'iDRAC6 et/ou la configuration Active Directory a été achevée avant d'activer la fonctionnalité 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 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 de l'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 de l'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**.

   L'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 carte à puce. Si l'utilisateur n'est pas créé localement, l'iDRAC6 vous invite à saisir le mot de passe pour le compte Active Directory de l'utilisateur.

REMARQUE : Si vous êtes un utilisateur Active Directory pour lequel **Activer le contrôle CRL pour l'ouverture de session par carte à puce** est sélectionné, l'iDRAC6 tente de télécharger la CRL et contrôle celle-ci pour ce qui est du certificat de l'utilisateur. L'ouverture de session via Active Directory échoue si le certificat est répertorié comme révoqué dans le CRL ou si la CRL ne peut pas être téléchargée pour une raison quelconque.

   Vous êtes connecté à l'iDRAC6.

Ouvrir une session de l'iDRAC6 avec l'authentification par carte à puce Active Directory

1. Ouvrez une session sur l'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 de l'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. Introduisez la carte à puce, puis cliquez sur **Ouverture de session**.

   La boîte de dialogue contextuelle Code PIN s'affiche.

3. Saisissez le code NIP, puis cliquez sur **OK**.

4. Saisissez le mot de passe d'authentification Active Directory de l'utilisateur pour authentifier l'utilisateur et cliquez sur **OK**.

   Vous avez ouvert une session iDRAC6 avec vos références telles qu'elles sont configurées dans Active Directory.

REMARQUE : Si l'utilisateur de la carte à puce est présent dans Active Directory, un mot de passe Active Directory est exigé ainsi que le code PIN de la carte à puce. Dans les versions ultérieures, le mot de passe Active Directory peut ne pas être requis.

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

Code 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'entreprise peut vous aider à obtenir une nouvelle carte à puce.

Impossible d'ouvrir une session sur l'iDRAC6 local

Si un utilisateur de l'iDRAC6 local ne parvient pas à ouvrir une session, vérifiez si le nom d'utilisateur et les certificats utilisateur téléversés sur l'iDRAC6 ont expiré. Les journaux de suivi de l'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 l'iDRAC6 en tant qu'utilisateur Active Directory

Si vous ne parvenez pas à ouvrir une session iDRAC6 en tant qu'utilisateur Active Directory, essayez d'ouvrir une session iDRAC6 sans activer l'ouverture de session par carte à puce. Si vous avez activé le contrôle CRL, essayez d'ouvrir une session Active Directory sans activer le contrôle CRL. Le journal de suivi d'iDRAC6 doit mentionner 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 cfgActiveDirectory -o cfgADSmartCardLogonEnable 0
```

Retour á la page du sommaire

Retour á la page du sommaire

Utilisation de la redirection de console de la GUI

Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.1

Cette section fournit des informations sur l'utilisation de la fonctionnalité de redirection de la console iDRAC6.

Présentation

La fonctionnalité de redirection du panneau de la console iDRAC6 vous permet d'accéder à la console locale à distance en mode graphique ou texte. À l'aide de la redirection de la console, 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. Vous pouvez, au contraire, gérer les serveurs depuis n'importe quel endroit, à partir de votre bureau ou ordinateur portable. Vous pouvez aussi partager les informations avec d'autres, à distance et instantanément.

Utilisation de la redirection de console

REMARQUE : Quand vous ouvrez une session de console, le serveur géré n'indique pas que la console a été redirigée.

REMARQUE : Si une session de redirection de console est déjà ouverte sur la station de gestion vers l'iDRAC6, une tentative pour ouvrir une nouvelle session à partir de la station de gestion vers cet iDRAC6 entraîne l'activation de la session existante. Une nouvelle session n'est pas générée.

REMARQUE : Il est possible d'ouvrir simultanément des sessions de redirection de console multiples à partir d'une station de gestion vers plusieurs contrôleurs iDRAC6.

La page **Redirection de la Console** permet de gérer le système distant en utilisant le clavier, la vidéo et la souris de la station de gestion locale pour contrôler les périphériques correspondants du 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 de redirection de console :

- Quatre sessions de redirection de console simultanées sont prises en charge au maximum. Toutes les sessions affichent la même console de serveur géré simultanément.
- Il est possible d'ouvrir une seule session sur un serveur distant (iDRAC6) à partir d'une console client (station de gestion). Toutefois, il est possible d'ouvrir sur le même client des sessions multiples vers plusieurs serveurs distants.
- Une session de redirection de console 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 de redirection de console d'iDRAC est une session à accès complet. Si un deuxième utilisateur lance une session de redirection de console, le premier utilisateur est prévenu et il a la possibilité de rejeter, **autoriser en lecture seule** ou **approuver** la session. Le deuxième utilisateur est averti qu'un autre utilisateur contrôle la session. Le premier utilisateur doit répondre dans les trente secondes sinon l'accès est refusé au deuxième utilisateur.

Toutes les sessions **autorisées en lecture seule** prennent automatiquement fin lorsque la dernière session à accès complet est arrêtée.

Configuration de votre station de gestion

Pour utiliser la redirection de console 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 »
   - « Configuration d'un navigateur Web pris en charge »

   REMARQUE : L'environnement d'exécution Java doit être installé sur la station de gestion pour que la fonctionnalité de redirection de console fonctionne.

2. Si vous utilisez Internet Explorer, vérifiez que le navigateur autorise le téléchargement de contenu crypté :
   - Cliquez sur Options ou Paramètres d'Internet et sélectionnez **Outils**→ **Options Internet** → **Avancé**.
   - Défilez jusqu'à **Sécurité** et désélectionnez l'option suivante :

     Do not save encrypted pages to disk (Ne pas enregistrer les pages chiffrées sur le disque)

3. Il est recommandé de configurer la résolution d'affichage de votre moniteur sur au moins 1280x1024 pixels.

REMARQUE : Si votre serveur exécute un système d'exploitation Linux, une console X11 peut ne pas être visible sur le moniteur local. Appuyez sur <Ctrl><Alt><F1> sur le KVM iDRAC pour faire basculer Linux en console texte.

REMARQUE : Vous pouvez occasionnellement rencontrer une erreur de compilation de script Java : « Expected: ; ». Pour résoudre ce problème, réglez les paramètres du réseau afin d'utiliser une « connexion directe » dans JavaWebStart : « Edition->Préférences->Général->Paramètres réseau » et sélectionnez « Connexion directe » à la place de « Utiliser les paramètres du navigateur ».

Configuration de la redirection de console dans l'interface Web d'iDRAC6

Pour configurer la redirection de console dans l'interface Web iDRAC6, effectuez les étapes suivantes :

1. Cliquez sur **Système**→ **Console/Média**→ **Configuration** pour configurer les paramètres de redirection iDRAC.
2. Configurez les propriétés de la redirection de console. Le Tableau 10-1 décrit les paramètres de la redirection de console.
3. Lorsque vous avez terminé, cliquez sur **Appliquer les modifications**.
4. Cliquez sur le bouton approprié pour continuer. Reportez-vous au Tableau 10-2.

Tableau 10-1. Propriétés de configuration de la redirection de console

Propriété	Description
Activé	Cliquez pour activer ou désactiver la redirection de console. Si cette option est cochée, cela signifie que la redirection de console est activée. L'option par défaut est **Activé**. **REMARQUE :** Le fait de cocher ou de décocher l'option **Activé** dès que le KVM virtuel est lancé risque de déconnecter toutes vos sessions KVM virtuelles existantes.
Nombre maximal de sessions	Affiche le nombre maximal de sessions de redirection de console possibles, 1 à 4. Utilisez le menu déroulant pour modifier le nombre maximal de sessions de redirection de console permises. L'adresse par défaut est **2**.
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 pour connecter à l'option clavier/souris de la redirection de console. Ce trafic est toujours crypté. Vous devrez peut-être changer ce numéro si un autre programme utilise le port par défaut. L'adresse par défaut est **5900**. **REMARQUE :** Le fait de modifier la valeur du **Port de présence à distance** dès que le KVM virtuel est lancé risque de déconnecter toutes vos sessions KVM virtuelles existantes.
Cryptage vidéo activé	**Coché** indique que le cryptage vidéo est activé. Tout le trafic à destination du port vidéo est crypté. **Décoché** indique que le cryptage vidéo est désactivé. Le trafic allant au port vidéo n'est pas crypté. La valeur par défaut est **Crypté. La désactivation du cryptage peut améliorer les performances sur les réseaux plus lents.** **REMARQUE :** Le fait d'activer ou de désactiver l'option **Cryptage vidéo activé** dès que le KVM virtuel est lancé risque de déconnecter toutes vos sessions KVM virtuelles existantes.
Vidéo locale du serveur activée	Si cette case est cochée, cela signifie que la sortie vers le KVM iDRAC est désactivée lors de la redirection de console. Ceci assure que les tâches que vous effectuez avec la **redirection de console** ne sont pas visibles sur le moniteur local du serveur géré.

REMARQUE : Pour obtenir des informations sur l'utilisation du média virtuel avec la redirection de console, voir Configuration et utilisation du média virtuel.

Les boutons répertoriés dans le Tableau 10-2 sont disponibles sur la page **Configuration**.

Tableau 10-2. Boutons de la page de configuration

Bouton	Définition
Imprimer	Imprime la page
Actualiser	Recharge la page **Configuration**
Appliquer les modifications	Enregistrer tout nouveau paramètre ou tout paramètre enregistré

Ouverture d'une session de redirection de console

Lorsque vous ouvrez une session de redirection de console, l'application du visualiseur KVM virtuel de Dell™ démarre et le bureau du système distant apparaît dans le visualiseur. Grâce à l'application permettant de visualiser le KVM virtuel, vous pouvez contrôler les fonctions de souris et de clavier du système distant

à partir de votre station de gestion locale.

Pour ouvrir une session de redirection de console dans l'interface Web, effectuez les étapes suivantes :

1. Cliquez sur **Système**→ **Console/Média**→ **Redirection de console et Média virtuel**.

2. Servez-vous des informations du Tableau 10-3 pour vérifier qu'une session de redirection de console est disponible.

   Pour reconfigurer les valeurs des propriétés affichées, voir « Configuration de la redirection de console dans l'interface Web d'iDRAC6 ».

Tableau 10-3. Console Redirection

Propriété	Description
Redirection de console activée	Oui/Non (coché\non coché)
Cryptage vidéo activé	Oui/Non (coché\non coché)
Nombre maximal de sessions	Affiche le nombre maximal de sessions de redirection de console prises en charge
Sessions actives	Affiche le nombre actuel de sessions de redirection de console ouvertes
Vidéo locale du serveur activée	Oui = Activé ; Non = Désactivé.
Port de présence à distance	Numéro de port réseau utilisé pour connecter à l'option clavier/souris de la redirection de console. Ce trafic est toujours crypté. Vous devrez peut-être changer ce numéro si un autre programme utilise le port par défaut. L'adresse par défaut est 5900.

REMARQUE : Pour obtenir des informations sur l'utilisation du média virtuel avec la redirection de console, voir Configuration et utilisation du média virtuel.

Les boutons répertoriés dans le Tableau 10-4 sont disponibles sur la page **Redirection de console et média virtuel**.

Tableau 10-4. Boutons de la page Redirection de la console et média virtuel

Bouton	Définition
Actualiser	Recharge la page **Redirection de console et Média virtuel**
Lancer le visualiseur	Ouvre une session de redirection de console sur le système distant cible.
Imprimer	Imprime la page **Redirection de console et Média virtuel**

3. Si une session de redirection de console est disponible, cliquez sur **Lancer le visualiseur**.

   REMARQUE : Plusieurs boîtes de message peuvent apparaître après le lancement de l'application. Afin d'empêcher l'accès non autorisé à l'application, vous devez naviguer à travers ces boîtes de message pendant trois minutes maximum. Sinon, vous serez 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 l'iDRAC6 et le bureau du système distant apparaît dans l'application de visualiseur KVM iDRAC.

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 KVM iDRAC.

Utilisation du visualiseur vidéo

L'application Video Viewer fournit une interface utilisateur entre la station de gestion et le serveur géré, vous permettant 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, le visualiseur de vidéo démarre dans une fenêtre séparée.

REMARQUE : Si le serveur distant est éteint, le message **No Signal (Aucun signal)** s'affiche.

Video Viewer fournit divers réglages 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** Redirection de la console et média virtuel.

Lorsque vous démarrez une session de redirection de console et que le visualiseur vidéo apparaît, il est possible que vous ayez à synchroniser les pointeurs de souris.

Désactivation ou activation de la vidéo locale du serveur

Vous pouvez configurer iDRAC6 pour interdire les connexions KVM iDRAC 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 **Redirection de console**.

REMARQUE : Si vous désactivez (éteignez) la vidéo locale sur le serveur, le moniteur, le clavier et la souris connectés à iDRAC KVM 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 iDRAC6. Pour plus d'informations, voir « Accès à l'interface Web ».
2. Cliquez sur **Système**→ **Console/Média**→ **Configuration**.
3. Pour désactiver (éteindre) la vidéo locale sur le serveur, décochez la case **Serveur vidéo local activé** de la page de **Configuration,** puis cliquez sur **Appliquer**. La valeur par défaut est Désactivé.

   REMARQUE : Si le serveur vidéo local est activé, comptez 15 secondes pour qu'il se désactive.

4. Pour activer (allumer) la vidéo locale sur le serveur, cochez la case **Serveur vidéo local activé** de la page de **Configuration,** puis cliquez sur **Appliquer**.

Questions fréquemment posées concernant la redirection de console

Le Tableau 10-5 répertorie les questions les plus fréquentes et les réponses correspondantes.

Tableau 10-5. Utilisation de la redirection de console : Questions les plus fréquentes

Question	Réponse
Est-ce qu'une nouvelle session de vidéo à distance peut être démarrée lorsque la vidéo locale sur le serveur est désactivée ?	Oui.
Pourquoi la vidéo locale sur le serveur prend-elle 15 secondes pour se désactiver 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 aussi 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 aussi 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 l'état actuel de la vidéo locale du serveur ?	La condition est affichée dans la page **Configuration de la redirection de console** de l'interface Web iDRAC6. 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 Redirection de console.	Assurez-vous que la résolution du moniteur de la station de gestion est définie sur 1280x1024. Essayez également d'utiliser la barre de défilement du client iDRAC KVM.
La fenêtre de la console est tronquée.	Le visualiseur de console sur 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 dans la console de texte Linux ?	Le KVM virtuel requiert un pilote de souris USB, mais le pilote de souris USB est disponible uniquement sous le système d'exploitation X-Windows.
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 de redirection de console. Veillez à ce que l'option **Curseur simple**, dans la partie **Outils** du menu iDRAC KVM soit sélectionnée sur le client iDRAC KVM.
Je ne peux pas utiliser de clavier ou de souris lorsque j'installe un système d'exploitation Microsoft à distance en utilisant la redirection de console iDRAC6. Pourquoi ?	Lorsque vous installez à distance un système d'exploitation Microsoft pris en charge sur un système dont la fonction de redirection de console 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 redirection de console dans le BIOS. Ce message est généré par Microsoft pour avertir l'utilisateur que la redirection de console est activée. Pour que ce message n'apparaisse pas, désactivez toujours la redirection de console dans le BIOS avant d'installer

	un système d'exploitation à distance.
Pourquoi l'indicateur Verr Num sur ma station de gestion ne reflète-t-il pas l'état Verr Num sur le serveur distant ?	Lors d'un accès via l'iDRAC6, l'indicateur du verrouillage numérique sur la station de gestion ne correspond pas nécessairement à l'état du verrouillage numérique sur le serveur distant. L'état Verr Num dépend du paramètre sur le serveur distant lorsqu'une 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 de redirection de console à partir de l'hôte local ?	Vous configurez une session de redirection de console à partir du système local. Cette opération n'est pas prise en charge.
Si j'exécute une session de redirection de console 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 de redirection de console ?	Dell recommande une connexion de 5 Mo/s pour une performance optimale. Une connexion de 1 Mo/s suffit pour une performance minimale.
Quelle est la configuration système minimale requise pour que ma station de gestion exécute la redirection de console ?	La station de gestion nécessite un processeur Intel® Pentium® III 500 MHz avec au moins 256 Mo de RAM.
Pourquoi est-ce qu'un message **Aucun signal** s'affiche dans le visualiseur vidéo iDRAC KVM ?	Ce message peut s'afficher lorsque le plugin iDRAC KVM virtuel ne reçoit pas la vidéo du bureau du serveur distant. En règle générale, cette situation a lieu lorsque le serveur distant est éteint. Parfois, ce message peut s'afficher en raison de problèmes de réception de la vidéo du bureau du serveur distant.
Pourquoi est-ce qu'un message **Hors plage** s'affiche dans le visualiseur vidéo iDRAC KVM ?	Ce message peut s'afficher si un paramètre nécessaire à la capture de la vidéo se situe au-delà de la plage dans laquelle iDRAC peut capturer la vidéo. Des paramètres tels que la résolution de l'affichage ou un taux d'actualisation 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.

Retour á la page du sommaire

Retour á la page du sommaire

Activation de l'authentification Kerberos

Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.1

Kerberos est un protocole d'authentification de réseau qui permet aux systèmes de communiquer sans danger sur un réseau ouvert. Pour cela, il permet aux systèmes de 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 individuelles et par carte à puce Active Directory.

Microsoft® Windows® 2000, Windows XP, Windows Server® 2003, Windows Vista® et Windows Server 2008 utilisent à Kerberos comme méthode d'authentification par défaut.

L'iDRAC6 utilise Kerberos pour prendre en charge deux types de mécanismes d'authentification : les ouvertures de session individuelles Active Directory et les ouvertures de session par carte à puce Active Directory. Pour l'ouverture de session individuelle, l'iDRAC6 utilise les références d'utilisateur mises en cache dans le système d'exploitation après que l'utilisateur a ouvert une session via un compte Active Directory valide.

Pour l'ouverture de session par carte à puce Active Directory, l'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 l'iDRAC6 échoue si l'heure de l'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** l'iDRAC6.

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>
```

Critères requis pour les authentifications d'ouverture de session individuelle et Active Directory avec carte à puce

- Configurez l'iDRAC6 en vue de l'ouverture de session Active Directory. Pour plus d'informations, voir « Utilisation d'Active Directory pour ouvrir une session iDRAC6 ».
- Enregistrez l'iDRAC6 comme un ordinateur dans le domaine racine Active Directory.
  a. Cliquez sur **Accès distant**→ **Configuration** → sous-onglet **Réseau**.
  b. Fournissez une adresse IP valide pour le **serveur DNS préféré/auxiliaire**. Cette valeur est l'adresse IP du DNS faisant partie du domaine racine et authentifiant les comptes Active Directory des utilisateurs.
  c. Sélectionnez **Enregistrer l'iDRAC auprès du DNS.**
  d. Fournissez un **Nom de domaine DNS** valide.

