Dell™ Remote Access Controller 5 Guide d'utilisation de la version 1.45 du micrologiciel

---

Remarques et avertissements

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

PRÉCAUTION : Une PRÉCAUTION vous avertit d'un risque de dommage matériel ou de perte de données en cas de non-respect des instructions données.

Novembre 2008

Retour à la page su sommaire

Présentation de la sous-commande RACADM

Dell™ Remote Access Controller 5 Guide d'utilisation de la version 1.45 du micrologiciel

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

---

help

REMARQUE : Pour utiliser cette commande, vous devez avoir le droit **Ouvrir une session sur le DRAC 5**.

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**.

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**.

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 avoir le droit **Ouvrir une session sur le DRAC 5**.

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

Tableau A-4. config/getconfig

Sous-commande	Définition
config	Configure le DRAC 5.
getconfig	Récupère les données de configuration du DRAC 5.

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 du DRAC 5 individuellement ou de les regrouper dans un fichier de configuration. Si les données sont différentes, l'objet DRAC 5 est réécrit avec la nouvelle valeur.

Entrée

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>** indique à **config** de lire le contenu du fichier indiqué par le **<nom de fichier>** et de configurer le DRAC 5. 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 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'écriture sur le DRAC 5. Cette option sert uniquement de vérification.

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 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 le DRAC 5. 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 désirez 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 du DRAC 5 un par un ou d'extraire et d'enregistrer dans un fichier l'ensemble des groupes de configuration du RAC.

Entrée

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 du RAC 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.cf**g. 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 valde 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 par la valeur de l'index, et 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 la CLI 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 du RAC sur **myrac.cfg**.

- `racadm getconfig -h`

  Affiche la liste des groupes de configuration disponibles sur le DRAC 5.

- `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**.

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

Tableau A-7. coredump

Sous-commande	Définition
coredump	Affiche le dernier vidage de mémoire du DRAC 5.

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 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.

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**.

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

Tableau A-8. coredumpdelete

Sous-commande	Définition
coredumpdelete	Supprime le vidage de mémoire stocké sur le DRAC 5.

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 avoir le droit **Configurer le DRAC 5**.

REMARQUE : Avant de commencer la mise à jour de votre micrologiciel, voir « Connexion au système géré via le port série local ou une station de gestion Telnet (système client) » pour des instructions supplémentaires.

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

Tableau A-9. fwupdate

Sous-commande	Définition
fwupdate	Met le micrologiciel du DRAC 5 à jour.

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>
```

Description

La sous-commande **fwupdate** permet aux utilisateurs de mettre à jour le micrologiciel du DRAC 5. L'utilisateur peut :

- Vérifier l'état du processus de mise à jour du micrologiciel
- Mettre à jour le micrologiciel du DRAC 5 à partir d'un serveur TFTP en fournissant une adresse IP et un chemin d'accès optionnel
- Mettre à jour le micrologiciel du DRAC 5 à partir du système de fichiers local à l'aide de la RACADM locale

Interfaces prises en charge

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

Entrée

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.

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, le DRAC 5 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 du DRAC 5.
-p	L'option **-p**, ou **put**, est utilisée pour mettre à jour le fichier de micrologiciel du système géré vers le DRAC 5. L'option **-u** doit être utilisée avec l'option **-p**.

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, le DRAC 5 est réinitialisé.

  Si le téléchargement excède 15 minutes et expire, transférez l'image flash du micrologiciel sur un lecteur local du serveur. Puis, à l'aide de la redirection de console, connectez-vous au système distant et installez localement le micrologiciel en utilisant la racadm locale.

- `racadm fwupdate -s`

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

- `racadm fwupdate -p -u -d c:\ <images>`

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

- `racadm -r 192.168.0.120 -u root -p racpassword fwupdate -g -u -a 192.168.0.120 -d <images>`

  Dans cet exemple, la RACADM est utilisée pour mettre à jour à distance le micrologiciel d'un DRAC spécifique à l'aide du nom d'utilisateur et du mot de passe DRAC fournis. L'image est récupérée depuis un serveur TFTP.

REMARQUE : L'option **-p** n'est pas prise en charge dans l'interface RACADM distante pour la sous-commande fwupdate.

---

getssninfo

REMARQUE : Pour utiliser cette commande, vous devez avoir le droit **Ouvrir une session sur le DRAC 5**.

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 qui sont connectés au DRAC. 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

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"

- racadm getssninfo -A -u *

  "root" "143.166.174.19" "Telnet" "NONE"

  "bob" "143.166.174.19" "GUI" "NONE"

getsysinfo

REMARQUE : Pour utiliser cette commande, vous devez avoir le droit **Ouvrir une session sur le DRAC 5**.

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

Tableau A-14. getsysinfo

Commande	Définition
getsysinfo	Affiche des informations sur le DRAC 5, le système et l'état de la surveillance.

Synopsis

```
racadm getsysinfo [-d] [-s] [-w] [-A]
```

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

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

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

Option	Description
-d	Affiche les Informations sur le DRAC 5.
-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            = Thu Dec 8 20:01:33 2005
Firmware Version         = 1.0
Firmware Build           = 05.12.08
Last Firmware Update     = Thu Dec 8 08:09:36 2005

Hardware Version         = A00
Current IP Address       = 192.168.0.120
Current IP Gateway       = 192.168.0.1
Current IP Netmask       = 255.255.255.0
DHCP Enabled             = 0
MAC Address              = 00:14:22:18:cd:f9
Current DNS Server 1     = 0.0.0.0
```

```
Current DNS Server 2     = 0.0.0.0
DNS Servers from DHCP    = 0
Register DNS RAC Name    = 0
DNS RAC Name             = rac-48192
Current DNS Domain       =

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
```

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 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 avoir le droit **Ouvrir une session sur le DRAC 5**.

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 avoir le droit **Exécuter des commandes de diagnostic** ou **Configurer le DRAC 5**.

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**.

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 avoir le droit **Exécuter des commandes de diagnostic** ou **Configurer le DRAC 5**.

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

Tableau A-19. ping

Sous-commande	Définition
ping	Vérifie qu'il est possible d'atteindre l'adresse IP de destination à partir du DRAC 5 avec le contenu actuel de la table 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 la commande **setniccfg**, vous devez avoir le droit **Configurer le DRAC 5**.