  Consultez l'***aide en ligne d'iDRAC6*** pour plus d'informations.

Pour prendre en charge les deux nouveaux types de mécanismes d'authentification, l'iDRAC6 endosse la configuration pour se définir en tant que service « kerberisé » sur un réseau Windows Kerberos. La configuration Kerberos sur l'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 d'établir ainsi une relation de confiance entre un utilisateur ou système externe et le KDC (Key Distribution Centre). Le fichier keytab contient une clé de cryptage 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 que l'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 établir une correspondance entre l'iDRAC6 et 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. Les propriétés suivantes du compte utilisateur auquel le nom principal du service est mappé doivent être activées :

- Utiliser les types de cryptage DES pour ce compte
- Ne pas demander la pré-authentification Kerberos

REMARQUE : Il est recommandé d'utiliser le dernier utilitaire **ktpass** pour créer le fichier keytab.

Cette procédure génère un fichier keytab que vous devrez téléverser dans l'iDRAC6.

REMARQUE : Le fichier keytab contient une clé de cryptage à conserver en lieu sûr.

Pour plus d'informations sur l'utilitaire **ktpass**, voir le site Web 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.

Configuration d'iDRAC6 pour les authentifications des ouvertures de session individuelle et Active Directory avec carte à puce

Téléversez le fichier keytab obtenu à partir du domaine racine Active Directory dans l'iDRAC6 :

1. Cliquez sur **Accès distant**→ onglet **Configuration**→ sous-onglet **Active Directory** → Cliquez sur **Configurer Active Directory**.
2. Sélectionnez **Téléverser le fichier Keytab Kerberos**, puis cliquez sur **Suivant**.
3. Dans la page **Téléversement du fichier keytab Kerberos**, sélectionnez le fichier keytab à téléverser, puis cliquez sur **Appliquer**.

Vous pouvez également téléverser le fichier dans l'iDRAC6 à l'aide des commandes racadm de la CLI. La commande suivante permet de téléverser le fichier keytab dans l'iDRAC6 :

```
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.

Configuration des utilisateurs Active Directory pour l'ouverture de session individuelle

Avant d'utiliser la fonctionnalité d'ouverture de session individuelle Active Directory, assurez-vous que vous avez déjà configuré l'iDRAC6 pour l'ouverture de session Active Directory et que le compte d'utilisateur de domaine à utiliser pour vous connecter au système a été activé pour l'ouverture de session iDRAC6 Active Directory.

En outre, assurez-vous que vous avez activé le paramètre d'ouverture de session Active Directory. Voir « Utilisation d'iDRAC6 avec Microsoft Active Directory » pour plus d'informations sur la configuration des utilisateurs Active Directory. Vous devez également activer l'iDRAC6 pour lui permettre de devenir un service « kerberisé » en téléversant un fichier *keytab* valide, obtenu auprès du domaine racine Active Directory, dans l'iDRAC6.

Consultez « Configuration d'iDRAC6 pour utiliser une ouverture de session individuelle » pour plus d'informations sur la façon d'activer l'ouverture de session individuelle à l'aide de la GUI et de la CLI.

Connexion à l'iDRAC6 via l'ouverture de session individuelle pour les utilisateurs Active Directory

REMARQUE : Pour ouvrir une session iDRAC6, vérifiez que vous disposez des derniers composants au moment de l'exécution des bibliothèques Microsoft Visual C++ 2005. Pour plus d'informations, consultez le site Web de Microsoft.

1. Ouverture d'une session de système avec un compte Active Directory valide.
2. Tapez l'adresse Web d'iDRAC6 dans la barre d'adresse de votre navigateur.

   REMARQUE : Selon les paramètres de votre navigateur, il se peut que vous soyez invité à télécharger et installer le plug-in ActiveX d'ouverture de session individuelle lorsque vous utilisez cette fonctionnalité pour la première fois.

   Vous avez ouvert une session iDRAC6 avec les privilèges Microsoft Active Directory appropriés si :

   - vous êtes un utilisateur Microsoft Active Directory ;
   - vous êtes configuré dans l'iDRAC6 comme pouvant ouvrir une session Active Directory ;
   - l'iDRAC6 est activé pour l'authentification Kerberos Active Directory.

Configuration des utilisateurs 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 l'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 d'iDRAC6.

En outre, assurez-vous que vous avez activé le paramètre d'ouverture de session Active Directory. Voir « Utilisation d'iDRAC6 avec Microsoft Active Directory » pour plus d'informations sur la configuration des utilisateurs Active Directory. Vous devez également activer l'iDRAC6 pour lui permettre de devenir un service « kerberisé » en téléversant un fichier *keytab* valide, obtenu auprès du domaine racine Active Directory, dans l'iDRAC6.

Retour á la page du sommaire

Retour á la page du sommaire

Utilisation de l'interface Web WS-MAN

Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.1

Le micrologiciel iDRAC6 fournit la gestion accessible par réseau au moyen du protocole WS-MAN (Web Services for Management). WS-MAN est un mécanisme de transport destiné à l'échange d'informations. WS-MAN offre un langage universel permettant aux dispositifs de partager des données de manière à pouvoir être gérés plus aisément. WS-MAN est l'une des composantes essentielles d'une solution de gestion de systèmes distants.

WS-MAN utilise HTTPS pour assurer la sécurité du trafic de gestion. Le client doit ouvrir une session avec des privilèges d'utilisateur local ou Microsoft® Active Directory® pour authentifier la session. HTTPS utilise le protocole SSL (Secure Socket Layer) sur le port IP 443 pour authentifier les communications.

Les données disponibles via WS-MAN constituent un sous-ensemble de données fournies par l'interface d'instrumentation de l'iDRAC6 mappée sur les profils DMTF (Distributed Management Task Force) et les profils d'extension Dell suivants.

L'utilisation de WS-MAN pour transmettre des informations de gestion DMTF basées sur le schéma CIM (modèle commun d'informations) est l'utilisation la plus commune de WS-MAN. Le schéma CIM définit les types d'informations de gestion qui peuvent être manipulées au sein d'un système de gestion. Il fournit les objets dont parlent le client et le service sur le réseau. WS-MAN ne précise pas des actions standard qui peuvent être effectuées sur les objets de gestion. Par exemple, WS-MAN permet à un système client de trouver un assortiment d'objets de gestion, d'obtenir le contenu d'un objet de gestion et de définir son contenu sur de nouvelles valeurs. WS-MAN fournit les verbes de la conversation de gestion ; les classes CIM et les propriétés sont les noms, c'est à dire les objets sur lesquels agissent les verbes.

Pour assurer l'interopérabilité entre les clients et les services, DMTF et Dell précisent en outre un *vocabulaire* normalisé minimum composé de classes, de propriétés et de comportements CIM que toutes les parties doivent comprendre. Ces profils DMTF et spécifiques à Dell définissent un ensemble de conventions qui doivent être mises en uvre par tous les services conformes à la norme. Tous les clients peuvent donc se fier à ces conventions afin de bien fonctionner.

Profils CIM pris en charge

Tableau 11-1. Profils CIM pris en charge

DMTF standard
1. Serveur de base Définit les classes CIM pour la représentation du serveur hôte.
2. Processeur de service : Contient la définition des classes CIM pour la représentation de l'iDRAC6. **REMARQUE :** Le profil du serveur de base (ci-dessus) et le profil du processeur de service sont autonomes en ce sens que les objets qu'ils décrivent sont amalgamés avec les autres objets CIM définis par le profil des composants.
3. Bien physique : Définit les classes CIM pour la représentation de l'aspect physique des éléments gérés. L'iDRAC6 utilise ce profil pour représenter le serveur hôte et les informations FRU de ses composants, ainsi que la topologie physique.
4. Domaine d'administration du protocole de ligne de commande Server Management (SM-CLP) Définit les classes CIM pour la représentation de la configuration du protocole CLP. L'iDRAC6 utilise ce profil pour sa propre mise en uvre du protocole CLP.
5. Gestion de l'état de l'alimentation Définit les classes CIM pour les opérations de contrôle de l'alimentation. L'iDRAC6 utilise ce profil pour les opérations de contrôle de l'alimentation du serveur hôte.
6. Bloc d'alimentation (version 1.1) Définit les classes CIM pour la représentation des blocs d'alimentation. L'iDRAC6 utilise ce profil pour représenter les blocs d'alimentation du serveur hôte afin de décrire la consommation énergétique, tels que les filigranes de consommation énergétique élevée ou basse.
7. Service CLP Définit les classes CIM pour la représentation de la configuration du protocole CLP. L'iDRAC6 utilise ce profil pour sa propre mise en uvre du protocole CLP.
8. Interface IP
9. Client DHCP
10. Client DNS
11. Port Ethernet Les profils ci-dessus définissent les classes CIM pour la représentation des piles de réseau. L'iDRAC6 utilise ces profils pour représenter la configuration du NIC (contrôleur d'interface réseau) de l'iDRAC6.
12. Enregistrement des journaux Définit les classes CIM pour la représentation de différents types de journaux. L'iDRAC6 utilise ce profil pour représenter le SEL (journal des

événements système) et le journal RAC de l'iDRAC6.
13. Inventaire de logiciel Définit les classes CIM pour faire l'inventaire des logiciels installés ou disponibles. L'iDRAC6 utilise ce profil pour faire l'inventaire des versions du micrologiciel de l'iDRAC6 actuellement installées via le protocole TFTP.
14. Autorisation basée sur les rôles Définit les classes CIM pour la représentation des rôles. L'iDRAC6 utilise ce profil pour configurer les privilèges de compte iDRAC6.
15. Mise à jour de logiciel Définit les classes CIM pour faire l'inventaire des mises à jour de logiciels disponibles. L'iDRAC6 utilise ce profil pour faire l'inventaire des mises à jour du micrologiciel via le protocole TFTP.
16. Recueil SMASH Définit les classes CIM pour la représentation de la configuration du protocole CLP. L'iDRAC6 utilise ce profil pour sa propre mise en uvre du protocole CLP.
17. Enregistrement des profils Définit les classes CIM pour l'annonce des mises en uvre des profils. L'iDRAC6 utilise ce profil pour annoncer ses propres profils mis en uvre comme l'indique ce tableau.
18. Paramètres de base Définit les classes CIM pour la représentation des paramètres. L'iDRAC6 utilise ce profil pour représenter les paramètres du serveur hôte afin de décrire la consommation énergétique, tels que les filigranes de consommation énergétique élevée ou basse.
19. Gestion simple des identités Définit les classes CIM pour la représentation des identités. L'iDRAC6 utilise ce profil pour configurer les comptes iDRAC6.
20. Redirection USB Définit les classes CIM pour la représentation de la redirection à distance des ports USB locaux. L'iDRAC6 utilise ce profil en concomitance avec le profil de média virtuel pour configurer le média virtuel.
Extensions Dell
1. Dell™ Active Directory Client, Version 2.0.0 Définit les classes d'extension CIM et Dell pour configurer le client Active Directory de l'iDRAC6 et les privilèges locaux pour les groupes Active Directory.
2. Média virtuel Dell Définit les classes d'extension CIM et Dell pour la configuration du média virtuel de l'iDRAC6. Étend le profil de redirection USB.
3. Port Ethernet Dell Définit les classes d'extension CIM et Dell pour la configuration de l'interface NIC bande latérale pour le NIC de l'iDRAC6. Étend le profil du port Ethernet.
4. Gestion de l'utilisation de l'alimentation Dell Définit les classes d'extension CIM et Dell pour la représentation du budget d'alimentation du serveur hôtel et pour la configuration/le contrôle du budget d'alimentation du serveur hôte.

Pour plus d'informations, voir le site **www.dmtf.org/standards/profiles/**. Pour des mises à jour de cette liste de profils ou des informations, voir les notes de diffusion WS-MAN ou le fichier « Lisez-moi ».

La mise en uvre WS-MAN est conforme aux spécifications DMTF WS-MAN, version 1.0.0. Parmi les outils compatibles qui prennent en charge le protocole WS-MAN citons (sans toutefois être exhaustif) Microsoft Windows® Remote Management (WinRM), open wsman et wsmancli.

Retour á la page du sommaire

Retour á la page du sommaire

Utilisation de l'interface de ligne de commande SM-CLP iDRAC6

Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.1

Cette section fournit des informations sur le protocole Server Management-Command Line Protocol (SM-CLP) du consortium Distributed Management Task Force (DMTF) qui est incorporé dans l'iDRAC6.

REMARQUE : Cette section suppose que vous connaissez l'initiative SMASH (Systems Management Architecture for Server Hardware) et les spécifications SM-CLP. Pour plus d'informations sur ces spécifications, consultez le site Web de DMTF (Distributed Management Task Force) à l'adresse **www.dmtf.org**.

SM-CLP iDRAC6 est un protocole qui fournit des standards aux implémentations CLI de gestion de systèmes. SM-CLP est un sous-composant de l'initiative DMTF SMASH destinée à rationaliser la gestion de serveur à travers des plateformes multiples. La spécification SM-CLP, conjointement à MEAS (Managed Element Addressing Specification) et à de nombreux profils SM-CLP, décrit les verbes et les cibles correspondant à l'exécution de diverses tâches de gestion.

Prise en charge de SM-CLP iDRAC6

La SM-CLP est hébergée 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. SM-CLP iDRAC6 prend en charge tous les profils décrits dans le Tableau 11-1 « Profils CIM pris en charge ».

Les sections suivantes fournissent un aperçu de la fonctionnalité SM-CLP qui est hébergée par l'iDRAC6.

Fonctionnalités de la SM-CLP

La SM-CLP encourage la conception de verbes et de cibles pour fournir des capacités de gestion de systèmes par la CLI. Le verbe indique l'opération à effectuer et la cible détermine l'entité (ou l'objet) qui exécute l'opération.

Voici un exemple de la syntaxe de ligne de commande de la SM-CLP.

```
<verbe> [<options>] [<cible>] [<propriétés>]
```

Pendant une session SM-CLP type, vous pouvez effectuer des opérations à l'aide des verbes énumérés dans le Tableau 12-1.

Tableau 12-1. Verbes 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.
start	Active une cible.
stop	Désactive 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) au iDRAC6 avec les bonnes références.

L'invite SMCLP (/admin1->) est affichée.

Cibles SM-CLP

Le Tableau 12-2 fournit une liste des cibles fournies par la SM-CLP pour prendre en charge les opérations décrites dans le Tableau 12-1 ci-dessus.

Tableau 12-2. Cibles SM-CLP

Cible	Définitions
admin1	domaine admin
admin1/profiles1	Profils enregistrés dans iDRAC6.
admin1/hdwr1	Matériel
admin1/system1	Système cible géré
admin1/system1/redundancyset1	Bloc d'alimentation
admin1/system1/redundancyset1/pwrsupply*	Alimentation du système géré
admin1/system1/sensors1	Détecteurs du système géré
admin1/system1/capabilities1	Capacités de collecte SMASH du système géré
admin1/system1/capabilities1/ pwrcap1	Capacités d'exploitation de l'alimentation du système géré
admin1/system1/capabilities1/ elecap1	Capacités cible du système géré
admin1/system1/logs1	Cible des collections de journal
admin1/system1/logs1/log1	Entrée 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 collecte SMASH du système géré
admin1/system1/settings1/ pwrmaxsetting1	Paramètre d'allocation de puissance du système géré
admin1/system1/settings1/ pwrminsetting1	Paramètre d'allocation de puissance minimale du système géré
admin1/system1/capacities1	Collecte SMASH des capacités du système géré
admin1/system1/consoles1	Collecte 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	Temps de service du processeur de service
admin1/system1/sp1/capabilities1	Capacités de collecte SMASH du processeur de service
admin1/system1/sp1/capabilities1/clpcap1	Capacités de service CLP
admin1/system1/sp1/capabilities1/pwrmgtcap1	Capacités de gestion de l'alimentation sur le système
admin1/system1/sp1/capabilities1/ipcap1	Capacités d'interface IP
admin1/system1/sp1/capabilities1/dhcpcap1	Capacités 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 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 stockage
admin1/system1/sp1/capabilities1/adcap1	Capacités Active Directory
admin1/system1/sp1/capabilities1/rolemgtcap*	Capacités de gestion basée sur le rôle local
admin1/system1/sp1/capabilities/PwrutilmgtCap1	Capacités de gestion de l'alimentation
admin1/system1/sp1/capabilities/metriccap1	Capacités de service métrique
admin1/system1/sp1/capabilities1/elecap1	Capacités d'authentification multifacteur
admin1/system1/sp1/capabilities1/lanendptcap1	Capacités de terminaison LAN (port Ethernet)
admin1/system1/sp1/logs1	Collecte de journaux du processeur de service
admin1/system1/sp1/logs1/log1	Journal des événements système
admin1/system1/sp1/logs1/log1/record*	Entrée du journal système
admin1/system1/sp1/settings1	Collecte de 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 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 client DHCP
admin1/system1/sp1/clpsvc1	Service de protocole de service CLP
admin1/system1/sp1/clpsvc1/ clpendpt*	Point de terminaison de protocole de service CLP

admin1/system1/sp1/clpsvc1/ tcpendpt*	Point de terminaison TCP de protocole de service CLP
admin1/system1/sp1/jobq1	File d'attente 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	Point de terminaison de protocole d'interface IP
admin1/system1/sp1/ ipendpt1/gateway1	Passerelle d'interface IP
admin1/system1/sp1/ ipendpt1/dhcpendpt1	Point de terminaison de protocole client DHCP
admin1/system1/sp1/ ipendpt1/dnsendpt1	Point de terminaison de protocole 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	Point de terminaison LAN
admin1/system1/sp1/ lanendpt1/enetport1	Port Ethernet
admin1/system1/sp1/VMediaSvc1	Service de média virtuel
admin1/system1/sp1/ VMediaSvc1/tcpendpt1	Point de terminaison de protocole TCP de média virtuel
admin1/system1/sp1/swid1	Identité logiciel
admin1/system1/sp1/ swinstallsvc1	service d'installation de logiciel
admin1/system1/sp1/ account1-16	Compte d'authentification multifacteur (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 le rôle (RBA) local
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 le réseau local (SOL) IPMI
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'alimentation
admin1/system1/sp1/ pwrutilmgtsvc1/pwrcurr1	Service de gestion de l'alimentation, données des paramètres d'affectation de puissance
admin1/system1/sp1/metricsvc1	Service métrique
/admin1/system1/sp1/metricsvc1/cumbmd1	Définition métrique base cumulée
/admin1/system1/sp1/metricsvc1/cumbmd1/cumbmv1	Valeur métrique base cumulée
/admin1/system1/sp1/metricsvc1/cumwattamd1	Définition métrique consolidation puissance cumulée

/admin1/system1/sp1/metricsvc1/cumwattamd1/cumwattamv1	Valeur métrique consolidation puissance cumulée
/admin1/system1/sp1/metricsvc1/cumampamd1	Définition métrique consolidation courant cumulée
/admin1/system1/sp1/metricsvc1/cumampamd1/cumampamv1	Valeur métrique consolidation courant cumulée
/admin1/system1/sp1/metricsvc1/loamd1	Définition métrique consolidation inférieure
/admin1/system1/sp1/metricsvc1/loamd1/loamv*	Valeur métrique consolidation inférieure
/admin1/system1/sp1/metricsvc1/hiamd1	Définition métrique consolidation supérieure
/admin1/system1/sp1/metricsvc1/hiamd1/hiamv*	Valeur métrique consolidation supérieure
/admin1/system1/sp1/metricsvc1/avgamd1	Définition métrique consolidation moyenne
/admin1/system1/sp1/metricsvc1/avgamd1/avgamv*	Valeur métrique consolidation moyenne

---

Retour á la page du sommaire

Retour á la page du sommaire

Déploiement de votre système d'exploitation en utilisant VMCLI

Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.1

L'utilitaire d'interface de ligne de commande de média virtuel (VMCLI) est une interface de ligne de commande qui fournit les fonctionnalités de média virtuel de la station de gestion à l'iDRAC6 dans le système distant. À l'aide de VMCLI et de méthodes cryptées, 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

L'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 de 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 de démarrage pour votre système Linux.

Pour exécuter l'utilitaire, ouvrez une invite de commande et tapez les commandes suivantes :

```
dd if=<périphérique-d'entrée> de=<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 fichier. Incluez les programmes et/ou 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).

   Lorsque vous créez le fichier image, procédez comme suit :

   - Suivez les procédures d'installation réseau standard
   - Mettez 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 dans les systèmes distants de votre réseau.

La procédure suivante fournit un aperçu de haut niveau du déploiement du système d'exploitation dans les systèmes distants cibles.