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 -s [<adresse IP> <masque de réseau> <passerelle>]

racadm setniccfg -o [<adresse IP> <masque de réseau> <passerelle>]
```

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 activé).
- L'option **-s** active les paramètres IP statiques. L'adresse IP, le masque de réseau et la passerelle peuvent être spécifiés. Sinon, les paramètres statiques existants sont utilisés. <*adresse IP*>, <*masque de réseau*> et <*passerelle*> doivent être entrés comme des chaînes de caractères séparées par des points.

  ```
  racadm setniccfg -s 192.168.0.120 255.255.255.0 192.168.0.1
  ```

- L'option **-o** désactive le port de gestion Ethernet complètement. <*adresse IP*>, <*masque de réseau*> et <*passerelle*> doivent être entrés comme des chaînes de caractères séparées par des points.

  ```
  racadm setniccfg -o 192.168.0.120 255.255.255.0 192.168.0.1
  ```

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 la commande **getniccfg**, vous devez avoir le droit **Ouvrir une session sur le DRAC 5**.

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, la sortie est affichée 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 avoir le droit **Ouvrir une session sur le DRAC 5**.

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**.

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

Tableau A-23. racdump

Sous-commande	Définition
racdump	Affiche des informations générales et d'état sur le DRAC 5.

Synopsis

```
racadm racdump
```

Description

La sous-commande **racdump** utilise une seule commande pour obtenir les informations sur le vidage et l'état, et des informations générales sur une carte DRAC 5.

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 avoir le droit **Configurer le DRAC 5**.

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

Tableau A-24. racreset

Sous-commande	Définition
racreset	Réinitialise le DRAC 5.

PRÉCAUTION : Lorsque vous émettez une sous-commande racreset, il faut jusqu'à une minute au DRAC pour retourner dans un état utilisable.

Synopsis

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

Description

La sous-commande **racreset** envoie une réinitialisation au DRAC 5. L'événement de réinitialisation est écrit dans le journal du DRAC 5.

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.

PRÉCAUTION : Vous devez redémarrer votre système après avoir effectué une réinitialisation matérielle du DRAC 5 comme décrit dans le tableau A-25.

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 RAC 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 redémarrage logicielle du DRAC 5.

- `racadm racreset hard`

  Démarre la séquence de redémarrage matérielle du DRAC 5.

Interfaces prises en charge

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

---

racresetcfg

REMARQUE : Pour utiliser cette commande, vous devez avoir le droit **Configurer le DRAC 5**.

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 du RAC.

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 la carte à ses paramètres par défaut d'origine. Après avoir réinitialisé les propriétés de la base de données, le DRAC 5 se réinitialise automatiquement.

PRÉCAUTION : Cette commande supprime votre configuration RAC actuelle et réinitialise les paramètres par défaut d'origine du RAC et de la configuration série. Après la réinitialisation, le nom et le mot de passe par défaut sont respectivement root et calvin 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 : Cette sous-commande réinitialise également le débit en bauds (57 600) et le port COM par défaut de l'interface série. Les paramètres série devront peut-être être reconfigurés via l'écran de configuration du BIOS du serveur pour accéder au RAC par le port série.

---

serveraction

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

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. 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 avoir le droit **Ouvrir une session sur le DRAC 5**.

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

Tableau A-29. getraclog

Commande	Définition
getraclog -i	Affiche le nombre d'entrées du journal du DRAC 5.
getraclog	Affiche les entrées du journal du DRAC 5.

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 du DRAC 5.

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 du RAC. 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 avoir le droit **Ouvrir une session sur le DRAC 5**.

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 avoir le droit **Ouvrir une session sur le DRAC 5**.

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

Tableau A-31. gettracelog

Commande	Définition
gettracelog -i	Affiche le nombre d'entrées du journal trace du DRAC 5.

gettracelog	Affiche le journal trace du DRAC 5.

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 trace du DRAC 5

-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 avoir le droit **Configurer le DRAC 5**.

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.

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 avoir le droit **Configurer le DRAC 5**.

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

Tableau A-34. sslcertupload

Sous-commande	Description
sslcertupload	Télécharge 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

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 télécharger, 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 télécharger. 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 avoir le droit **Configurer le DRAC 5**.

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

Tableau A-36. sslcertdownload

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

Synopsis

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

Options

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 avoir le droit **Configurer le DRAC 5**.

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

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
Organizational Unit (OU)  : Remote Access Group
Common Name (CN)          : DRAC5 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)          : DRAC5 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
DRAC5 default certificate
US
Texas
Round Rock
Dell Inc.
Remote Access Group
Certificat par défaut du DRAC 5
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 avoir le droit **Configurer le DRAC 5**.

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

Tableau A-40. sslkeyupload

Sous-commande	Description
sslkeyupload	Télécharge la clé SSL du client sur le DRAC 5.

Synopsis

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

Options

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 télécharger. 1 = certificat du serveur
-f	Spécifie le nom de fichier du certificat à télécharger. Si le fichier n'est pas spécifié, le fichier **sslcert** dans le répertoire actuel est sélectionné.

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. 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

---

krbkeytabupload

REMARQUE : Pour utiliser cette commande, vous devez avoir le droit **Configurer le DRAC 5**.

Tableau A-42 décrit la sous-commande **kerbkeytabupload**.

Tableau A-42. kerbkeytabupload

Sous-commande	Description
krbkeytabupload	Télécharge le fichier keytab Kerberos.

Synopsis

```
racadm krbkeytabupload [-f <nomdefichier>]
```

Options

Tableau A-43 décrit les option de la sous-commande **krbkeytabupload**.

Tableau A-43. Option de la sous-commande téléchargerkrbkeytab

Option	Description
-f	Spécifie le nom de fichier du keytab à télécharger. 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 une valeur non nulle 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

---

testemail

Tableau A-44 décrit la sous-commande **testemail**.

Tableau A-44. 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 d'essai du RAC vers une destination indiquée.

Avant d'exécuter la commande testemail, assurez-vous que l'index indiqué dans le groupe **cfgEmailAlert** RACADM est activé et configuré correctement. Tableau A-45 fournit une liste et les commandes associées pour le groupe **cfgEmailAlert**.

Tableau A-45. 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 SNMP est configurée correctement	racadm config -g cfgRemoteHosts -o cfgRhostsSmptServerIpAddr -i 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

Tableau A-46 décrit les options de la sous-commande **testemail**.

Tableau A-46. 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**.

Tableau A-47 décrit la sous-commande **testtrap**.

Tableau A-47. 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 du RAC 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-48 fournit une liste et les commandes associées pour le groupe **cfgIpmiPet**.

Tableau A-48. 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

Tableau A-49 décrit les options de la sous-commande **testtrap**.

Tableau A-49. 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**.

Tableau A-50 décrit la sous-commande **vmdisconnect**.

Tableau A-50. vmdisconnect

Sous-commande	Description
vmdisconnect	Ferme toutes les connexions au média virtuel du RAC 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 reflétera 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 RAC de fermer toutes les sessions de média virtuel actives. Les sessions de média virtuel actives peuvent être affichées dans l'interface Web du RAC ou à l'aide de la sous-commande **getsysinfo** racadm.

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**.

Tableau A-51 décrit la sous-commande **vmkey**.

Tableau A-51. 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 16Mo, sa taille par défaut.

Description

Quand une image de clé de média virtuel personnalisée est téléchargée 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 16 Mo sur le DRAC 5.

Interfaces prises en charge

- RACADM locale

- racadm distant
- RACADM telnet/ssh/série

---

usercertupload

REMARQUE : Pour utiliser cette commande, vous devez avoir le droit **Configurer le DRAC 5**.

Tableau A-52 décrit la sous-commande **usercertupload**.

Tableau A-52. usercertupload

Sous-commande	Description
usercertupload	Télécharge un certificat d'utilisateur ou un certificat CA d'utilisateur du client sur le DRAC.

Synopsis

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

Options

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

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

Option	Description
-t	Spécifie le type de certificat à télécharger, 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 télécharger. 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 avoir le droit **Configurer le DRAC 5**.

Tableau A-54 décrit la sous-commande **usercertview**.

Tableau A-54. usercertview

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

Synopsis

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

Options

Tableau A-55 décrit les options de la sous-commande **sslcertview**.

Tableau A-55. 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.

Tableau A-56 décrit la sous-commande **localConRedirDisable**.

Tableau A-56. 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.

Interfaces prises en charge

- RACADM locale

Retour à la page su sommaire

Retour à la page su sommaire

Définitions des groupes et des objets de la base de données de propriétés du DRAC 5

Dell™ Remote Access Controller 5 Guide d'utilisation de la version 1.45 du micrologiciel

La base de données des propriétés du DRAC 5 contient les informations de configuration du DRAC 5. 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 ID du groupe et de l'objet avec l'utilitaire racadm pour configurer le DRAC 5. Les sections suivantes décrivent chaque objet et indiquent si l'on peut lire et/ou écrire sur l'objet.

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 DRAC 5 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 au maximum.

Valeur par défaut

« Dell Remote Access Controller 5 »

Description

Utilise une chaîne de texte pour identifier le produit.

idRacDescriptionInfo (lecture seule)

Valeurs valides

Chaîne de 255 caractères ASCII au 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 RAC.

idRacVersionInfo (lecture seule)

Valeurs valides

Chaîne de 63 caractères ASCII au maximum.

Valeur par défaut

« 1.0 »

Description

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

idRacBuildInfo (lecture seule)

Valeurs valides

Chaîne de 16 caractères ASCII au maximum.

Valeur par défaut

Numéro de build du micrologiciel du RAC actuel. Par exemple, « 05.12.06 ».

Description

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

idRacName (lecture seule)

Valeurs valides

Chaîne de 15 caractères ASCII au maximum.

Valeur par défaut

DRAC 5

Description

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

idRacType (lecture seule)

Valeur par défaut

6

Description

Identifie le type de Remote Access Controller comme DRAC 5.

---

cfgLanNetworking

Ce groupe contient les paramètres qui permettent de configurer le NIC du DRAC 5.

Une seule instance du groupe est autorisée. Toutes les modifications/mises à jour des objets de ce groupe nécessitent une réinitialisation du NIC du DRAC 5, ce qui interrompra peut-être brièvement la connectivité. Les objets qui modifient les paramètres de l'adresse IP du NIC du DRAC 5 entraîneront la fermeture de toutes les sessions utilisateur actives et les utilisateurs devront se reconnecter en utilisant les paramètres de l'adresse IP mis à jour.

cfgDNSDomainNameFromDHCP (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

1

Description

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

cfgDNSDomainName (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

Chaîne de 254 caractères ASCII au maximum. 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

""

Description

Le nom de domaine DNS. Ce paramètre n'est valide que si **cfgDNSDomainNameFromDHCP** est défini sur 0 (FALSE).

cfgDNSRacName (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

Chaîne de 63 caractères ASCII au maximum.

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

Valeur par défaut

Numéro de service du RAC

Description

Affiche le nom du RAC, qui est son *numéro de service* (par défaut). Ce paramètre n'est valide que si **cfgDNSRegisterRac** est défini sur 1 (TRUE).

cfgDNSRegisterRac (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

Enregistre le nom du DRAC 5 auprès du serveur DNS.

cfgDNSServersFromDHCP (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

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

cfgDNSServer1 (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

Chaîne de caractères représentant une adresse IP valide. Par exemple : « 192.168.0.20 ».

Description

Spécifie l'adresse IP du serveur DNS 1. Cette propriété n'est valide que si **cfgDNSServersFromDHCP** est défini sur **0** (FALSE).

REMARQUE : cfgDNSServer1 et **cfgDNSServer2** peuvent être définis sur les mêmes valeurs pendant l'échange d'adresses.

cfgDNSServer2 (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

Chaîne de caractères représentant une adresse IP valide. Par exemple : « 192.168.0.20 ».

Valeur par défaut

0.0.0.0

Description

Récupère l'adresse IP du serveur DNS 2. Ce paramètre n'est valide que si **cfgDNSServersFromDHCP** est défini sur 0 (FALSE).

REMARQUE : cfgDNSServer1 et **cfgDNSServer2** peuvent être définis sur les mêmes valeurs pendant l'échange d'adresses.

cfgNicEnable (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

Active ou désactive le contrôleur d'interface réseau du RAC. Si le NIC est désactivé, les interfaces réseau distantes du RAC ne sont plus accessibles et le RAC est seulement disponible via les interfaces RACADM série ou locale.

cfgNicIpAddress (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**. Ce paramètre n'est configurable que si le paramètre **cfgNicUseDhcp** est défini sur 0 (FALSE).

Valeurs valides

Chaîne de caractères représentant une adresse IP valide. Par exemple : « 192.168.0.20 ».

Valeur par défaut

192.168.0.120

Description

Spécifie l'adresse IP statique à attribuer au RAC. Cette propriété n'est valide que si **cfgNicUseDhcp** est défini sur **0** (FALSE).