1. Répertoriez les adresses IPv4 iDRAC6 des systèmes distants qui seront déployés dans le fichier texte **ip.txt**, en indiquant une adresse IPv4 par ligne.
2. Insérez un CD ou DVD de système d'exploitation amorçable 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 idrac> -c {<image iso9660> | <chemin>} -f {<image disquette>|<chemin>}
```

où

- <*utilisateur idrac*> est le nom d'utilisateur iDRAC6, par exemple **root**
- <*mot de passe idrac*> est le mot de passe de l'utilisateur iDRAC6, par exemple **calvin**
- <*image iso9660*> est le chemin d'accès à une image ISO9660 du CD ou DVD d'installation du système d'exploitation
- <*chemin*> est le chemin d'accès au périphérique contenant le CD ou DVD d'installation du système d'exploitation
- <*image disquette*> est le chemin d'une image de disquette valide

Le script **vm6deploy** transmet ses options de ligne de commande à l'utilitaire **VMCLI**. Voir « 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 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 d'interface de ligne de commande de média virtuel (VMCLI) est une interface de ligne de commande scriptable qui fournit les fonctionnalités de média virtuel de la station de gestion à l'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, seule une 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 de démarrage unique du micrologiciel iDRAC6 est activée
- Les communications sécurisées avec l'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 pouvoir exécuter iDRAC6.

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 d'administrateur sont également requis pour exécuter la commande VMCLI.

L'administrateur du système client contrôle les groupes et les privilèges d'utilisateurs, et contrôle 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 d'enregistrer 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 l'iDRAC6 dans le système distant et d'exécuter l'utilitaire.

Installation de l'utilitaire de gestion du contrôleur 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 logiciels de gestion de systèmes, notamment les diagnostics, la gestion du stockage, le service d'accès à distance et l'utilitaire IPMItool. Ce DVD contient aussi des fichiers lisez-moi, qui fournissent les dernières informations sur les produits logiciels de gestion de systèmes.

Le DVD *Dell Systems Management Tools and Documentation* inclut **vm6deploy**, un modèle de script qui illustre comment utiliser les 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 présents dans ce dernier. Si l'utilitaire IPMI 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 du système d'exploitation]`*

La syntaxe de ligne de commande respecte la casse. Pour plus d'informations, voir « Paramètres VMCLI ».

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 de la commande de système d'exploitation. Par exemple, dans 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 iDRAC6 et le port SSL, dont l'utilitaire a besoin pour établir une connexion de média virtuel avec l'iDRAC6 cible. Si vous entrez une adresse IPv4 ou un nom DDNS non valide, un message d'erreur s'affiche et la commande se termine.

<adresse IPv4 iDRAC> est une adresse IP unique valide ou le nom DDNS (Dynamic Domain Naming System) de l'iDRAC6 (s'il est pris en charge). Si le *<port SSL iDRAC>* est omis, le port 443 (port par défaut) est utilisé. À moins que le port SSL par défaut iDRAC6 n'ait été modifié, le port SSL optionnel n'est pas obligatoire.

Nom d'utilisateur iDRAC6

`-u <nom d'utilisateur iDRAC>`

Ce paramètre fournit le nom d'utilisateur iDRAC6 qui exécutera le média virtuel.

Le *<nom d'utilisateur iDRAC>* doit avoir les attributs suivants :

- Nom d'utilisateur valide
- Droit d'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 {<nom-du-périphérique> | <fichier-image>}`

où <*nom de périphérique*> est une lettre de lecteur valide (pour les systèmes Windows) ou un nom de fichier de périphérique valide (pour les systèmes Linux) et <*fichier image*> 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 # 4th partition on device (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 kernel prend en charge cette fonctionnalité, mais vous devez permettre 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 jusqu'à 8 LUN.)

2. Récupérez le nom de l'image de kernel en tapant la commande suivante à l'invite de commande :

   uname -r

3. Allez dans le répertoire **/boot** et supprimez le fichier de l'image de kernel, 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'écrira pas sur le média.

Omettez ce paramètre de la ligne de commande si vous ne virtualisez pas le lecteur de disquette. Si une valeur non valide est détectée, un message d'erreur s'affiche et la commande est interrompue.

Périphérique de CD/DVD ou fichier image

`-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 fournira 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 CD/DVD. Si une valeur non valide est détectée, un message d'erreur est répertorié et la commande est interrompue.

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. Le cas échéant, un message d'erreur s'affiche et la commande est interrompue 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 pour le cryptage de média virtuel sur *activé* dans les autres interfaces de configuration d'iDRAC6 comme RACADM ou l'interface Web.

Options d'environnement du système d'exploitation VMCLI

Les fonctionnalités du 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 serait 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.

Retour á la page du sommaire

Retour á la page du sommaire

Configuration de l'interface de gestion de plate-forme intelligente (IPMI)

Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.1

Configuration d'IPMI

Cette section fournit des informations sur la configuration et l'utilisation de l'interface IPMI de l'iDRAC6. L'interface comprend :

- IPMI sur le LAN
- IPMI sur série
- Série sur LAN

L'iDRAC6 est compatible IPMI 2.0. Vous pouvez configurer l'IPMI de l'iDRAC6 en utilisant :

- la GUI de l'iDRAC6 depuis votre navigateur,
- un utilitaire Open Source comme *IPMItool*,
- l'environnement IPMI Dell™ OpenManage™ : *ipmish*,
- la RACADM.

Pour plus d'informations sur l'utilisation de l'environnement IPMI, ipmish, consultez le Guide d'utilisation *Dell OpenManage Baseboard Management Controller Utilities* à l'adresse **support.dell.com \ manuals**.

Pour plus d'informations sur l'utilisation de la RACADM, voir « Utilisation de la RACADM à distance ».

Configuration d'IPMI à l'aide de l'interface Web

Pour des informations détaillées, voir « Configuration d'IPMI ».

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. Consultez « Utilisation de la RACADM à distance ».

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.

      Ouvrez une 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 du 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 : L'interface IPMI de l'iDRAC6 prend en charge le protocole RMCP+. Pour plus d'informations, consultez les spécifications d'IPMI 2.0.

      Ouvrez une 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 à 20 caractères au format hexadécimal valide.

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

Ouvrez une 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 minimum d'IPMI SOL.

REMARQUE : Le niveau de privilège minimum d'IPMI SOL détermine le privilège minimum requis pour activer l'IPMI SOL. Pour plus d'informations, consultez la spécification d'IPMI 2.0.

Ouvrez une 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.

Ouvrez une 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 9600, 19200, 57600 ou 115200 b/s.

Par exemple :

racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate 57600

c. Active le SOL pour un utilisateur individuel.

REMARQUE : Le SOL peut être activé ou désactivé pour chaque utilisateur individuel.

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

racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable -i *<id>* 2

où *<id>* est l'ID unique de l'utilisateur.

4. Configurez IPMI série.

a. Remplacez le mode de connexion IPMI série par le paramètre approprié.

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

racadm config -g cfgSerial -o cfgSerialConsoleEnable 0

b. Configurez le débit en bauds 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 9600, 19200, 57600 ou 115200 b/s.

Par exemple :

racadm config -g cfgIpmiSerial -o cfgIpmiSerialBaudRate 57600

c. Activez le contrôle du débit matériel IPMI série.

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

racadm config -g cfgIpmiSerial -o cfgIpmiSerialFlowControl 1

d. Configurez le niveau de privilège minimum de canal IPMI série.

Ouvrez une 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 le privilège de canal 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 IPMI série est 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, consultez la spécification d'IPMI 2.0.

Utilisation de l'interface série d'accès à distance IPMI

Dans l'interface série IPMI, 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 commande 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 RAC.

   À l'invite de commandes, 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 plus d'informations, voir « Définitions des groupes et des objets de la base de données des propriétés iDRAC6 ».

Configuration Série sur le LAN au moyen de l'interface Web

Pour des informations détaillées, voir « Configuration d'IPMI ».

REMARQUE : Vous pouvez utiliser Série sur le LAN avec les outils Dell OpenManage suivants : SOLProxy et IPMItool. Pour plus d'informations, voir le Guide d'utilisation *Dell OpenManage Baseboard Management Controller Utilities* à l'adresse **support.dell.com\manuals**.

Retour á la page du sommaire

Retour á la page du sommaire

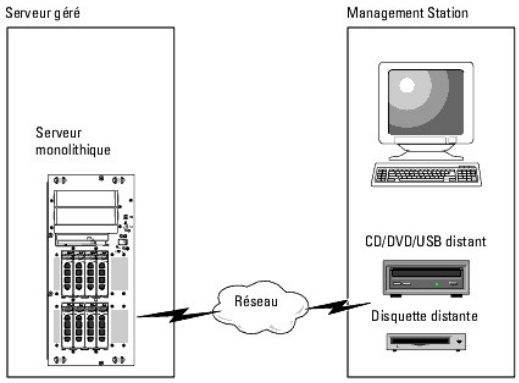
Configuration et utilisation du média virtuel

Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.1

Présentation

La fonctionnalité **Média virtuel**, accessible via le visualiseur de redirection de console, permet au serveur géré d'accéder au média connecté à un système distant sur le réseau. La Figure 15-1 illustre l'architecture globale d'un **média virtuel**.

Figure 15-1. 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 ou de 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 en condition 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 15-1 énumère 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 15-1. 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 patrimonial avec disquette 1.44	CD-ROM, DVD, CD-RW, lecteur mixte avec média de CD-ROM
Lecteur de disquette USB avec une disquette 1.44	Fichier image de CD-ROM/DVD au format ISO9660
Image de lecteur de disquette 1.44	Lecteur de CD-ROM USB avec média CD-ROM.
Disque amovible USB	

Station de gestion Windows

Pour exécuter la fonctionnalité de **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). Voir « Navigateurs Web pris en charge » pour obtenir des informations détaillées.

Station de gestion Linux

Pour exécuter la fonctionnalité de média virtuel sur une station de gestion exécutant le système d'exploitation Linux, installez une version prise en charge de Firefox. Pour plus d'informations, voir « Navigateurs Web pris en charge ».

Un environnement d'exécution Java (JRE) est requis pour exécuter le plug-in de redirection de console. Vous pouvez télécharger une version JRE à l'adresse **java.sun.com**. La version JRE 1.6 ou supérieure est recommandée.

Configuration du média virtuel

1. Connectez-vous à l'interface Web iDRAC6.
2. Sélectionnez **Système**→ **Console/Média**.
3. Cliquez sur **Configuration**→ **Média virtuel** pour configurer les paramètres du média virtuel.

   Le Tableau 15-2 décrit les valeurs de configuration du **média virtuel**.
4. Une fois les paramètres configurés, cliquez sur **Appliquer**.
5. Cliquez sur le bouton approprié pour continuer. Reportez-vous au Tableau 15-3.

Tableau 15-2. Propriétés de configuration du média virtuel

Attribut	Valeur
Condition de connexion du média distant	**Connecter** : connecte immédiatement le **média virtuel** au serveur. **Déconnecter** : déconnecte immédiatement le **média virtuel** du serveur. **Autoconnecter** : connecte le **média virtuel** au serveur uniquement quand une session de média virtuel est démarrée.
Nombre maximal de sessions	Affiche le nombre maximum de sessions de **média virtuel** autorisé qui est toujours fixé à 1.
Sessions actives	Affiche le nombre actuel de sessions de média virtuel.
Cryptage de média virtuel activé	Cochez la case 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 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 est décochée, elle apparaît comme un lecteur de clé USB.
Activer le démarrage une seule fois	Cochez cette case pour activer l'option de **démarrage unique**. Utilisez cet attribut pour démarrer à partir du média virtuel au prochain démarrage ; le système démarre alors à partir de l'entrée suivante dans la séquence d'amorçage. Cette option termine automatiquement la session du **média virtuel** après le premier démarrage du système.

Tableau 15-3. Boutons de la page de configuration

Bouton	Description
Imprimer	Imprime les valeurs de **Configuration** qui apparaissent à l'écran.
Actualiser	Recharge la page **Configuration**.
Appliquer les modifications	Enregistre les éventuels nouveaux paramètres de la page **Configuration**.

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 : La fenêtre Visualiseur de console doit rester active lorsque vous accédez au média virtuel.

REMARQUE : Suivez les étapes suivantes pour activer Red Hat® Enterprise Linux® (version 4) pour reconnaître un périphérique SCSI avec de multiples 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 lecteur CD/DVD ou le lecteur de disquette virtuel :

   cat /proc/scsi/scsi

REMARQUE : Avec le média virtuel, il n'est possible de virtualiser qu'une seule disquette/clé USB/image/clé et un seul lecteur optique à partir de la 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 lecteur de disquette et un 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 lecteur de disquette disponible. Les lecteurs optiques pris en charge incluent un lecteur optique disponible ou un fichier image ISO maximum.

Connexion du média virtuel

Suivez les étapes suivantes pour exécuter le média virtuel :

1. Ouvrez un navigateur Web pris en charge sur votre station de gestion. Pour plus d'informations, consultez la section « Navigateurs Web pris en charge ».

2. Démarrez l'interface Web iDRAC6. Pour plus d'informations, voir « Accès à l'interface Web ».

3. Sélectionnez **Système**→ **Console/Média**.

   La page **Redirection de console et Média virtuel** s'affiche. Si vous souhaitez modifier les valeurs des attributs affichés, voir « Configuration du média virtuel ».

   REMARQUE : L'option **Fichier image de disquette** dans **Lecteur de disquette** (si applicable) peut apparaître, comme ce périphérique peut être virtualisé comme un lecteur de disquette virtuel. Vous pouvez sélectionner simultanément un lecteur optique et un lecteur flash de disquette /USB afin de les 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 du système d'exploitation Windows qui sont configurés avec l'option de sécurité avancée d'Internet Explorer. Pour résoudre ce problème, consultez la documentation de votre système d'exploitation Microsoft ou contactez votre administrateur système.

4. Cliquez sur **Lancer le visualiseur**.

   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 **iDRACKVM Agent** se lance dans une fenêtre distincte.

5. Cliquez sur **Outils**→ **Lancer média virtuel**.

   L'assistant Redirection de média s'affiche.

   REMARQUE : Ne fermez pas cet assistant, sauf si vous désirez mettre fin à la session média virtuel.

6. Si le média est connecté, vous devez le déconnecter avant d'établir une connexion avec une source de média différente. Décochez la case à gauche du lecteur que vous souhaitez déconnecter.

7. Cochez la case à côté du type de lecteur que vous souhaitez connecter.

   Si vous souhaitez connecter une image de disquette ou une image ISO, entrez le chemin (sur votre ordinateur local) d'accès à 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 média virtuel**.

2. Décochez la case à gauche du lecteur 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 Redirection de média.

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 énumérés dans le bon ordre.

Pour changer le paramètre du BIOS, effectuez les étapes suivantes :

1. Démarrez le serveur géré.

2. Appuyez sur<F2> pour entrer dans 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 énuméré comme étant le premier périphérique avec un média de démarrage. 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 essaie de démarrer à partir d'un périphérique d'amorçage en suivant la séquence d'amorçage. Si le périphérique virtuel est connecté et qu'un média de démarrage est présent, le système démarre sur ce périphérique virtuel. Autrement, le système ignore le périphérique, tout comme un périphérique physique sans média de démarrage.

Installation de systèmes d'exploitation avec un média virtuel

Cette section décrit une méthode manuelle interactive pour installer le système d'exploitation sur votre station de gestion, ce qui peut prendre plusieurs heures. Une procédure d'installation sous forme de script du système d'exploitation utilisant le **média virtuel** peut prendre moins de 15 minutes. Pour plus d'informations, voir « Déploiement du système d'exploitation ».

1. Vérifiez les points suivants :
   - Le CD d'installation de votre 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 » afin de garantir que le BIOS est configuré 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) du panneau de configuration du média virtuel.

2. Insérez le CD/DVD suivant/ dans le lecteur optique distant.

3. Mappez (redirigez) ce CD/DVD du panneau de configuration du média virtuel.

   L'insertion d'un nouveau CD/DVD dans le lecteur optique distant sans démappage peut se solder par un échec.

Fonctionnalité de démarrage unique

La fonctionnalité de démarrage unique vous aide à modifier temporairement l'ordre de démarrage afin de démarrer à partir d'un périphérique média virtuel. Cette fonctionnalité est utilisée conjointement au média virtuel, en règle générale lors de l'installation de systèmes d'exploitation.

REMARQUE : Vous devez disposer de privilèges de **Configuration iDRAC6** pour utiliser cette fonctionnalité.

REMARQUE : Les périphériques distants doivent être redirigés à l'aide du média virtuel pour utiliser cette fonctionnalité.

Utilisation de la fonctionnalité de démarrage unique :

1. Allumez le serveur et accédez au gestionnaire de démarrage du BIOS.
2. Modifiez la séquence d'amorçage afin de démarrer à partir du périphérique média virtuel.
3. Connectez-vous à l'iDRAC6 par le biais de l'interface Web et cliquez sur **Système**→ **Console/Média**→ **Configuration**.
4. Cochez l'option **Activer le démarrage unique** sous Média virtuel.
5. Arrêtez et redémarrez le serveur.

   Le serveur démarre à partir du périphérique média virtuel. Au prochain redémarrage du serveur, la connexion au média virtuel distant est interrompue.

   REMARQUE : Le média virtuel doit être en condition de **connexion** de manière à ce que les lecteurs virtuels apparaissent dans la séquence d'amorçage. Assurez-vous que le support amorçable est présent dans le lecteur virtualisé pour activer la fonctionnalité de **démarrage unique**.

Utilisation d'un média virtuel pendant 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 fréquemment posées concernant le média virtuel

Le Tableau 15-4 répertorie les questions les plus fréquentes et les réponses correspondantes.

Tableau 15-4. 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 le lien entre le serveur et le lecteur virtuel. Si les paramètres de configuration du média virtuel sont modifiés dans l'interface Web iDRAC6 ou via les commandes RACADM locales, tout média connecté est déconnecté lorsque les modifications de la configuration sont appliquées. 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 pour obtenir la liste des systèmes d'exploitation pris en charge.
Quels sont les navigateurs Web pris en charge par iDRAC6 ?	Pour une liste des navigateurs Web pris en charge, voir « Navigateurs Web pris en charge ».
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 d'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 la GUI et continuez l'opération précédente. • Si le délai d'attente du réseau expire, le micrologiciel iDRAC6 interrompt la connexion, en déconnectant le lien 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 entré des commandes RADACM. Pour rétablir la connexion au lecteur virtuel, utilisez la fonctionnalité du **média virtuel**.
Une installation du système d'exploitation Windows par vMédia 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 d'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.
Comment puis-je configurer mon périphérique virtuel comme périphérique de démarrage ?	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 l'ordre de démarrage des périphériques, si nécessaire. En outre, rendez le périphérique virtuel amorçable en appuyant sur la touche « Espace » dans la séquence d'amorçage de l'installation CMOS. Par exemple, pour démarrer à partir d'un lecteur de CD, définissez-le en tant que premier lecteur dans la séquence de démarrage.

À partir de quels types de média puis-je démarrer ?	L'iDRAC6 vous permet de démarrer à partir des médias de démarrage suivants : • Média de données CD-ROM/DVD • Image ISO 9660 • Disquette 1.44 ou image de disquette • Clé USB qui est reconnue par le système d'exploitation comme disque amovible • Image de clé USB
Comment faire pour faire de ma clé USB une clé de démarrage ?	Recherchez l'utilitaire de démarrage Dell sur le site **support.dell.com**, un programme Windows que vous pouvez utiliser pour rendre votre clé USB Dell amorçable. Vous pouvez également démarrer à l'aide d'une disquette d'amorçage Windows 98 et copier les fichiers système de la disquette d'amorçage sur votre clé USB. Par exemple, à l'invite du DOS, tapez la commande suivante : `sys a: x: /s` où *x*: est la clé USB que vous voulez utiliser comme clé de démarrage.
Je n'arrive pas à trouver mon lecteur de disquette/CD virtuel sur un système exécutant le système d'exploitation Red Hat Enterprise Linux ou sous 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 installer le lecteur de disquette virtuel, recherchez le nud de périphérique que Linux attribue au lecteur de disquette virtuel. Procédez comme suit pour rechercher et monter correctement le lecteur de disquette virtuel : 1. Ouvrez une invite de commande Linux et exécutez la commande suivante : `grep "Virtual Floppy" /var/log/messages` 2. Recherchez la dernière entrée de ce message et notez l'heure. 3. À l'invite de Linux, exécutez la commande suivante : `grep "hh:mm:ss" /var/log/messages` où *hh:mm:ss* correspond au cachet horaire du message retourné par grep à l'étape 1. 4. À l'étape 3, lisez le résultat de la commande grep et recherchez le nom du périphérique qui est donné à la disquette virtuelle Dell. 5. Assurez-vous que vous êtes relié et connecté au lecteur de disquette virtuel. 6. À l'invite de Linux, exécutez la commande suivante : `mount /dev/sdx /mnt/floppy` où */dev/sdx* est le nom du périphérique trouvé à l'étape 4 /mnt/floppy est le point de montage.
Je n'arrive pas à trouver mon lecteur de disquette/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)* Pour installer le lecteur de CD virtuel, recherchez le nud de périphérique que Linux attribue au lecteur de CD virtuel. Suivez ces étapes pour trouver et installer le lecteur de CD virtuel : 1. Ouvrez une invite de commande Linux et exécutez la commande suivante : `grep "Virtual CD" /var/log/messages` 2. Recherchez la dernière entrée de ce message et notez l'heure. 3. À l'invite de Linux, exécutez la commande suivante : `grep "hh:mm:ss" /var/log/messages` où hh:mm:ss correspond au cachet horaire du message retourné par grep à l'étape 1. 4. À l'étape 3, lisez le résultat de la commande grep et recherchez le nom du périphérique qui est donné à « Dell Virtual CD ». 5. Assurez-vous que vous êtes relié et connecté au lecteur de CD virtuel. 6. À l'invite de Linux, exécutez la commande suivante : `mount /dev/sdx /mnt/CD` où */dev/sdx* est le nom du périphérique trouvé à l'étape 4 /mnt/floppy est le point de montage.
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 du micrologiciel entraînent une 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 média virtuel et les périphériques flash virtuel sont connectés au BUS hôte USB comme un périphérique USB composite et ils partagent un port USB commun. À chaque fois qu'un périphérique média virtuel ou flash virtuel est connecté au BUS hôte USB ou déconnecté du BUS, tous les périphériques média virtuel ou flash virtuel sont momentanément déconnectés du bus hôte USB et seront par la suite reconnectés. Si un périphérique média virtuel est utilisé par le système d'exploitation hôte, vous devez éviter de connecter ou déconnecter un ou plusieurs périphérique(s) média virtuel ou flash virtuel. Il est conseillé de commencer par connecter tous les

	périphériques USB nécessaires avant de les utiliser.
Que fait le bouton de réinitialisation USB ?	Il réinitialise les périphériques USB distants et locaux connectés au serveur.

Retour á la page du sommaire

Retour á la page du sommaire

Configuration d'une carte de support vFlash pour utilisation avec l'iDRAC6

Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.1

La carte de support vFlash est une carte Secure Digital (SD) qui se connecte dans un logement de carte iDRAC6 Enterprise en option à l'arrière du système. Son espace de stockage se comporte comme toute clé de mémoire flash USB. Pour plus d'informations sur l'installation et le retrait de la carte de support vFlash de votre système, consultez le *Manuel du propriétaire du matériel* à l'adresse **support.dell.com\manuals**.

Configuration de la carte de support vFlash via l'interface Web iDRAC6

Activation ou désactivation de la carte de support vFlash

REMARQUE : L'option **Carte Flash virtuelle activée** est active uniquement si une carte de support vFlash est présente. Si aucune carte n'est présente, le message suivant s'affiche :

```
SD Card not inserted. Please insert an SD card of size greater than 256MB. (Pas de carte SD insérée. Insérez une carte SD d'une capacité supérieure à 256 Mo.)
```

1. Assurez-vous que la carte de support VFlash a été installée.
2. Ouvrez une fenêtre de navigateur Web prise en charge et connectez-vous à l'interface Web iDRAC6.
3. Dans l'arborescence Système, cliquez sur **Système**.
4. Cliquez sur l'onglet **Carte Flash virtuelle**.

   L'écran **Carte Flash virtuelle** s'affiche.
5. Sélectionnez l'option **Carte Flash virtuelle activée** pour activer la carte de support vFlash. L'activation de la carte Flash virtuelle présente le fichier image **ManagedStore.IMG** créé sur la carte SD sous forme de clé USB de la taille sélectionnée. La carte Flash virtuelle peut être activée uniquement si une image **ManagedStore.IMG** valide est présente sur la carte SD. Pour désactiver, décochez l'option.

   REMARQUE : Les fichiers ManagedStore.IMG et ManagedStore.ID vus sur la page de la GUI *Carte Flash virtuelle* sont visibles sur la carte SD et non sur le système d'exploitation du serveur hôte.
6. Cliquez sur **Appliquer les modifications**.

Formatage de la carte de support vFlash

REMARQUE : L'option **Formater** est active uniquement si une carte de support vFlash est présente. En outre, la carte SD peut être formatée uniquement si la carte Flash virtuelle est désactivée.

1. Connectez-vous à l'interface Web iDRAC6.
2. Dans l'arborescence Système, cliquez sur **Système**.
3. Cliquez sur l'onglet **Carte Flash virtuelle**.

   L'écran **Carte Flash virtuelle** s'affiche.
4. Désactivez l'option **Carte Flash virtuelle activée**.
5. Cliquez sur **Formater** pour créer le fichier image de la carte Flash virtuelle, **ManagedStore.IMG**, sur la carte SD. Le fichier texte **ManagedStore.ID** est également créé sur la carte SD et fournit des informations sur l'image de la carte Flash virtuelle.

   Un message d'alerte indiquant que toutes les images présentes sur la carte seront supprimées lors du formatage s'affiche et vous demande de confirmer ce formatage. Cliquez sur **OK** pour continuer.

   Une barre d'état s'affiche, indiquant la progression du formatage.

Téléversement d'une image de disque

1. Assurez-vous que la taille du fichier image n'excède pas 256 Mo.

   REMARQUE : Bien que la carte vFlash puisse être supérieure à 256 Mo, seulement 256 Mo sont accessibles à l'heure actuelle.

   REMARQUE : La carte Flash virtuelle vous permet de stocker l'image d'amorçage d'urgence et les outils de diagnostic directement sur le support vFlash. Le fichier image peut être une image de disquette amorçable DOS sous forme de fichier ***.img** pour Windows ou un fichier **diskboot.img** généré par le support Red Hat® Enterprise Linux® pour Linux. Le fichier **diskboot.img** peut servir à créer un disque de secours ou un disque permettant d'effectuer des installations réseau. Vous pouvez utiliser la carte Flash virtuelle pour héberger une image persistante à des fins d'utilisation générale ou d'urgence dans le futur.

2. Connectez-vous à l'interface Web iDRAC6.

3. Dans l'arborescence Système, cliquez sur **Système**.

4. Cliquez sur l'onglet **Carte Flash virtuelle**.

   L'écran **Carte Flash virtuelle** s'affiche.

5. Désactivez l'option **Carte Flash virtuelle activée**.

6. Dans la section **Lecteur Flash virtuel**, tapez le chemin d'accès au fichier image ou cliquez sur **Parcourir** pour accéder à son emplacement sur le système.

   Cliquez sur **Téléverser**.

   Une barre d'état s'affiche, indiquant la progression du téléversement.

REMARQUE : Vous pouvez téléverser une image ISO amorçable vers la partition Flash virtuelle, mais elle ne sera dès lors plus amorçable. Convertissez l'image ISO en image IMG afin de rendre l'image IMG amorçable.

Affichage de la taille de clé Flash virtuelle

Le menu déroulant **Virtual Flash Key Size** (Taille de la clé Flash virtuelle) affiche le paramètre de taille actuel.

Configuration de la carte de support vFlash à l'aide de RACADM

Activation ou désactivation de la carte de support vFlash

Ouvrez une console locale sur le serveur, puis une session et tapez :