cfgNicNetmask (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**. Ce paramètre n'est configurable que si le paramètre **cfgNicUseDhcp** est défini sur 0 (FALSE).

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

Masque de sous-réseau utilisé pour l'attribution statique de l'adresse IP du RAC. Cette propriété n'est valide que si **cfgNicUseDhcp** est défini sur **0** (FALSE).

cfgNicGateway (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**. Ce paramètre n'est configurable que si le paramètre **cfgNicUseDhcp** est défini sur 0 (FALSE).

Valeurs valides

Chaîne de caractères représentant une adresse IP de passerelle valide. Par exemple : « 192.168.0.1 ».

Valeur par défaut

192.168.0.1

Description

Adresse IP de passerelle utilisée pour l'attribution statique de l'adresse IP du RAC. Cette propriété n'est valide que si **cfgNicUseDhcp** est défini sur **0** (FALSE).

cfgNicUseDhcp (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

Spécifie si le DHCP est utilisé pour attribuer l'adresse IP du RAC. Si cette propriété est définie sur 1 (TRUE), l'adresse IP du RAC, le masque de sous-réseau et la passerelle sont attribués à partir du serveur DHCP sur le réseau. Si cette propriété est définie sur **0** (FALSE), l'adresse IP statique, le masque de sous-réseau et la passerelle sont attribués à partir des propriétés **cfgNicIpAddress**, **cfgNicNetmask** et **cfgNicGateway**.

REMARQUE : Si vous mettez à jour votre système à distance, utilisez la commande **setniccfg**.

cfgNicSelection (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

0 (partagé)

1 (partagé avec basculement)

2 (dédié)

Valeur par défaut

2

Description

Spécifie le mode de fonctionnement actuel pour le contrôleur d'interface réseau du RAC (NIC). 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	Active les capacités de partage entre les contrôleurs d'interface réseau intégrés au serveur hôte.
Dédié	Spécifie que le NIC du RAC est utilisé comme NIC dédié pour l'accessibilité à distance.

cfgNicMacAddress (lecture seule)

Valeurs valides

Chaîne de caractères représentant l'adresse MAC du NIC du RAC.

Valeur par défaut

Adresse MAC actuelle du NIC du RAC. Par exemple, « 00:12:67:52:51:A3 ».

Description

Adresse MAC du NIC du RAC.

cfgNicVLanEnable (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

Active ou désactive les capacités VLAN du RAC/BMC.

cfgNicVLanId (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

0 - 4 094

Valeur par défaut

0

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)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

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).

---

cfgRemoteHosts

Ce groupe fournit des propriétés permettant de configurer différents composants distants, qui incluent le serveur SMTP pour les alertes par e-mail et les adresses IP du serveur TFTP pour les mises à jour de micrologiciel.

cfgRhostsSmtpServerIpAddr (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

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

Valeur par défaut

0.0.0.0

Description

Adresse IP du serveur SMTP réseau. Le serveur SMTP transmet les alertes par e-mail du RAC si les alertes sont configurées et activées.

cfgRhostsFwUpdateTftpEnable (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

1

Description

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

cfgRhostsFwUpdateIpAddr (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

Chaîne de caractères représentant une adresse IP valide du serveur TFTP. Par exemple, `192.168.0.61`.

Valeur par défaut

0.0.0.0

Description

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

cfgRhostsFwUpdatePath (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

Chaîne de caractères. Longueur maximale = 255.

Valeur par défaut

""

Description

Spécifie le chemin d'accès TFTP où le fichier image du micrologiciel du RAC 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**).

---

cfgUserAdmin

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

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

cfgUserAdminIpmiLanPrivilege (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer les utilisateurs**.

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.

cfgUserAdminIpmiSerialPrivilege (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer les utilisateurs**.

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 série IPMI.

cfgUserAdminPrivilege (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer les utilisateurs**.

Valeurs valides

de 0x0000000 à 0x00001ff et 0x0

Valeur par défaut

0x0000000

Description

Cette propriété spécifie les privilèges d'autorité 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. Tableau B-2 décrit les masques binaires des privilèges utilisateur autorisés.

Tableau B-2. Masques binaires pour les privilèges utilisateur

Privilège utilisateur	Masque binaire de privilège
Ouvrir une session sur le DRAC 5	0x0000001
Configurer le DRAC 5	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

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 au RAC.	0x00000000
L'utilisateur peut seulement ouvrir une session sur le RAC et afficher les informations de configuration du RAC et du serveur.	0x00000001
L'utilisateur peut ouvrir une session sur le RAC et modifier la configuration.	0x00000001 + 0x00000002 = 0x00000003
L'utilisateur peut ouvrir une session sur le RAC, accéder au média virtuel et à la redirection de console.	0x00000001 + 0x00000040 + 0x00000080 = 0x000000C1

cfgUserAdminUserName (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer les utilisateurs**.

Valeurs valides

Chaîne de caractères. Longueur maximale = 16.

Valeur par défaut

""

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. Vous ne pouvez pas modifier le nom. Vous devez supprimer puis recréer le nom. La chaîne de caractères ne doit pas contenir de barre oblique (/), de barre oblique inverse (\), de point (.), d'arobase (@) ou de guillemets (").

REMARQUE : Cette valeur de propriété DOIT être unique à partir d'autres instances utilisateur.

cfgUserAdminPassword (lecture seule)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer les utilisateurs**.

Valeurs valides

Chaîne de 20 caractères ASCII au 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 cette propriété écrite.

cfgUserAdminEnable

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer les utilisateurs**.

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

Active ou désactive un utilisateur.

cfgUserAdminSolEnable

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer les utilisateurs**.

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

Active ou désactive un accès utilisateur SOL (communication série sur LAN).

---

cfgEmailAlert

Ce groupe contient des paramètres pour configurer les capacités d'alerte par e-mail du RAC.

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

Ce paramètre est renseigné en fonction des instances existantes.

Description

Index unique d'une instance d'alerte.

cfgEmailAlertEnable (lecture/écriture)

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

Spécifie l'adresse e-mail de destination pour les alertes par e-mail. Par exemple, `user1@company.com`.

cfgEmailAlertAddress (lecture seule)

Valeurs valides

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

Valeur par défaut

""

Description

Adresse e-mail de la source d'alertes.

cfgEmailAlertCustomMsg (lecture seule)

Valeurs valides

Chaîne de caractères. Longueur maximale = 32.

Valeur par défaut

""

Description

Spécifie un message personnalisé qui est envoyé avec l'alerte.

---

cfgSessionManagement

Ce groupe contient les paramètres de configuration du nombre de sessions qui peuvent se connecter au DRAC 5.

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

cfgSsnMgtConsRedirMaxSessions (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 - 2

Valeur par défaut

2

Description

Spécifie le nombre maximum de sessions de redirection de console autorisées sur le RAC.

cfgSsnMgtRacadmTimeout (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

10 -1 920

Valeur par défaut

30

Description

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

cfgSsnMgtWebserverTimeout (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

60 - 1 920

Valeur par défaut

300

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 la session ouverte (vous devez fermer la session et la rouvrir pour que les nouveaux paramètres soient pris en compte).

Une session de serveur Web expirée ferme la session actuelle.

cfgSsnMgtSshIdleTimeout (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

0 (pas de délai d'attente)

60 - 1 920

Valeur par défaut

300

Description

Définit le délai d'attente d'inactivité de Secure Shell. 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 la session ouverte (vous devez fermer la session et la rouvrir pour que les nouveaux paramètres soient pris en compte).

Une session Secure Shell expirée affiche le message d'erreur suivant lorsque vous appuyez sur <Entrée> :

```
Warning: Session no longer valid, may have timed out (Avertissement : La session n'est plus valide, elle a peut-être expiré)
```

Après que le message apparaît, le système vous renvoie à l'environnement qui a généré la session Secure Shell.

cfgSsnMgtTelnetTimeout (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

0 (pas de délai d'attente)

60 - 1 920

Valeur par défaut

0

Description

Définit le délai d'attente d'inactivité Telnet. 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 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 seulement lorsque vous appuyez sur <Entrée> :

```
Warning: Session no longer valid, may have timed out (Avertissement : La session n'est plus valide, elle a peut-être expiré)
```

Après que le message apparaît, le système vous renvoie à l'environnement qui a généré la session Telnet.

---

cfgSerial

Ce groupe contient les paramètres de configuration du port série du DRAC 5.

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

cfgSerialBaudRate (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

9600, 28800, 57600, 115200

Valeur par défaut

57600

Description

Définit le débit en bauds du port série du DRAC 5.

cfgSerialConsoleEnable (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

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

cfgSerialConsoleQuitKey (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

STRING

MaxLen = 2

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 **connect com2**. La valeur **cfgSerialConsoleQuitKey** peut être représentée par :

- 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)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

0 = pas de 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)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

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)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Description

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

Valeur par défaut

""

Exemple

« connect com2 »

cfgSerialHistorySize (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

0 - 8 192

Valeur par défaut

8192

Description

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

cfgSerialSshEnable (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

1

Description

Active ou désactive l'interface Secure Shell (SSH) sur le DRAC 5.

cfgSerialTelnetEnable (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

Active ou désactive l'interface de console telnet sur le RAC.

cfgSerialCom2RedirEnable (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeur par défaut

1

Valeurs valides

1 (TRUE)

0 (FALSE)

Description

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

---

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)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 (activé)

0 (désactivé)

Valeur par défaut

1

Description

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

cfgNetTuningNic100MB (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

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)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

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)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

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 du DRAC 5.

cfgNetTuningTcpSrttDflt (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

6 - 384

Valeur par défaut

6

Description

La valeur minimale arrondie de base du délai d'attente aller-retour pour la durée de retransmission aller-retour TCP en unités de ½ seconde. (Tapez des valeurs hexadécimales.)

---

cfgOobSnmp

Le groupe contient les paramètres de configuration de l'agent et des capacités d'interruption SNMP du DRAC 5.

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

cfgOobSnmpAgentCommunity (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

Chaîne de caractères. Longueur maximale = 31.

Valeur par défaut

public

Description

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

cfgOobSnmpAgentEnable (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

Active ou désactive l'agent SNMP dans le RAC.

cfgRacTuning

Ce groupe est utilisé pour configurer des propriétés de configuration du RAC différentes, comme les ports valides et les restrictions de port de sécurité.

cfgRacTunePluginType

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 (TRUE) : plug-in Java

0 (FALSE) : plug-in Natif

Valeur par défaut

0

Description

Configure le type de plug-in KVM virtuel (vKVM).

cfgRacTuneHttpPort (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

10 - 65 535

Valeur par défaut

80

Description

Spécifie le numéro de port à utiliser pour la communication réseau HTTP avec le RAC.

cfgRacTuneHttpsPort (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

10 - 65 535

Valeur par défaut

443

Description

Spécifie le numéro de port à utiliser pour la communication réseau HTTPS avec le RAC.

cfgRacTuneIpRangeEnable

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

Active ou désactive la fonctionnalité Validation de la plage d'adresses IP du RAC.

cfgRacTuneIpRangeAddr

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

Chaîne de caractères, adresse IP formatée. Par exemple, `192.168.0.44`.

Valeur par défaut

`192.168.1.1`

Description

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

cfgRacTuneIpRangeMask

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

Valeurs de masque IP standard avec bits justifiés à gauche

Valeur par défaut

`255.255.255.0`

Description

Chaîne de caractères, adresse IP formatée. Par exemple, `255.255.255.0`.

cfgRacTuneIpBlkEnable

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

Active ou désactive la fonctionnalité Blocage de l'adresse IP du RAC.

cfgRacTuneIpBlkFailCount

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

2 - 16

Valeur par défaut

5

Description

Nombre maximum d'échecs d'ouverture de session dans la fenêtre avant que les tentatives d'ouverture de session depuis l'adresse IP soient rejetées.

cfgRacTuneIpBlkFailWindow

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

2 - 65 535

Valeur par défaut

60

Description

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

cfgRacTuneIpBlkPenaltyTime

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

2 - 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)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 - 65 535

Valeur par défaut

22

Description

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

cfgRacTuneTelnetPort (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 - 65 535

Valeur par défaut

23

Description

Spécifie le numéro de port utilisé pour l'interface telnet du RAC.

cfgRacTuneRemoteracadmEnable (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

1

Description

Active ou désactive l'interface RACADM distante dans le RAC.

cfgRacTuneConRedirEncryptEnable (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

Encrypte la vidéo dans une session de redirection de console.

cfgRacTuneConRedirPort (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 - 65 535

Valeur par défaut

5901

Description