```
racadm cfgRacVirtual cfgVirMediaKeyEnable [ 1 ou 0 ]
```

où `1` signifie activé et `0` signifie désactivé.

REMARQUE : Pour plus d'informations sur la commande **cfgRacVirtual**, y compris le détail des résultats renvoyés, voir « cfgRacVirtual ».

REMARQUE : La commande RACADM fonctionne uniquement si une carte de support vFlash est présente. Si aucune carte n'est présente, le message suivant s'affiche : *ERROR: Unable to perform the requested operation. Ensure that a non–write protected SD Card is inserted.* (*ERREUR : Impossible d'effectuer l'opération demandée. Assurez-vous qu'une carte SD non protégée en écriture est insérée.*)

Réinitialisation de la carte de support vFlash

Ouvrez une console texte Telnet/SSH sur le serveur, ouvrez une session et tapez :

```
racadm vmkey reset
```

PRÉCAUTION : La réinitialisation de la carte de support vFlash à l'aide de la commande RACADM permet de redéfinir la taille de la clé sur 256 Mo et de supprimer toutes les données existantes.

REMARQUE : Pour plus d'informations sur la clé vmkey, consultez « vmkey ». La commande RACADM fonctionne uniquement si une carte de support vFlash est présente. Si aucune carte n'est présente, le message suivant s'affiche : *ERROR: Unable to perform the requested operation. Ensure that a SD Card is inserted.* (*ERREUR : Impossible d'effectuer l'opération demandée. Assurez-vous qu'une carte SD est insérée.*)

Retour á la page du sommaire

Retour á la page du sommaire

Surveillance et gestion de l'alimentation

Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.1

Les systèmes Dell™ PowerEdge™ intègrent de nombreuses fonctionnalités améliorées de gestion de l'alimentation. La plateforme entière, des matériels aux micrologiciels en passant par les logiciels de gestion de systèmes, a été conçue dans l'optique de réduire la consommation et d'améliorer la surveillance et la gestion de l'alimentation.

La conception du matériel de base a été optimisée selon la perspective de l'alimentation :

- Des alimentations hautes performances et des régulateurs de tension ont été incorporés.
- 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 surveillance et de gestion de l'alimentation.

- **Bilan de puissance et budgétisation :** au démarrage, un inventaire système permet de calculer un bilan de puissance système de la configuration actuelle.
- **Seuil de puissance :** les systèmes peuvent comporter un limiteur pour maintenir un seuil de puissance spécifié.
- **Surveillance de l'alimentation :** l'iDRAC6 interroge les modules d'alimentation pour collecter des mesures. L'iDRAC6 constitue 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 afficher les informations dans l'écran **Surveillance de l'alimentation**.

Bilan de puissance, budgétisation de l'alimentation et seuil de puissance

Sur le plan de l'exploitation, vous pouvez ne disposer que d'un refroidissement limité au niveau du rack. Avec un seuil de puissance défini par l'utilisateur, vous pouvez distribuer l'alimentation conformément aux besoins pour obtenir les performances requises.

L'iDRAC6 surveille la consommation électrique et limite dynamiquement les processeurs en fonction du seuil de puissance que vous avez défini, pour optimiser les performances avec vos critères de consommation.

Surveillance de l'alimentation

L'iDRAC6 contrôle continuellement la consommation électrique dans les serveurs PowerEdge. L'iDRAC6 calcule les valeurs de puissance suivantes et fournit les informations via son interface Web ou CLI RACADM :

- Consommation énergétique cumulée
- Consommation de puissance moyenne, minimale et maximale
- Valeurs de hauteur de puissance
- Consommation de puissance (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 RACADM (CLI) pour gérer et configurer les boutons 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 unités d'alimentation, notamment la consommation de puissance potentielle minimale et maximale ;
- afficher et configurer le seuil du bilan de puissance du serveur ;

Afficher l'état d'intégrité des unités d'alimentation

La page **Blocs d'alimentation** indique l'état et la puissance des unités d'alimentation installées sur le serveur.

Utilisation de l'interface Web

Pour afficher l'état d'intégrité des unités d'alimentation :

1. Connectez-vous à l'interface Web iDRAC6.
2. Sélectionnez **Blocs d'alimentation** dans l'arborescence du système. La page **Blocs d'alimentation** fournit les informations suivantes :
   - **État de la redondance des blocs d'alimentation** - Les valeurs possibles sont les suivantes :
     - **Totale** : les blocs d'alimentation PS1 et PS2 sont du même type et fonctionnent correctement.
     - **Perdue** : les blocs d'alimentation PS1 et PS2 sont de type différent ou l'un des deux ne fonctionne pas correctement. Aucune redondance n'existe.
     - **Désactivée** : un seul des deux blocs d'alimentation est disponible. Aucune redondance n'existe.
   - **Blocs d'alimentation individuels** - Les valeurs possibles sont les suivantes :
   - **État** peut indiquer :
     - **OK** signifie que l'unité d'alimentation est présente 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 de l'unité d'alimentation PS-n concernée, 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 limite maximale de la puissance CA disponible pour le système sur le 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 puissance suffisante est disponible pour la configuration du système.
   - **Condition de la connexion** indique l'état des blocs d'alimentation : présent et OK, entrée perdue, absent ou panne prévisible.
   - **Version FW** 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 RACADM

Ouvrez une console texte Telnet/SSH sur l'iDRAC, ouvrez une session et tapez :

```
racadm getconfig -g cfgServerPower
```

Affichage du Bilan de puissance

Le serveur fournit des aperçus 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. Connectez-vous à l'interface Web iDRAC6.
2. Cliquez sur l'onglet **Gestion de l'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 représentes la plage des consommations en courant alternatif que vous pouvez définir comme seuil système. Une fois sélectionné, ce seuil constitue la charge CA maximale que le système peut faire supporter au centre de données.

Consommation de puissance potentielle minimale représente la valeur de seuil du bilan de puissance la plus basse que vous puissiez définir.

Consommation de puissance potentielle maximale représente la valeur de seuil du bilan de puissance la plus élevée que vous puissiez définir. Cette valeur

est également la consommation de puissance maximale absolue de la configuration système actuelle.

Utilisation de RACADM

Ouvrez une console texte Telnet/SSH sur l'iDRAC, ouvrez une session et tapez :

```
racadm getconfig -g cfgServerPower
```

REMARQUE : Pour plus d'informations concernant la commande cfgServerPower, y compris le détail des résultats renvoyés, voir « cfgServerPower ».

Seuil du bilan de puissance

Le seuil du bilan de puissance, s'il est activé, permet de définir une limite de consommation pour le système. Les performances du système sont dynamiquement ajustées afin de maintenir la consommation à proximité du seuil spécifié. La consommation de puissance réelle peut être inférieure pour les faibles charges de travail et peut momentanément excéder le seuil jusqu'à ce que les réglages de performances soient terminés.

Si vous cochez **Activé** pour Seuil du bilan de puissance, le système impose le seuil spécifié par l'utilisateur. Si vous laissez la valeur Seuil du bilan de puissance **non cochée**, le système n'est pas limité en alimentation. Par exemple, pour une configuration du système déterminée, la consommation de puissance potentielle maximale est de 700 W et la consommation de puissance 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 ne dépasse pas le seuil de 525 W spécifié par l'utilisateur.

Utilisation de l'interface Web

1. Connectez-vous à l'interface Web iDRAC6.
2. Cliquez sur l'onglet **Power Management** (Gestion de l'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 **Seuil du 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 de puissance potentielle minimale-maximale. Par exemple, un seuil de 100 % signifie une consommation de puissance potentielle maximale, tandis que 0 % signifie une consommation de puissance potentielle minimale.

   REMARQUE : Le seuil du bilan de puissance ne peut pas être supérieur à la consommation de puissance potentielle maximale, ni inférieur à la consommation de puissance potentielle minimale.

5. Cochez **Activé** pour activer le seuil ou laissez non coché. Si vous spécifiez **Activé**, le système impose le seuil spécifié par l'utilisateur. Si vous laissez l'option **non cochée**, le système n'est pas limité en alimentation.
6. Cliquez sur **Appliquer les modifications**.

Utilisation de RACADM

```
racadm config -g cfgServerPower -o cfgServerPowerCapWatts <valeur de la capacité d'alimentation d'entrée en watts>

racadm config -g cfgServerPower -o cfgServerPowerCapBTUhr <valeur de la capacité d'alimentation d'entrée en BTU/h>

racadm config -g cfgServerPower -o - cfgServerPowerCapPercent <valeur de la capacité d'alimentation d'entrée en %>
```

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 différente de la valeur lue, par exemple un seuil défini sur 600 BTU/h sera relu avec la valeur 601 BTU/h.

Affichage de la surveillance de l'alimentation

Utilisation de l'interface Web

Pour afficher les données de surveillance de l'alimentation :

1. Connectez-vous à l'interface Web iDRAC6.
2. Sélectionnez **Surveillance de l'alimentation** dans l'arborescence du système. La page **Surveillance de l'alimentation** s'affiche.

Les informations affichées sur cette page sont décrites ci-après.

Surveillance de l'alimentation

- **Etat : OK** indique que les unités d'alimentation sont présentes et communiquent avec le serveur. **Avertissement** indique qu'une alerte d'avertissement a été émise et **Critique** indique qu'une alerte de panne a été générée.
- **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 électrique actuelle en watts/BTU/h.

Intensité

- **Emplacement :** indique le nom de l'unité d'alimentation PS-n concernée, n étant le numéro du bloc d'alimentation.
- **Lecture :** la consommation électrique actuelle en ampères

Statistiques de consommation de puissance

REMARQUE : Il existe actuellement une erreur dans le listage de l'heure en cours et de l'heure de consommation maximale. La valeur apparaissant pour l'heure en cours est en fait l'heure de consommation maximale et inversement.

- Cumulée affiche la consommation d'énergie cumulée actuelle du serveur, mesurée à l'entrée des blocs d'alimentation. La valeur est indiquée en KWh et représente l'énergie totale utilisée par le système. Vous pouvez réinitialiser cette valeur à l'aide du bouton **Réinitialiser les statistiques d'alimentation cumulée**.
- **Intensité maximale** spécifie l'intensité maximale au cours de l'intervalle spécifié par l'heure de début et l'heure actuelle. Vous pouvez réinitialiser cette valeur à l'aide du bouton **Réinitialiser les statistiques d'alimentation maximale**.
- **Puissance maximale** spécifie la puissance maximale au cours de l'intervalle spécifié par l'heure de début et l'heure actuelle. Vous pouvez réinitialiser cette valeur à l'aide du bouton **Réinitialiser les statistiques d'alimentation maximale**.
- **Heure de début des mesures** affiche la date et l'heure enregistrées depuis que la dernière valeur relative à la consommation d'énergie du système a été effacée et qu'un nouveau cycle de mesures a débuté. Pour **Cumulée**, vous pouvez réinitialiser la valeur avec le bouton **Réinitialiser les statistiques d'alimentation cumulée**, mais elle persistera jusqu'à une opération de réinitialisation ou de basculement du système. Pour **Intensité maximale** et **Puissance maximale**, vous pouvez réinitialiser la valeur avec le bouton **Réinitialiser les statistiques d'alimentation maximale**, mais elle persistera également jusqu'à une opération de réinitialisation ou de basculement du système.
- **Heure de fin** pour **Cumulée** affiche la date et l'heure de calcul de la consommation d'énergie du système pour l'affichage. Pour **Intensité maximale** et **Puissance maximale**, les champs **Heure de fin** affichent l'heure à laquelle ces pics se sont produits.

REMARQUE : Les statistiques de consommation de puissance sont conservées lors des réinitialisations du système, reflétant ainsi l'ensemble des activités qui se sont produites dans l'intervalle entre les heures de début et de fin indiquées. Le bouton **Réinitialiser les statistiques d'alimentation maximale** permet de redéfinir le champ respectif sur la valeur zéro. Dans le tableau suivant, les données de consommation électrique ne sont pas conservées lors des réinitialisations du système et sont ramenées à la valeur zéro. Les valeurs de puissance affichées sont des moyennes cumulatives au cours de l'intervalle de temps respectif (minute, heure, jour et semaine précédentes). Comme les intervalles de temps du début à la fin peuvent ici différer de ceux des statistiques de consommation de puissance, les valeurs de puissance maximale (Maximum en watts par rapport à Consommation de puissance maximale) peuvent différer.

Consommation de puissance

- Affiche la puissance consommée moyenne, maximale et minimale du système au cours de la minute, de l'heure, de la journée et de la semaine précédente.
- Consommation de puissance moyenne : moyenne de la minute précédente, heure précédente, jour précédent et semaine précédente.
- Consommation de puissance maximale et Consommation de puissance minimale : les consommations de puissance maximale et minimale observées au cours de l'intervalle de temps donné.
- Heure de puissance max et Heure de puissance min : heure à laquelle les consommations de puissance maximale et minimale ont été observées.

hauteur

La hauteur instantanée du système indique la différence entre la puissance disponible dans les unités d'alimentation et la consommation actuelle du système.

La hauteur maximale du système indique la différence entre la puissance disponible dans les unités d'alimentation et la consommation maximale du système.

Afficher graphique

Cliquez sur ce bouton pour afficher des graphiques illustrant la consommation de puissance et de courant, respectivement en watts et en ampères de l'iDRAC6 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 figurant 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 de consommation de puissance ou de courant.

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 d'**Administrateur de contrôle du châssis.**

iDRAC vous permet d'effectuer plusieurs actions de gestion de l'alimentation à distance, par exemple un arrêt méthodique.

Utilisation de l'interface Web

1. Connectez-vous à l'interface Web iDRAC6.
2. Cliquez sur l'onglet **Power Management** (Gestion de l'alimentation). La page **Power Control** (Contrôle de l'alimentation) s'affiche.
3. Sélectionnez l'une des **opérations de contrôle de l'alimentation** suivantes en cliquant sur le bouton d'option 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 un NMI pour arrêter le système.
   - **Arrêt normal** arrête le système.
   - **Réinitialisation du système** (redémarrage à chaud) redémarre le système sans le mettre hors tension. Cette option est désactivée si le système est déjà hors tension.
   - **Cycle d'alimentation du système** (redémarrage 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 lancer la tâche de gestion de l'alimentation (réinitialisation du système, par exemple).

Utilisation de 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 (état de l'alimentation).

Retour á la page du sommaire

Retour á la page du sommaire

Utilisation de l'utilitaire de configuration iDRAC

Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.1

Présentation

L'utilitaire de configuration iDRAC est un environnement de configuration de prédémarrage vous permettant d'afficher et de définir les paramètres de la carte iDRAC6 et du serveur géré. Vous pouvez notamment :

- afficher les numéros de révision du micrologiciel pour iDRAC6 et le micrologiciel de fond de panier principal ;
- activer ou désactiver le réseau local iDRAC6 ;
- activer ou désactiver IPMI sur le LAN ;
- configurer les paramètres LAN ;
- configurer le média virtuel ;
- configurer la carte à puce ;
- changer le nom d'utilisateur et le mot de passe d'administration
- rétablir les paramètres d'usine de la configuration iDRAC ;
- afficher les messages du journal des événements système (SEL) ou d'effacer les messages du journal ;
- configurer le LCD ;
- configurer les Services système.

Les tâches que vous pouvez réaliser à l'aide de l'utilitaire de configuration iDRAC peuvent également être menées à bien avec d'autres utilitaires fournis par le logiciel iDRAC 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.

Démarrage de l'utilitaire de configuration iDRAC

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 sec...** s'affiche, appuyez immédiatement sur <Ctrl><E>.

REMARQUE : Si votre système d'exploitation commence à se charger avant que vous avez appuyé sur <Ctrl><E>, laissez le système terminer son démarrage, puis redémarrez votre serveur et réessayez.

L'utilitaire de configuration iDRAC s'affiche. Les deux premières lignes fournissent des informations sur le micrologiciel iDRAC6 et les révisions 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, les interfaces SM-CLP et 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 iDRAC

Sous les messages de révision du micrologiciel, le reste de l'utilitaire de configuration iDRAC se compose d'un menu d'éléments auxquels vous pouvez accéder à l'aide de la <flèche vers le haut> et de 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 gauche>, la <flèche droite> ou sur <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 iDRAC, 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 iDRAC.

LAN iDRAC6

Utilisez la <flèche gauche>, la <flèche 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 redirection de console et le média virtuel.

Si vous choisissez de désactiver le LAN, l'avertissement suivant s'affiche :

```
iDRAC6 Out-of-Band interface will be disabled if the LAN Channel is OFF.

Press any key to clear the message and continue.