Spécifie le port utilisé pour le clavier et la souris pendant l'activité de redirection de console avec le RAC.

REMARQUE : Cet objet exige une réinitialisation du DRAC 5 pour s'activer.

cfgRacTuneConRedirVideoPort (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 - 65 535

Valeur par défaut

5901

Description

Spécifie le port utilisé pour la vidéo pendant l'activité de redirection de console avec le RAC.

REMARQUE : Cet objet exige une réinitialisation du DRAC 5 pour s'activer.

cfgRacTuneAsrEnable (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

0 (FALSE)

1 (TRUE)

Valeur par défaut

1

Description

Active ou désactive la fonctionnalité Capture d'écran de panne du RAC.

REMARQUE : Cet objet exige une réinitialisation du DRAC 5 pour s'activer.

cfgRacTuneDaylightOffset (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

0 - 60

Valeur par défaut

0

Description

Spécifie le décalage des économies de lumière du jour (en minutes) à utiliser pour l'heure du RAC.

cfgRacTuneTimezoneOffset (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

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 communs pour les fuseaux horaires des États-Unis sont illustrés 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)

cfgRacTuneWebserverEnable (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

0 (FALSE)

1 (TRUE)

Valeur par défaut

1

Description

Active et désactive le serveur Web du RAC. Si cette propriété est désactivée, le RAC n'est pas accessible à l'aide de navigateurs Web clients ou de la RACADM distante. Cette propriété n'a aucun effet sur les interfaces telnet/ssh/série ou RACADM locale.

cfgRacTuneLocalServerVideo (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 (active)

0 (désactive)

Valeur par défaut

1

Description

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

cfgRacTuneLocalConfigDisable

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

Active ou désactive la capacité d'un utilisateur local à configurer le DRAC 5 à l'aide de la racadm locale ou des utilitaires de Dell OpenManage Server Administrator.

cfgRacTuneCtrlEConfigDisable

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

Active ou désactive la capacité de l'utilisateur local à configurer le DRAC 5 depuis l'option ROM du POST du BIOS.

---

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/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

Chaîne de caractères. Longueur maximale = 255.

Valeur par défaut

""

Description

Le nom d'hôte du système géré.

ifcRacMnOsOsName (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

Chaîne de caractères. Longueur maximale = 255.

Valeur par défaut

""

Description

Nom du système d'exploitation du système géré.

---

cfgRacSecurity

Ce groupe est utilisé pour configurer les paramètres relatifs à la fonctionnalité Requête de signature de certificat (CSR) SSL du RAC. Les propriétés de ce groupe DOIVENT être configurées avant de générer une CSR à partir du RAC.

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)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

Chaîne de caractères. Longueur maximale = 254.

Valeur par défaut

""

Description

Spécifie le nom commun (CN) de la CSR.

cfgRacSecCsrOrganizationName (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

Chaîne de caractères. Longueur maximale = 254.

Valeur par défaut

""

Description

Spécifie le nom de compagnie (O) de la CSR.

cfgRacSecCsrOrganizationUnit (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

Chaîne de caractères. Longueur maximale = 254.

Valeur par défaut

""

Description

Spécifie le service de la compagnie (OU) de la CSR.

cfgRacSecCsrLocalityName (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

Chaîne de caractères. Longueur maximale = 254.

Valeur par défaut

""

Description

Spécifie la ville (L) de la CSR.

cfgRacSecCsrStateName (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

Chaîne de caractères. Longueur maximale = 254.

Valeur par défaut

""

Description

Spécifie le nom d'état (S) de la CSR.

cfgRacSecCsrCountryCode (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

Chaîne de caractères. Longueur maximale = 2.

Valeur par défaut

""

Description

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

cfgRacSecCsrEmailAddr (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

Chaîne de caractères. Longueur maximale = 254.

Valeur par défaut

""

Description

L'adresse e-mail de la CSR.

cfgRacSecCsrKeySize (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1024

2048

4096

Valeur par défaut

1024

Description

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

---

cfgRacVirtual

Ce groupe contient les paramètres qui permettent de configurer la fonctionnalité Média virtuel du DRAC 5. Une seule instance du groupe est autorisée. Les sous-sections suivantes décrivent les objets de ce groupe.

cfgVirMediaAttached (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

Cet objet est utilisé pour relier vos 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 du DRAC5 ou de la CLI. Lorsque cet objet est défini sur **0**, les périphériques ne sont plus reliés au bus USB.

REMARQUE : Vous devez redémarrer votre système pour activer toutes les modifications.

cfgVirAtapiSrvPort (lecture/écriture)

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

Valeurs valides

1 - 65 535

Valeur par défaut

3669

Description

Spécifie le numéro de port utilisé pour les connexions de média virtuel cryptées sur le RAC.

cfgVirAtapiSrvPortSsl (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

Tout numéro de port inutilisé en décimal, compris entre 0 et 65 535.

Valeur par défaut

3669

Description

Définit le port utilisé pour les connexions de média virtuel SSL.

cfgVirMediaKeyEnable (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

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

cfgVirtualBootOnce (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

0 - Désactiver : désactive cette option.

1 - Disque flash virtuel/Média virtuel : démarrer à partir du disque flash virtuel ou d'un média virtuel quelconque.

2 - Disquette virtuelle : démarrer à partir d'un lecteur de disquette virtuel.

3 - CD/DVD/ISO virtuel : démarrer à partir d'un CD/DVD/ISO virtuel.

4 - PXE : démarrer le serveur sur PXE (en réseau).

5 - Disque dur : démarrer sur le disque dur par défaut.

6 - Partition d'utilitaires : démarrer sur la partition d'utilitaires. Une partition d'utilitaires doit déjà exister.

7 - CD/DVD par défaut : lecteur de CD/DVD par défaut du serveur.

8 - Configuration du BIOS : écran de configuration du BIOS.

9 - Média amovible principal : démarrer à partir d'un média USB amovible émulé en tant que disquette de démarrage.

Valeur par défaut

0

Description

Définit le périphérique à un seul démarrage. Si cette propriété est définie sur un périphérique pris en charge et lorsque le serveur hôte est redémarré, cette fonctionnalité va tenter de démarrer à partir du périphérique sélectionné, si le média approprié est installé dans le périphérique.

REMARQUE : Pour activer la fonctionnalité Un seul démarrage sur le *disque flash virtuel*, allez dans la configuration du BIOS et modifiez manuellement l'ordre de démarrage durant le redémarrage du système.

REMARQUE : Les périphériques à un seul démarrage autres que *Disque flash virtuel (1)*, *PXE (4)* et *Désactiver (0)* sont pris en charge uniquement sur certains systèmes ayant des versions de micrologiciel BIOS et de contrôleur de gestion de la carte mère (BMC) prises en charge. Consultez le site Web de Dell à l'adresse **www.dell.com** pour vérifier si votre système prend en charge tous les périphériques à un seul démarrage.

REMARQUE : Sur les systèmes ne prenant pas en charge la *Disquette virtuelle* et le *CD/DVD/ISO virtuel*, utilisez « 1 » (*disque flash virtuel/média virtuel*) pour exécuter le Démarrage unique soit sur la *Disquette virtuelle*, soit sur le *CD/DVD/ISO virtuel* ou le *Disque flash virtuel*. Dans ce cas, définissez le périphérique virtuel requis en tant que premier périphérique de démarrage dans la configuration du BIOS. Le DRAC 5 déconnecte automatiquement ce périphérique une fois que le serveur a redémarré sur le périphérique et le système redémarre à nouveau.

REMARQUE : Sur les systèmes prenant en charge la *Disquette virtuelle* et le *CD/DVD/ISO virtuel* comme options séparées, le DRAC 5 ne déconnecte pas ou ne détache pas automatiquement la connexion du média virtuel après la procédure Un seul démarrage.

cfgFloppyEmulation (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 (True)

0 (False)

Valeur par défaut

0

Description

Lorsque cette propriété est définie sur 0, le lecteur de disquette virtuel est reconnu comme lecteur 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:.

---

cfgActiveDirectory

Ce groupe contient les paramètres qui permettent de configurer la fonctionnalité Active Directory du DRAC 5.

cfgADRacDomain (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

Toute chaîne de texte imprimable sans espace. La longueur est limitée à 254 caractères.

Valeur par défaut

""

Description

Domaine Active Directory où se trouve le DRAC.

cfgADRacName (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

Toute chaîne de texte imprimable sans espace. La longueur est limitée à 254 caractères.

Valeur par défaut

""

Description

Nom du DRAC enregistré dans la forêt Active Directory.

cfgADEnable (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

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

cfgADSpecifyServerEnable (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 ou 0 (True ou False).

Valeur par défaut

0

Description

1 (True) vous permet de spécifier un serveur LDAP ou de catalogue global. 0 (False) désactive cette option.

cfgADDomainController (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

Adresse IP ou nom de domaine pleinement qualifié (FQDN) valide

Valeur par défaut

Pas de valeur par défaut

Description

Le DRAC 5 utilise la valeur que vous spécifiez afin d'effectuer la recherche par noms d'utilisateur sur le serveur LDAP.

cfgADGlobalCatalog (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

Adresse IP ou FQDN valide

Valeur par défaut

Pas de valeur par défaut

Description

Le DRAC 5 utilise la valeur que vous spécifiez afin d'effectuer la recherche par noms d'utilisateur sur le serveur de catalogue global.

cfgAODomain (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

Adresse IP ou FQDN valide

Formater

<domaine> :<IP ou FQDN>

Valeur par défaut

Pas de valeur par défaut

Description

Le DRAC 5 utilise la valeur que vous spécifiez afin d'effectuer la recherche d'objet Association pour les noms d'utilisateur.

cfgADSmartCardLogonEnable (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

Active ou désactive l'ouverture de session par carte à puce sur le DRAC 5.

cfgADCRLEnable (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 (TRUE)

0 (FALSE)

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.

cfgADAuthTimeout (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

15 - 300

Valeur par défaut

120

Description

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

cfgADRootDomain (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

Toute chaîne de texte imprimable sans espace. La longueur est limitée à 254 caractères.

Valeur par défaut

""

Description

Domaine racine de la forêt de domaine.

cfgADType (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 = active le schéma étendu avec Active Directory.

2 = active le schéma standard avec Active Directory.

Valeur par défaut

1 = schéma étendu

Description

Détermine le type de schéma à utiliser avec Active Directory.

cfgADSSOEnable (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 (TRUE)

0 (FALSE)

Valeur par défaut

0

Description

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

---

cfgStandardSchema

Ce groupe contient les paramètres de configuration des paramètres Schéma standard.

cfgSSADRoleGroupIndex (lecture seule)

Valeurs valides

Entier de 1 à 5.

Description

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

cfgSSADRoleGroupName (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

Toute chaîne de texte imprimable sans espace. La longueur est limitée à 254 caractères.

Valeur par défaut

(vide)

Description

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

cfgSSADRoleGroupDomain (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

Toute chaîne de texte imprimable sans espace. La longueur est limitée à 254 caractères.

Valeur par défaut

(vide)

Description

Domaine Active Directory où se trouve le groupe de rôles.

cfgSSADRoleGroupPrivilege (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

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 sur le DRAC 5	0x00000001
Configurer le DRAC 5	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

---

cfgIpmiSerial

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

cfgIpmiSerialConnectionMode (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

0 (terminal)

1 (de base)

Valeur par défaut

1

Description

Lorsque la propriété **cfgSerialConsoleEnable** du DRAC 5 est définie sur 0 (désactivé), le port série du DRAC 5 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)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

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)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

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)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

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)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

0 (FALSE)

1 (TRUE)

Valeur par défaut

1

Description

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

cfgIpmiSerialLineEdit (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

0 (FALSE)

1 (TRUE)

Valeur par défaut

1

Description

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

cfgIpmiSerialEchoControl (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

0 (FALSE)

1 (TRUE)

Valeur par défaut

1

Description

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

cfgIpmiSerialDeleteControl (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

0 (FALSE)

1 (TRUE)

Valeur par défaut

0

Description