(L'interface hors bande iDRAC6 sera 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 iDRAC 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 sur LAN

Appuyez sur la <flèche gauche>, la <flèche 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 :

```
iDRAC IPMI Over LAN Out-of-Band interface will be disabled if the LAN Channel is OFF. (L'interface LAN hors bande iDRAC IPMI est désactivée si le canal LAN est désactivé. )
```

Appuyez sur n'importe quelle touche pour effacer le message et continuer. Voir « LAN iDRAC6 » 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 18-1. Paramètres LAN

Élément	Description
Paramètres communs	
Sélection de NIC	Appuyez sur la <flèche droite>, la <flèche gauche> et la barre d'espace pour basculer d'un mode à l'autre. Les modes disponibles sont : **Dédié, Partagé**, **Partagé avec basculement LOM2** et **Partagé avec basculement tous LOM**. Ces modes permettent à iDRAC6 de se servir de l'interface correspondante pour communiquer avec l'extérieur.
MAC Address (Adresse Mac)	Il s'agit de l'adresse MAC non modifiable de l'interface réseau iDRAC6.
Activer le VLAN	Sélectionnez **Activé** pour activer le filtrage du réseau local virtuel pour iDRAC6.
ID du VLAN	Si **Activer le VLAN** est **Activé**, entrez une ID du VLAN ID entre 1 et 4 094.
VLAN	Si **Activer le VLAN** est **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 accéder au nom iDRAC6 dans DNS.
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 **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. Entrez le nom de l'hôte des alertes Platform Event Trap (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 **Activé**, entrez 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 **Activer** ou **Désactiver** 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 0s (zéros).
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. 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. Si la **source d'adresse IP** est définie sur **Statique**, entrez l'adresse IP que vous souhaitez attribuer à iDRAC6. 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. Si la **source d'adresse IP** est définie sur **Statique**, entrez 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. Si la **source d'adresse IP** est définie sur **Statique**, entrez 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 **désactivé**, entrez l'adresse IP du premier serveur DNS.
Serveur DNS 2	Si **Serveurs DNS de DHCP** est **désactivé**, entrez l'adresse IP du deuxième serveur DNS.
Paramètres IPv6	Activez ou désactivez la prise en charge de la connexion IPv6.
Source d'adresse IP	Choisissez entre **AutoConfig** et **Statique**. Lorsque **AutoConfig** est sélectionné, les champs **Adresse 1 IPv6**, **Longueur du préfixe** et **Passerelle par défaut** sont obtenus auprès de DHCP. Lorsque **Statique** est sélectionné, les éléments **Adresse 1 IPv6**, **Longueur du préfixe** et **Passerelle par défaut** deviennent modifiables.
Adresse 1 IPv6	Si la **source d'adresse IP** est définie sur **DHCP**, ce champ affiche l'adresse IP obtenue auprès de DHCP. Si la **source d'adresse IP** est définie sur **Statique**, entrez 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 **AutoConfi**g, ce champ affiche l'adresse IP de la passerelle par défaut obtenue auprès de DHCP. Si la **source d'adresse IP** est définie sur **Statique**, entrez l'adresse IP de la passerelle par défaut.
Adresse locale du lien IPv6	Il s'agit de l'**adresse locale du lien IPv6** non modifiable de l'interface réseau iDRAC.
Adresse 2 IPv6	Il s'agit de l'**adresse 2 IPv6** non modifiable de l'interface réseau iDRAC.
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 **désactivé**, entrez l'adresse IP du premier serveur DNS.
Serveur DNS 2	Si **Serveurs DNS de DHCP** est **désactivé**, entrez l'adresse IP du premier serveur DNS.
Configurations LAN avancées	
Négociation automatique	Si **Sélection NIC** est **Dédiée**, choisissez entre **Activé** et **Désactivé**. 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 **Désactivée**, choisissez entre 10 Mbits/s et 100 Mbits/s.
Paramètre de duplex du LAN	Si **Négociation automatique** est **Désactivée**, choisissez entre **Semi-duplex** et **Duplex intégral**.

Configuration du média virtuel

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 **redirection de console**.

Si vous sélectionnez **Déconnecté**, les utilisateurs ne peuvent pas accéder aux périphériques de média virtuel lors des sessions de **redirection de console**.

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.

Disque flash virtuel

Appuyez sur <Entrée> pour sélectionner **Désactivé** ou **Activé**.

La **désactivation/activation** entraîne une **Déconnexion** et une **Connexion** de tous les périphériques Média virtuel du bus USB.

La **désactivation** entraîne la suppression du disque flash virtuel et le rend non disponible à l'utilisation.

REMARQUE : Ce champ est en lecture seule si une carte SD de plus de 256 Mo n'est pas présente dans le logement de carte iDRAC6 Express.

Ouvrir une session avec une 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**, **IPMI sur LAN** est désactivé et ne peut pas être modifié.

Configuration des services du système

System Services (Services du système)

Appuyez sur <Entrée> pour sélectionner **Activé** ou **Désactivé**. Consultez le *Guide de l'utilisateur d'Unified Server Configurator* disponible sur le site Web de support de Dell à l'adresse **support.dell.com\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.

Annuler les services système

Appuyez sur <Entrée> pour sélectionner **Non** ou **Oui**.

Lorsque vous sélectionnez **Oui**, toutes les sessions de Unified Server Configurator sont fermées, et le serveur redémarre lorsque vous utilisez **Enregistrer** et **Quitter** pour appliquer les nouveaux paramètres.

Configuration de l'écran LCD

Appuyez sur <Entrée> pour afficher le sous-menu **Configuration LCD**. Une fois la configuration des paramètres LCD terminée, appuyez sur <Échap> pour revenir au menu précédent.

Tableau 18-2. Configuration utilisateur LCD

Ligne 1 LCD	Appuyez sur la <flèche droite>, la <flèche gauche> et la barre d'espace pour basculer d'une option à l'autre. Cette option définit l'affichage de l'**Écran d'accueil** sur l'écran LCD suivant l'une des options suivantes : **Temp ambiante, Numéro d'inventaire**, **Nom de l'hôte**, **Adresse IPv4 d'iDRAC6**, **Adresse IPv6 d'iDRAC6**, **Adresse MAC d'iDRAC6**, **Numéro de modèle**, **Aucun**, **Numéro de service**, **Alimentation système**, **Chaîne définie par l'utilisateur**.
Chaîne définie par l'utilisateur de l'écran?LCD	Si **Ligne 1 LCD** est une **Chaîne définie par l'utilisateu**r, visualisez ou entrez la chaîne devant s'afficher sur l'écran LCD. La chaîne ne peut comporter que 62 caractères au maximum.
Blocs d'alimentation du système LCD	Si **Ligne 1 LCD** est définie comme **Alimentation système**, sélectionnez **Watt** ou **BTU/hr** pour spécifier l'unité à afficher sur l'écran LCD.
Unités de temp. ambiante de l'écran LCD	Si **Ligne 1 LCD** est définie comme **Température ambiante**, 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 évènements système). Cette fonctionnalité permet l'affichage des messages d'erreur sur l'écran LCD dans l'un des deux formats : Le format Simple consiste en une description, en anglais, de l'évènement. Avec le format SEL, c'est une chaîne du journal des évènements système qui s'affiche
Indication KVM distant de l'écran LCD	Sélectionnez **Activé** pour afficher le texte *KVM* à chaque fois qu'un KVM virtuel est actif sur l'unité.
Accès au panneau avant de l'écran LCD	Appuyez sur la <flèche droite>, la <flèche gauche > et la barre d'espace pour passer d'une option à l'autre : **Désactivé**, **Affichage/Modification** et **Affichage uniquement**. Ce paramétrage permet de définir le niveau d'accès utilisateur pour l'écran LCD.

Configuration utilisateur LAN

L'utilisateur LAN est le compte administrateur iDRAC, soit **root** par défaut. Appuyez sur <Entrée> pour afficher le sous-menu Configuration utilisateur LAN. Une fois la configuration de l'utilisateur LAN terminée, appuyez sur <Échap> pour revenir au menu précédent.

Tableau 18-3. Configuration utilisateur LAN

Élément	Description
Accès au compte	Sélectionnez **Activé** pour activer le compte administrateur. Sélectionnez **Désactivé** pour désactiver le compte administrateur.
Privilèges de compte	Choisissez entre **Administrateur**, **Utilisateur**, **Opérateur** et **Aucun accès**.
Nom d'utilisateur de 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**.
Entrer 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.
Confirmer le mot de passe	Retapez le nouveau mot de passe du compte administrateur. Si les caractères que vous avez entrés ne correspondent pas à ceux que vous avez tapés dans le champ **Entrer le mot de passe**, un message s'affiche et vous devez entrer à nouveau le mot de passe.

Rétablir les paramètres par défaut

Utilisez l'élément de menu **Rétablir les paramètres par défaut** pour rétablir 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 :

```
Resetting to factory defaults will restore remote Non-Volatile user settings. Continue?

< NO (Cancel) >

< YES (Continue) >

(Le rétablissement des paramètres d'usine va restaurer les paramètres utilisateur non volatiles. Continuer ?

< NON (Annuler) >

< OUI (Continuer) >)
```

Sélectionnez **OUI** et appuyez sur <Entrée> pour rétablir les paramètres par défaut d'iDRAC.

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 gauche> pour accéder au message précédent (plus ancien) et la <flèche droite> pour accéder au message suivant (plus récent). Entrez un nombre d'enregistrement pour atteindre cet enregistrement. Appuyez sur <Échap> lorsque vous avez fini d'afficher les messages du journal SEL.

Pour effacer les messages du 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 iDRAC

Lorsque vous avez fini d'apporter des modifications à la configuration iDRAC, appuyez sur la touche <Échap> pour afficher le menu Quitter.

Sélectionnez **Enregistrer les modifications et quitter** et appuyez sur <Entrée> pour conserver vos modifications.

Sélectionnez **Ignorer les modifications et quitter** et appuyez sur <Entrée> pour ignorer les modifications que vous avez apportées.

Sélectionnez **Retour au programme d'installation** et appuyez sur <Entrée> pour revenir dans l'utilitaire de configuration iDRAC.

Retour á la page du sommaire

Retour á la page du sommaire

Surveillance et gestion des alertes.

Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.1

Cette section explique comment surveiller l'iDRAC6 et les procédures pour configurer votre système et l'iDRAC6 pour recevoir des alertes.

Configuration du système géré pour la saisie de l'écran de la dernière panne

Pour que l'iDRAC6 puisse saisir l'écran de la dernière panne, 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 Managed System, consultez 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 de la dernière panne (désactivé par défaut).

   Pour activer l'écran de la dernière panne 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 de la dernière panne soit saisi, l'horloge de **récupération automatique** doit être définie sur 60 secondes ou plus. Le paramètre par défaut est 480 secondes.

   L'écran de la dernière panne 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 d'écran de la dernière panne de l'interface Web de l'iDRAC6 soit opérationnelle, vous devez désactiver l'option **Redémarrage automatique** sur les systèmes gérés qui utilisent 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 **Avancé**.

4. Sous **Démarrage et récupération**, cliquez sur **Paramètres**.

5. Décochez la case **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 **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 plate-forme

La configuration des événements sur plate-forme offre un outil de configuration du périphérique d'accès distant 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 plate-forme [PET] et/ou e-mail).

Les événements sur plate-forme pouvant être filtrés incluent :

- Filtre Assertion Ventilateur critique
- Filtre Assertion Avertissement concernant la batterie
- Filtre Assertion Batterie critique
- Filtre Assertion Tension discrète critique
- Filtre Assertion Avertissement concernant la température
- Filtre Assertion Température critique
- Filtre Assertion Intrusion critique
- Filtre Dégradation de la redondance
- Filtre Perte de la redondance
- Filtre Assertion Avertissement concernant un processeur
- Filtre Assertion Processeur critique
- Filtre Processeur absent
- Filtre Assertion Avertissement concernant le bloc d'alimentation du processeur
- Filtre Assertion Avertissement concernant le bloc d'alimentation du processeur critique
- Filtre Assertion Avertissement concernant le bloc d'alimentation du processeur absent
- Filtre Assertion Journal des événements critique
- Filtre Assertion Surveillance critique
- Filtre Assertion Avertissement concernant le bloc d'alimentation système
- Filtre Assertion Bloc d'alimentation système critique

Lorsqu'un événement sur plate-forme se produit (par exemple, une panne de capteur de ventilateur), un événement système est généré et enregistré dans le journal des événements système (SEL). Si cet événement correspond à un filtre d'événement sur plate-forme (PEF) dans la liste des filtres d'événements sur plate-forme dans l'interface Web et que vous avez configuré ce filtre pour générer une alerte (PET ou e-mail), une alerte PET ou e-mail est alors envoyée à une ou plusieurs destinations configurées.

Si le même filtre d'événement sur plate-forme est aussi configuré pour effectuer une action (tel qu'un redémarrage du système), l'action est effectuée.

Configuration des filtres d'événements sur plate-forme (PEF)

Configurez vos filtres d'événements sur plate-forme avant de configurer les interruptions d'événement sur plate-forme ou les paramètres d'alerte par e-mail.

Configuration du PEF à l'aide de l'interface Web

Pour des informations détaillées, voir « Configuration des filtres d'événements sur plate-forme (PEF) ».

Configuration du PEF à l'aide de la CLI RACADM

1. Activez le 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 19. La sélection activer/désactiver peut être définie sur 1 (Activé) ou 0 (Désactivé).

   Par exemple, pour activer le 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 activer le PEF pour 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 du PET à l'aide de l'interface utilisateur Web

Pour des informations détaillées, voir « Configuration des interruptions d'événement sur plate-forme (PET) ».

Configuration du 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 le 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 le 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 de destination du système qui reçoit les alertes d'événement sur plate-forme.

4. Configurez la chaîne Nom de communauté.

   À l'invite de commandes, 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 ».

Configuration d'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 plate-forme.

   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 par e-mail et *<message_personnalisé>* est le message affiché dans l'alerte par e-mail.

Test des alertes par e-mail

La fonctionnalité d'alerte 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 d'alerte 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 d'alerte par e-mail. Pour plus d'informations, voir « Configuration des alertes par e-mail ».

Test de la fonctionnalité d'alerte par interruption SNMP du RAC

La fonctionnalité d'alerte par interruption SNMP du RAC permet aux configurations d'écoute 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 d'alerte par interruption SNMP du RAC.

```
racadm testtrap -i 2
```

Avant de tester la fonctionnalité d'alerte par interruption SNMP du RAC, assurez-vous que les paramètres SNMP et d'interruption sont configurés correctement. Voir les descriptions des sous-commandes « testtrap » et « sslkeyupload » pour configurer ces paramètres.

Questions fréquemment posées concernant l'authentification SNMP

Explication de l'affichage du message suivant :

`Remote Access: SNMP Authentication Failure (Accès distant : Échec d'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 de définition, l'agent iDRAC6 génère une erreur d'authentification SNMP car il accepte uniquement les requêtes de la **communauté = public**.

REMARQUE : Ce nom est celui de la communauté de l'agent SNMP utilisé pour la découverte.

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 afficher le nom de communauté iDRAC6, utilisez la commande suivante :

```
racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <nom de communauté>
```

Pour accéder/configurer le nom de communauté iDRAC6 de l'agent SNMP à l'aide de l'interface Web, accédez à **Accès à distance**→ **Configuration**→ **Services** et cliquez sur **Agent SNMP**.

Pour éviter de générer des erreurs d'authentification SNMP, vous devez saisir des noms de communauté qui sont acceptés par l'agent. Comme l'iDRAC6 n'accepte qu'un nom de communauté, vous devez utiliser le même nom de communauté **Get** et **Set** pour configurer les découvertes sous IT Assistant.

Retour á la page du sommaire

Retour á la page du sommaire

Récupération et dépannage du système géré

Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.1

Cette section explique comment utiliser l'interface Web de l'iDRAC6 pour effectuer les tâches de récupération et de dépannage d'un système distant en panne.

- « Premières étapes de dépannage d'un système distant »
- « Gestion de l'alimentation d'un système distant »
- « Informations sur IPv6 »
- « Affichage de l'écran de la dernière panne système »

Premières étapes de dépannage d'un système distant

Les questions suivantes aident souvent à dépanner les problèmes de haut niveau du 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, consultez l'écran de la dernière panne (voir « Affichage de l'écran de la dernière panne système ») et utilisez la redirection de console et la gestion de l'alimentation à distance (voir « Gestion de l'alimentation d'un système distant ») pour redémarrer le système et observer le processus de redémarrage.

Gestion de l'alimentation d'un système distant

L'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, consultez « Exécution de tâches de contrôle de l'alimentation sur le serveur ».

Sélection d'actions de contrôle de l'alimentation depuis la CLI de l'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 sur le système

La page **Résumé du système** affiche des informations sur les composants système suivants :

- Châssis principal du système
- Integrated Dell Remote Access Controller 6 - Entreprise

Pour accéder aux informations système, développez l'arborescence **Système** et cliquez sur **Propriétés**.

Châssis principal du système

Le Tableau 20-1 et le Tableau 20-2 décrivent les principales propriétés du châssis du système.

REMARQUE : Pour recevoir les informations sur le **nom d'hôte** et le **nom du système d'exploitation**, les services iDRAC6 doivent être installés sur le système géré.

Tableau 20-1. Champs Informations système

Champ	Description
Description	Description du système.
Version du BIOS	Version du BIOS du système.
Numéro de service	Numéro de service du système.
Nom de l'hôte	Nom du système hôte.
Nom du système d'exploitation	Système d'exploitation fonctionnant sur le système.

Tableau 20-2. Champs Récupération automatique

Champ	Description
Action de récupération	Lorsqu'un blocage système est détecté, l'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 arrêt imprévu du système, avant que l'iDRAC6 n'effectue une action de récupération.
Compte à rebours actuel	Valeur actuelle, en secondes, du compte à rebours.

Integrated Dell Remote Access Controller 6 Enterprise

Le Tableau 20-3 décrit les propriétés d'iDRAC6 Enterprise.

Tableau 20-3. Options des champs iDRAC6 Enterprise

Champ	Description
Date/Heure	Heure courante au format : Jour Mois JJ HH:MM:SS:AAAA
Version du micrologiciel	Version du micrologiciel iDRAC
Mise à jour du micrologiciel	Date de dernier flashage du micrologiciel au format : Jour Mois JJ HH:MM:SS:AAAA
Version du matériel	Version du contrôleur d'accès distant.
MAC Address (Adresse Mac)	Adresse de contrôle d'accès aux médias (MAC) qui identifie de manière unique chaque nud d'un réseau.

Informations sur IPv4

Le Tableau 20-4 décrit les propriétés IPv4.

Tableau 20-4. Champs d'informations IPv4

Champ	Description
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	Masque de sous-réseau qui 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.
Passerelle	Adresse d'un routeur ou d'un commutateur. La valeur est affichée au format séparé par des points, par exemple 143.166.154.1.
Protocole DHCP activé	Oui ou Non. Indique si le protocole de configuration dynamique d'hôte (DHCP) est activé.

Informations sur IPv6

Le Tableau 20-5 décrit les propriétés IPv6.

Tableau 20-5. Champs d'informations IPv6

Champ	Description
Activé	Indique si la pile Ipv6 est activée.
Adresse IP 1	Spécifie l'adresse IPv6 du NIC d'iDRAC6.
Longueur du préfixe	Une valeur entière spécifiant la longueur du préfixe de l'adresse IPv6. Il peut s'agir de toute valeur comprise entre 1 et 128.
Passerelle IP	Spécifie la passerelle du NIC d'iDRAC6.
Adresse locale du lien	Spécifie l'adresse IPv6 du NIC d'iDRAC6.
Adresse IP 2	Spécifie l'adresse IPv6 supplémentaire du NIC d'iDRAC6 en cas de disponibilité.
Auto Config	AutoConfig permet à Server Administrator d'obtenir l'adresse IPv6 du NIC iDRAC à partir du serveur DHCPv6 (Dynamic Host Configuration Protocol). En outre, il désactive et vide les valeurs d'adresse IP statique, de longueur de préfixe et de passerelle statique.

Utilisation du journal des événements système (SEL)

La page **Journal SEL** affiche les événements critiques qui se produisent sur le système géré.

Pour afficher le journal des événements système :

1. Dans l'arborescence **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 20-6.
3. Cliquez sur le bouton approprié de la page **Journal des événements système** pour continuer (voir le Tableau 20-6).

Tableau 20-6. Icônes indicatrices de condition

Icône/Catégorie	Description
	Une coche verte indique une condition saine (normale).
	Un triangle jaune autour d'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 l'état est inconnu.
Date/Heure	La date et l'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 mm/jj/aaaa hh:mm:ss, basé sur une horloge de 24 heures.
Description	Une brève description de l'événement

Tableau 20-7. Boutons de la page SEL

Bouton	Action
Imprimer	Imprime le journal **SEL dans l'ordre de tri qui apparaît dans la fenêtre.**
Actualiser	Recharge la page du **journal SEL**.
Effacer le journal	Efface le **journal SEL**. **REMARQUE :** Le bouton **Effacer le journal** n'apparaît que si vous disposez du droit **Effacer les journaux**.

Enregistrer sous	Ouvre une fenêtre contextuelle qui vous permet d'enregistrer le **journal SEL** dans le répertoire de votre choix. **REMARQUE :** Si vous utilisez Internet Explorer et rencontrez un problème lors de l'enregistrement, téléchargez Cumulative Security Update for Internet Explorer à partir du site Web de support de Microsoft à l'adresse support.microsoft.com.

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, tout le journal est affiché.

REMARQUE : Voir « getsel » pour plus d'informations sur les options que vous pouvez utiliser.

La commande **clrsel** supprime tous les enregistrements existants du journal SEL.

```
racadm clrsel
```

Utilisation des journaux POST et de démarrage

REMARQUE : Tous les journaux iDRAC6 sont effacés après le redémarrage de l'iDRAC6.

Cette fonction de l'iDRAC6 vous permet de lire une vidéo image par image des trois dernières occurrences de démarrage POST BIOS.

Pour afficher les journaux de capture de démarrage POST :

1. Dans l'arborescence **Système**, cliquez sur **Système**.
2. Cliquez sur l'onglet **Journaux**, puis sur l'onglet **saisie DÉMARRAGE.**
3. Sélectionnez le numéro du journal de capture de démarrage et cliquez sur **Lire**.

   La vidéo des journaux est lue sur un nouvel écran.

   REMARQUE : Vous devez fermer une vidéo de journal de capture de démarrage POST 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 de démarrage POST.
5. Cliquez sur **STOP** pour arrêter la vidéo.

La carte Express iDRAC6 est liée à l'iDRAC6 lorsque vous entrez dans l'application Unified Server Configurator (USC) en appuyant sur **F10** au cours de l'amorçage. Si la liaison réussit, le message suivant est consigné dans le journal SEL et LCD : `iDRAC6 Upgrade Successful (Mise à niveau d'iDRAC6 réussie)`. Si la liaison échoue, le message suivant est consigné dans le journal SEL et LCD : (`Échec de mise à niveau d'iDRAC6)`. En outre, lorsqu'une carte iDRAC6 Express contenant un micrologiciel iDRAC6 ancien ou obsolète ne prenant pas en charge la plate-forme spécifique est insérée dans la carte mère et que le système a été amorcé, un journal est généré sur l'écran POST : `iDRAC firmware is out-of-date. Please update to the latest firmware (Le micrologiciel iDRAC est obsolète. Veuillez installer la version la plus récente du micrologiciel.`) Mettez à jour la carte iDRAC6 Express avec le dernier micrologiciel iDRAC6 pour la plate-forme spécifique. Pour plus d'informations, consultez le Guide d'utilisation *Dell Unified Server Configurator et Dell Unified Server Configurator–Contrôleur du cycle de vie activé*.

Affichage de l'écran de la dernière panne système

REMARQUE : La fonctionnalité d'écran de la dernière panne 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 de l'iDRAC6. Accédez à la page **Services** dans l'onglet **Configuration** de la section **Accès à distance** pour activer cette fonctionnalité.

La page **Écran de la dernière panne** affiche l'écran de la dernière panne. Les informations sur la dernière panne système sont enregistrées dans la mémoire de l'iDRAC6 et sont accessibles à distance.

Pour afficher la page **Écran de la dernière panne** :

1. Dans l'arborescence **Système**, cliquez sur **Système**.
2. Cliquez sur l'onglet **Journaux** puis sur **Dernière panne**.

La page **Écran de la dernière panne** est dotée des boutons suivants (voir le Tableau 20-8) en haut à droite de l'écran :

Tableau 20-8. Boutons de la page Écran de la dernière panne

Bouton	Action
Imprimer	Imprime la page **Écran de la dernière panne**.
Actualiser	Recharge la page **Écran de la dernière panne**.

REMARQUE : En raison des fluctuations dans l'horloge de récupération automatique, l'**écran de la dernière panne** peut ne pas être capturé 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 ou plus et vous assurer que l'**écran de la dernière panne** fonctionne correctement. Pour plus d'informations, voir « Configuration du système géré pour la saisie de l'écran de la dernière panne ».

Retour á la page du sommaire

Retour á la page du sommaire

Récupération et dépannage de l'iDRAC6

Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.1

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 diagnostic
- Journal de suivi
- racdump
- coredump

Utilisation du journal du RAC

Le **journal RAC** est un journal permanent conservé dans le micrologiciel iDRAC6. Le journal contient une liste des actions d'utilisateur (ouverture, fermeture de sessions et modifications des règles de sécurité par exemple) et des alertes envoyées par l'iDRAC6. Les entrées les plus anciennes sont écrasées quand le journal est plein.

Pour accéder au journal du RAC depuis l'interface utilisateur (UI) de l'iDRAC6 :

1. Dans l'arborescence du **système**, cliquez sur **Accès distant**.
2. Cliquez sur l'onglet **Journaux**, puis sur **Journal du RAC**.

Le **journal du RAC** contient les informations répertoriées dans le Tableau 21-1.

Tableau 21-1. Informations sur la page Journal du RAC

Champ	Description
Date/Heure	Date et heure (par exemple, 19 Déc 16:55:47). Lorsque l'iDRAC6 démarre à l'initiale et qu'il ne parvient pas à communiquer avec le système géré, l'heure est affichée comme System Boot (Démarrage du système).
Source	Interface qui a provoqué l'événement.
Description	Description brève de l'événement et nom d'utilisateur qui s'est connecté à l'iDRAC6.

Utilisation des boutons de la page Journal du RAC

La page **Journal du RAC** contient les boutons répertoriés dans le Tableau 21-2.

Tableau 21-2. Boutons de la page Journal du RAC

Bouton	Action
Imprimer	Imprime la page **Journal du RAC**.
Effacer le journal	Efface les entrées du **journal du RAC**. **REMARQUE :** Le bouton **Effacer le journal** n'apparaît que si vous disposez du droit **Effacer les journaux**.
Enregistrer sous	Ouvre une fenêtre contextuelle qui vous permet d'enregistrer le **journal du RAC** dans le répertoire de votre choix. **REMARQUE :** Si vous utilisez Internet Explorer et rencontrez un problème lors de l'enregistrement, téléchargez Cumulative Security Update for Internet Explorer à partir du site Web de support de Microsoft à l'adresse **support.microsoft.com**.

Actualiser	Recharge la page **Journal du RAC**.

Utilisation de la ligne de commande

Utilisez la commande `getraclog` pour afficher les entrées du journal du RAC.

```
racadm getraclog -i
```

La commande **getraclog -i** affiche le nombre d'entrées du journal iDRAC6.

```
racadm getraclog [options]
```

REMARQUE : Pour plus d'informations, voir « getraclog ».

Vous pouvez utiliser la commande `clrraclog` pour effacer toutes les entrées du journal du RAC.

```
racadm clrraclog
```

Utilisation de la console de diagnostic

L'iDRAC6 fournit un ensemble standard d'outils de diagnostic réseau (voir Tableau 21-3) qui sont 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.

Pour accéder à la page **Console de diagnostic** :

1. Dans l'arborescence du **système**, cliquez sur **Accès distant**.
2. Cliquez sur l'onglet **Diagnostics**.

Le Tableau 21-3 décrit les options disponibles sur la page **Console de diagnostic**. Tapez une commande et cliquez sur **Envoyer**. Les résultats du débogage apparaissent sur la page **Console de diagnostic**.

Pour actualiser la page **Console de diagnostic**, cliquez sur **Actualiser**. Pour exécuter une autre commande, cliquez sur **Retour à la page Diagnostics**.

Tableau 21-3. 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 facultatif de l'interface est indiqué dans la zone 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 de l'iDRAC6 avec le contenu actuel du tableau de routage. Il faut saisir une adresse IP de destination 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 de l'iDRAC6. Pour plus d'informations, voir « gettracelog ».

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 de l'iDRAC6.

Pour accéder au journal de suivi depuis l'interface Web de l'iDRAC6 :

1. Dans l'arborescence du **système**, cliquez sur **Accès distant**.
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 plus d'informations, consultez la section « gettracelog ».

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 : L'iDRAC6 ne renvoie pas d'ICMP (ping) si la taille du paquet dépasse 1 500 octets.

Utilisation de la commande racdump

La commande **racadm racdump** fournit une commande unique pour obtenir des informations sur le vidage et l'état ainsi que des informations générales sur la carte de l'iDRAC6.

REMARQUE : Cette commande est disponible uniquement sur les interfaces Telnet et SSH. Pour plus d'informations, voir la commande « racdump ».

Utilisation de la commande 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-là, les informations coredump portent sur la dernière erreur critique qui s'est produite.

La commande racadm c**oredumpdelete** peut être utilisée pour effacer toutes les données coredump actuellement stockées dans le RAC.

Voir les sous-commandes « coredump » et « coredumpdelete » pour plus d'informations.

Retour á la page du sommaire

Retour á la page du sommaire

Capteurs

Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.1

Les capteurs et sondes de matériel vous aident à surveiller les systèmes sur votre réseau plus efficacement en vous permettant de prendre des mesures appropriées pour prévenir les sinistres, tels que les dommages ou problèmes de stabilité du système.

Vous pouvez utiliser l'iDRAC6 pour surveiller le capteur de matériel pour les batteries, les sondes de ventilateurs, l'intrusion dans le châssis, les blocs d'alimentation, l'alimentation consommée, la température et les tensions.

Sondes de batterie

Les sondes de batterie donnent des informations concernant les batteries de CMOS de la carte système et de la mémoire vive de stockage sur la carte mère (ROMB).

REMARQUE : Les paramètres de la batterie ROMB de stockage sont disponibles uniquement si le système dispose d'un ROMB.

Sondes de ventilateur

Le capteur de la sonde du ventilateur donne des informations concernant :

- redondance du ventilateur : la capacité du ventilateur secondaire de remplacer le ventilateur primaire si celui-ci n'arrive pas à dissiper la chaleur à une vitesse prédéfinie.
- liste de la sonde du ventilateur : fournit des informations concernant la vitesse de ventilation pour tous les ventilateurs du système.

Sondes d'intrusion dans le châssis

Les sondes d'intrusion dans le châssis indiquent la condition du châssis, qu'il soit ouvert ou fermé.

Sondes des blocs d'alimentation

Les sondes des blocs d'alimentation fournissent des informations concernant :

- 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 **Désactivée**.

Sondes de surveillance de l'alimentation

Le contrôle de l'alimentation donne des informations concernant la consommation d'alimentation en *temps réel*, en watts et 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 l'iDRAC6.

Sonde de température

Le capteur de température donne des informations concernant la température ambiante de la carte système. La sonde de température indique si la condition de la sonde entre dans la valeur prédéfinie de seuil critique et d'avertissement.

Sondes de tension

Les sondes de tension types sont les suivantes. Votre système est peut-être dotés de celles-ci et/ou d'autres.

- UCT [n] VCORE
- Carte système 0.9V PG
- Carte système 1,5V ESB2 PG
- Carte système 1,5V PG
- Carte système 1,8V PG
- Carte système 3,3V PG
- Carte système 1,5V PG
- Fond de panier carte système PG
- Carte système UCT VTT
- Carte système linéaire PG

Les sondes de températures indiquent si la condition des sondes entre dans la valeur prédéfinie de seuil critique d'avertissement.

Retour á la page du sommaire

Retour á la page du sommaire

Configuration des fonctionnalités de sécurité

Guide d'utilisation d'Integrated Dell™ Remote Access Controller 6 (iDRAC6), version 1.1

L'iDRAC6 dispose des fonctionnalités de sécurité suivantes :

- Options Sécurité avancée pour l'administrateur d'iDRAC6 :
  - L'option de désactivation de la redirection de console permet à l'utilisateur du système *local* de désactiver la redirection de console à l'aide de la fonctionnalité Redirection de console 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) avec 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 accrue.
- 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 l'iDRAC6

Options Sécurité pour l'administrateur d'iDRAC6

Désactiver la configuration locale d'iDRAC6

Les administrateurs peuvent désactiver la configuration locale via l'interface utilisateur graphique (GUI) d'iDRAC6 en sélectionnant **Accès distant**→ **Configuration**→ **Services**. Lorsque la case **Désactiver la configuration locale d'iDRAC à l'aide de l'option ROM** est cochée, 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 coche la case **Désactiver la configuration locale d'iDRAC à l'aide de RACADM**, les utilisateurs locaux ne peuvent pas configurer l'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. En plus de les activer via l'interface Web, les administrateurs peuvent y parvenir à l'aide des commandes de la RACADM locale.

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 iDRAC6. Pour mettre à niveau vers cette version, mettez votre BIOS à niveau à l'aide du progiciel de mise à jour du BIOS disponible sur 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. Dell recommande d'utiliser ces fonctionnalités avec prudence et de ne désactiver qu'une seule interface à la fois pour éviter de perdre entièrement les privilèges d'ouverture de session.

REMARQUE : Consultez le livre blanc sur la *Désactivation de la configuration locale et du KVM virtuel distant dans le DRAC* sur le site de 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 localement des commandes de RACADM, ou encore un système d'exploitation à usage limité tel que Microsoft Windows® Preinstallation Environment ou vmlinux servant à exécuter localement les commandes de RACADM 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 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 d'iDRAC6 local et n'autorisent que les utilisateurs du service de répertoires Microsoft Active Directory® à ouvrir une session sur l'iDRAC6 et si l'infrastructure d'authentification d'Active Directory échoue par la suite, les administrateurs risquent de ne plus pouvoir ouvrir une session. De même, si les administrateurs ont désactivé toutes configurations locales et placent un iDRAC6 ayant une adresse IP statique sur un réseau comprenant déjà un serveur DHCP (Dynamic Host Configuration Protocol) et que ce 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 du KVM virtuel distant d'iDRAC6

Les administrateurs peuvent désactiver de manière sélective le KVM distant d'iDRAC6, offrant ainsi un mécanisme sécurisé flexible permettant à un utilisateur local de travailler sur le système sans qu'un tiers ne voit les actions de l'utilisateur par le biais de la redirection de console. L'utilisation de cette fonctionnalité nécessite l'installation du logiciel Managed node d'iDRAC sur le serveur. Les administrateurs peuvent désactiver le vKVM distant à l'aide de la commande suivante :

```
racadm LocalConRedirDisable 1
```

La commande LocalConRedirDisable désactive les fenêtres de la session vKVM distante 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 le vKVM distant. Ils peuvent le faire en utilisant l'argument 0 :

```
racadm LocalConRedirDisable 0
```

Plusieurs situations peuvent obliger à désactiver le vKVM distant d'iDRAC6. Par exemple, les administrateurs peuvent vouloir empêcher un utilisateur de l'iDRAC6 distant de voir les paramètres du BIOS qu'ils configurent sur un système. Dans ce cas, ils peuvent désactiver le vKVM distant lors du POST du système en utilisant la commande `LocalConRedirDisable`. Ils peuvent aussi vouloir renforcer la sécurité en désactivant automatiquement le vKVM distant 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 : Consultez le livre blanc sur la *Désactivation de la configuration locale et du KVM virtuel distant dans le DRAC* sur le site de 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) »
- « Requête de signature de certificat (RSC) »
- « Accès au menu principal SSL »
- « Génération d'une requête de signature de certificat »

Secure Sockets Layer (SSL)

L'iDRAC6 utilise un serveur Web, un serveur configuré pour utiliser le protocole de sécurité SSL standard de l'industrie afin de transférer des données cryptées sur Internet. Basé sur la technologie de cryptage à clé publique et à clé privée, SSL est une technique 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 de données. L'iDRAC6 applique la norme de cryptage SSL à 128 bits, la forme la plus fiable de cryptage généralement disponible pour les navigateurs Internet en Amérique du Nord.

Le serveur Web de l'iDRAC6 inclut un certificat numérique SSL Dell auto-signé (la référence serveur). Pour garantir un haut niveau de sécurité sur Internet, remplacez le certificat SSL du serveur Web en envoyant une requête à l'iDRAC6 pour générer une nouvelle requête de signature de certificat (RSC).

Requête de signature de certificat (RSC)

Une CSR est une demande numérique adressée à une autorité de certification (CA) 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, nous vous conseillons vivement de générer une CSR, de l'envoyer à une CA et de téléverser le certificat renvoyé par la CA.

Une CA est une entité commerciale reconnue en 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 de CA. Une fois que la CA a reçu votre CSR, ils examinent et vérifient les informations contenues dans la CSR. 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 la CA approuve la RSC et vous envoie le certificat, vous devez le téléverser dans le micrologiciel du contrôleur iDRAC6. Les informations de la RSC enregistrées sur le micrologiciel d'iDRAC6 doivent correspondre aux informations du certificat.

Accès au menu principal SSL

1. Développez l'arborescence du **système** et cliquez sur **Accès distant**.
2. Cliquez sur l'onglet **Configuration**, puis sur **SSL**.

Utilisez le **Menu principal SSL** (voir le Tableau 23-1) pour générer une RSC, pour téléverser un certificat de serveur existant ou pour visualiser un certificat de serveur existant. Les informations de la RSC sont stockées dans le micrologiciel iDRAC6. Le Tableau 23-2 décrit les boutons disponibles à la page **SSL**.

Tableau 23-1. Menu principal SSL

Champ	Description
Requête de signature de certificat (RSC)	Cliquez sur **Suivant** pour ouvrir la page qui permet de générer une RSC à envoyer à une autorité de certification pour demander un certificat Web sécurisé.
Téléverser le 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 l'iDRAC6. **REMARQUE :** L'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 l'iDRAC6.
Afficher le certificat de serveur	Cliquez sur **Suivant** pour afficher un certificat de serveur existant.

Tableau 23-2. Boutons du menu principal SSL

Bouton	Description
Imprimer	Imprime la page **Menu principal SSL**.
Actualiser	Recharge la page **Menu principal SSL**.
Suivant	Navigue jusqu'à la page suivante.

Génération d'une requête de signature de certificat

REMARQUE : Chaque nouvelle RSC supplante la RSC qui se trouve déjà sur le micrologiciel. Avant qu'iDRAC ne puisse accepter votre RSC signée, la RSC figurant dans le micrologiciel doit correspondre au certificat renvoyé par l'autorité de certification.

1. Sur la page **Menu principal SSL**, sélectionnez **Générer une nouvelle requête de signature de certificat (RSC)** et cliquez sur **Suivant**.
2. Sur la page **Générer une requête de signature de certificat (RSC)**, entrez une valeur pour chaque attribut RSC.

   Le Tableau 23-3 décrit les options de la page **Générer une requête de signature de certificat (CSR)**.
3. Cliquez sur **Générer** pour ouvert ou enregistrer la RSC.
4. Cliquez sur le bouton approprié de la page **Générer une requête de signature de certificat (CSR)** pour continuer. Le Tableau 23-4 décrit les boutons

disponibles dans la page **Générer une requête de signature de certificat (RSC)**.

Tableau 23-3. Options de la page Générer une requête de signature de certificat (CSR)

Champ	Description
Nom commun	Le nom exact à certifier (normalement, le nom de domaine du serveur Web, par exemple, **www.compagniexyz.com**). Seuls les caractères alphanumériques, les tirets, les traits de soulignement, les espaces et les points sont valides.
Nom de la société	Le nom associé à cette société (par exemple, Compagnie XYZ). Seuls les caractères alphanumériques, les tirets, les traits de soulignement, les points et les espaces sont valides.
Service de la société	Le nom associé au service de la société, comme un département (par exemple, Groupe de l'entreprise). Seuls les caractères alphanumériques, les tirets, les traits de soulignement, les points et les espaces sont valides.
Ville	La ville ou autre lieu où se trouve l'entité à certifier (par exemple, Round Rock). Seuls les caractères alphanumériques et les espaces sont valides. Ne séparez pas les mots par des traits de soulignement ou d'autres caractères.
Nom de l'état	L'état ou la province où se trouve l'entité qui fait la demande de certification (par exemple, Texas). Seuls les caractères alphanumériques et les espaces sont valides. N'utilisez pas d'abréviations.
Code du pays	Le nom du pays où se trouve l'entité qui fait la demande de certification. Utilisez le menu déroulant pour sélectionner le pays.
E-mail	L'adresse e-mail associée à la CSR. Vous pouvez taper l'adresse e-mail de votre compagnie ou une adresse e-mail que vous voulez associer à la CSR. Ce champ est optionnel.

Tableau 23-4. Boutons de la page Générer une requête de signature de certificat (CSR)

Bouton	Description
Imprimer	Imprime la page **Générer une requête de signature de certificat (CSR)**.
Actualiser	Recharge la page **Générer une requête de signature de certificat (RSC)**.
Retour au menu principal SSL	Retourne à la page **Menu principal SSL**.
Générer	Génère une CSR.

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 23-5 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 23-5. Informations relatives au certificat

Champ	Description
Numéro de série	Numéro de série du certificat
Informations sur le sujet	Attributs du certificat entrés par le demandeur
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 d'Active Directory, voir « Utilisation de Secure Shell (SSH) ».

Configuration des services

REMARQUE : Pour modifier ces paramètres, vous devez avoir le droit de **configurer iDRAC**. De plus, l'utilitaire de ligne de commande RACADM distant peut être activé uniquement si l'utilisateur a ouvert une session en tant que **root**.

1. Développez **l'arborescence** du système et cliquez sur **Accès distant**.

2. Cliquez sur l'onglet **Configuration**, puis sur **Services**.

3. Configurez les services suivants, si nécessaire :
   - Configuration locale (Tableau 23-6)
   - Tableau 23-7Serveur Web ()
   - SSH (Tableau 23-8)
   - Telnet (Tableau 23-9)
   - RACADM distante (Tableau 23-10)
   - Agent SNMP (Tableau 23-11)
   - Agent de récupération de système automatique (Tableau 23-12)

   Utilisez l'**agent de récupération de système automatique** pour activer la fonctionnalité **Écran de la dernière panne** 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 de la dernière panne** fonctionne dans iDRAC6.

4. Cliquez sur **Appliquer les modifications**.

5. Cliquez sur le bouton approprié de la page **Services** pour continuer. Reportez-vous au Tableau 23-13.

Tableau 23-6. 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 l'option RACADM	Désactive la configuration locale d'iDRAC à l'aide de l'option RACADM.

Tableau 23-7. Paramètres du serveur Web

Paramètre	Description
Activé	Active ou désactive Web Server. Coché = Activé ; Décoché = Désactivé.
Nombre maximal de sessions	Nombre maximal de sessions simultanées autorisées pour ce système.
Sessions actives	Nombre de sessions actuelles sur le système, inférieur ou égal au **Nombre maximal de sessions**.
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 aux paramètres du délai d'expiration prennent immédiatement effet et mettent fin à la session d'interface Web. 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 l'iDRAC pour une connexion serveur. Le paramètre par défaut est **80**.
Numéro de port HTTPS	Port utilisé par l'iDRAC pour une connexion serveur. Le paramètre par défaut est **443**.

Tableau 23-8. Paramètres SSH

Paramètre	Description
Activé	Active ou désactive SSH. Lorsqu'elle est cochée, cette case indique que SSH est activé.
Délai d'attente	Délai d'attente 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. L'adresse par défaut est **300**.
Numéro de port	Port sur lequel iDRAC6 écoute une connexion SSH. L'adresse par défaut est **22**.

Tableau 23-9. Paramètres Telnet

Paramètre	Description
Activé	Active ou désactive Telnet. Lorsqu'il est coché, Telnet est activé.
Délai d'attente	Délai d'expiration en cas d'inactivité de la commande 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. L'adresse par défaut est **300**.
Numéro de port	Port sur lequel l'iDRAC6 écoute une connexion Telnet. L'adresse par défaut est **23**.

Tableau 23-10. Paramètres RACADM distante

Paramètre	Description
Activé	Active ou désactive la RACADM distante. Lorsqu'il est coché, la RACADM distante est activée.
Sessions actives	Nombre de sessions ouvertes sur le système.
Sessions actives	Nombre de sessions actuelles sur le système, inférieur ou égal au **Nombre maximal de sessions**.

Tableau 23-11. Paramètres de l'agent SNMP

Paramètre	Description
Activé	Active ou désactive l'agent SNMP. Coché = Activé ; Décoché = Désactivé.
Nom de communauté	Nom de communauté qui contient l'adresse IP pour la destination de l'alerte SNMP. Le nom de communauté peut comporter jusqu'à 31 caractères non blancs. Le paramètre par défaut est **public**.

Tableau 23-12. Paramètre de l'agent de récupération de système automatique

Paramètre	Description
Activé	Active l'agent de récupération de système automatique.

Tableau 23-13. Boutons de la page Services

Bouton	Description
Imprimer	Imprime la page **Services**.
Actualiser	Actualise la page **Services**.
Appliquer les modifications	Applique les paramètres de la page **Services**.

Activation d'options de sécurité iDRAC6 supplémentaires

Pour empêcher tout accès non autorisé à votre système distant, l'iDRAC6 fournit les fonctionnalités suivantes :

- Filtrage des adresses IP (IPRange) : définit une plage spécifique d'adresses IP auxquelles peut accéder l'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 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 un message d'erreur.

L'ouverture de session a lieu si l'expression suivante est égale à zéro :

```
cfgRacTuneIpRangeMask & (<adresse_IP_entrante> ^ cfgRacTuneIpRangeAddr)
```

où & est l'opérateur bitwise AND des quantités et ^ est l'opérateur bitwise exclusif OR.

Voir « Définitions des groupes et des objets de la base de données des propriétés iDRAC6 » pour une liste complète des propriétés **cfgRacTune**.

Tableau 23-14. Propriétés de filtrage des adresses IP (IpRange)

Propriété	Description
cfgRacTuneIpRangeEnable	Active la fonctionnalité de contrôle de plage IP.
cfgRacTuneIpRangeAddr	Détermine le format binaire d'adresse IP accepté en fonction des 1 dans le masque de sous-réseau. Cette propriété correspond à l'opérateur bitwise 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 avec un iDRAC6. Les ouvertures de session à partir des adresses IP qui sont situées à l'extérieur de cette plage échoueront. 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 avec iDRAC6.
cfgRacTuneIpRangeMask	Définit les positions des bits de fort poids 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

Voici un exemple de commande pour la configuration du filtrage IP.

Consultez « Utilisation de la RACADM à distance » 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 ci-dessous.

```
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 ci-dessous :

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

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeAddr 192.168.0.212

racadm config -g cfgRacTuning -o cfgRacTuneIpRangeMask 252.255.255.255
```

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 empêche l'adresse de se connecter à iDRAC6 pendant une période prédéfinie.

Le paramètre de 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 on empêche l'adresse IP « coupable » d'établir une session lorsque 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 : ssh exchange identification: Connection closed by remote host (identification d'échange ssh : connexion fermée par l'hôte distant).

Voir « Définitions des groupes et des objets de la base de données des propriétés iDRAC6 » pour une liste complète des propriétés **cfgRacTune**.

Le Tableau 23-15 répertorie les paramètres définis par l'utilisateur.

Tableau 23-15. Propriétés de restriction des nouvelles tentatives d'ouverture de session

Propriété	Définition
cfgRacTuneIpBlkEnable	Active la fonctionnalité de blocage IP. Lorsque des échecs consécutifs (**cfgRacTuneIpBlkFailCount**) à partir d'une seule adresse IP sont rencontrés pendant une période de temps spécifique (**cfgRacTuneIpBlkFailWindow**), tous les essais ultérieurs d'établissement d'une session à partir de cette adresse sont rejetés pour 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 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 la GUI d'iDRAC6

REMARQUE : Vous devez disposer de la permission de **configuration iDRAC6** pour effectuer les étapes suivantes.

1. Dans l'arborescence du **système**, cliquez sur **Accès distant**.
2. Cliquez sur l'onglet **Configuration** 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 modifications**.

   Le Tableau 23-16 décrit les paramètres de la page **Sécurité réseau**.
5. Cliquez sur le bouton approprié de la page **Sécurité réseau** pour continuer. Voir Tableau 23-17 pour une description des boutons de la page **Sécurité réseau**.

Tableau 23-16. Paramètres de la page Sécurité réseau

Paramètres	Description
Plage IP activée	Active la fonctionnalité de vérification de la plage IP, qui définit une plage d'adresses IP spécifique pouvant accéder à l'iDRAC6.
Adresse de la plage IP	Détermine le format binaire d'adresse IP autorisé, en fonction des 1 dans le masque de sous-réseau. Cette valeur correspond à l'opérateur 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 avec un iDRAC6. Les ouvertures de session à partir des adresses IP qui sont situées à l'extérieur de cette plage échoueront. 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 avec iDRAC6.
Masque de sous-réseau de la plage IP	Définit les positions des bits de fort poids 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. Par exemple, **255.255.255.0.**
Blocage IP activé	Active la fonctionnalité de 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 prédéfinie.

Nombre d'échecs avant blocage IP	Définit le nombre d'échecs de tentatives d'ouverture de session à partir d'une adresse IP avant de rejeter les tentatives d'ouverture de session à partir de cette adresse.
Plage d'échecs avant blocage IP	Détermine la période en secondes pendant laquelle doivent se produire des échecs du nombre d'échecs avant blocage IP 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.

Tableau 23-17. Boutons de la page Sécurité réseau

Bouton	Description
Imprimer	Imprime la page **Sécurité réseau**
Actualiser	Recharge la page **Sécurité réseau**
Appliquer les modifications	Enregistre les modifications apportées à la page **Sécurité réseau**.
Retour à la page Configuration réseau	Retourne à la page **Configuration réseau**.

Retour á la page du sommaire