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

cfgIpmiSerialNewLineSequence (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

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)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

0 (<ENTRÉE>)

1 (NULL)

Valeur par défaut

1

Description

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

---

cfgIpmiSol

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

cfgIpmiSolEnable (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

0 (FALSE)

1 (TRUE)

Valeur par défaut

1

Description

Active ou désactive la communication série sur LAN (SOL).

cfgIpmiSolBaudRate (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

9600, 19200, 57600, 115200

Valeur par défaut

57600

Description

Débit en bauds pour la communication série sur le LAN.

cfgIpmiSolMinPrivilege (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

2 (utilisateur)

3 (opérateur)

4 (administrateur)

Valeur par défaut

4

Description

Spécifie le niveau de privilège minimal exigé pour la communication série sur le LAN.

cfgIpmiSolAccumulateInterval (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 - 255.

Valeur par défaut

10

Description

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

cfgIpmiSolSendThreshold (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 - 255

Valeur par défaut

255

Description

Valeur seuil SOL.

---

cfgIpmiLan

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

cfgIpmiLanEnable (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

0 (FALSE)

1 (TRUE)

Valeur par défaut

1

Description

Active ou désactive l'interface IPMI sur LAN.

cfgIpmiLanPrivLimit (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

2 (utilisateur)

3 (opérateur)

4 (administrateur)

Valeur par défaut

0

Description

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

cfgIpmiLanAlertEnable (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

0 (FALSE)

1 (TRUE)

Valeur par défaut

1

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)

REMARQUE : Pour afficher ou modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5** et des privilèges Administrateur.

Valeurs valides

Chaîne de chiffres hexadécimaux de 0 à 20 caractères sans espace.

Valeur par défaut

« 00000000000000000000 »

Description

Clé de cryptage IPMI.

cfgIpmiPetCommunityName (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

Chaîne de 18 caractères au maximum.

Valeur par défaut

« public »

Description

Nom de communauté SNMP pour les interruptions.

---

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 système géré.

cfgIpmiPefName (lecture seule)

Valeurs valides

Chaîne de caractères. Longueur maximale = 255.

Valeur par défaut

Nom du filtre d'index.

Description

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

cfgIpmiPefIndex (lecture seule)

Valeurs valides

1 - 17

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)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

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 système géré lorsque l'alerte est déclenchée.

cfgIpmiPefEnable (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

0 (FALSE)

1 (TRUE)

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 plate-forme du système géré.

cfgIpmiPetIndex (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

1 - 4

Valeur par défaut

Valeur d'index appropriée.

Description

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

cfgIpmiPetAlertDestIpAddr (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

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

Valeur par défaut

0.0.0.0

Description

Spécifie l'adresse IP 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 système géré.

cfgIpmiPetAlertEnable (lecture/écriture)

REMARQUE : Pour modifier cette propriété, vous devez avoir le droit **Configurer le DRAC 5**.

Valeurs valides

0 (FALSE)

1 (TRUE)

Valeur par défaut

1

Description

Active ou désactive une interruption spécifique.

Retour à la page su sommaire

Retour à la page su sommaire

Interfaces RACADM prises en charge

Dell™ Remote Access Controller 5 Guide d'utilisation de la version 1.45 du micrologiciel

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	✓	✗	✓
clearascreen	✓	✓	✓
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	✘	✔	✘
✔ = Pris en charge ; ✘ = Non pris en charge			

Retour à la page su sommaire

Retour à la page su sommaire

Présentation du DRAC 5

Dell™ Remote Access Controller 5 Guide d'utilisation de la version 1.45 du micrologiciel

Le Dell™ Remote Access Controller 5 (DRAC 5) est une solution matérielle et logicielle de gestion de systèmes conçue pour fournir des capacités de gestion à distance, de remise en état d'un système suite à une panne et de contrôle de l'alimentation pour les systèmes Dell .

En communiquant avec le contrôleur de gestion de la carte mère (BMC) du système, vous pouvez configurer le DRAC 5 (une fois installé) de sorte qu'il vous envoie des alertes par e-mail en cas d'avertissements ou d'erreurs liés aux tensions, aux températures, aux intrusions ainsi qu'aux vitesses des ventilateurs. De plus, le DRAC 5 journalise les données des événements et l'écran de la dernière panne (uniquement pour les systèmes exécutant le système d'exploitation Microsoft® Windows®) pour vous aider à diagnostiquer la cause probable d'une panne du système.

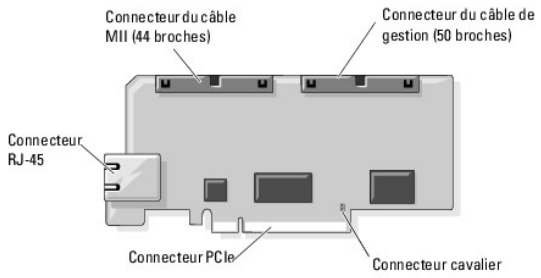
Le DRAC 5 a son propre microprocesseur et sa propre mémoire, et il est alimenté par le système dans lequel il est installé. Le DRAC 5 peut être préinstallé dans le système ou vous pouvez vous procurer un kit séparé.

Pour vous familiariser avec le DRAC 5, voir « Familiarisation avec le DRAC 5 ».

Spécifications et fonctionnalités du DRAC 5

Figure 1-1 illustre le matériel du DRAC 5.

Figure 1-1. Fonctionnalités matérielles du DRAC 5



Spécifications du DRAC 5

Spécifications de l'alimentation

Tableau 1-1 énumère les exigences concernant l'alimentation du DRAC 5.

Tableau 1-1. Spécifications de l'alimentation du DRAC 5

Alimentation système
1,2 A sur +3,3 V AUX (maximum
550 mA sur +3,3 V principal (maximum)
0 mA sur +5 V principal (maximum)

Connecteurs

REMARQUE : Les instructions d'installation relatives au matériel du DRAC 5 sont disponibles dans le document intitulé *Installation d'une carte d'accès à distance* ou dans le *Guide d'installation et de dépannage* fourni avec votre système.

Le DRAC 5 inclut un NIC RJ-45 10/100 Mb/s intégré, un câble de gestion à 50 broches et un câble MII à 44 broches. Voir Figure 1-1 pour prendre connaissance des connecteurs des câbles du DRAC 5.

Le câble de gestion à 50 broches est l'interface principale du DRAC qui fournit la connectivité au bus USB, série, vidéo et à circuit inter-intégré (I2C). Le câble MII à 44 broches connecte le NIC du DRAC à la carte mère du système. Le connecteur RJ-45 connecte le NIC du DRAC à une connexion hors bande lorsque le DRAC 5 est configuré en mode **NIC exclusif**.

Selon vos exigences, vous pouvez utiliser les câbles de gestion et MII pour configurer votre DRAC en trois modes séparés. Pour plus d'informations, voir

« Modes DRAC ».

Ports du DRAC 5

Tableau 1-2 identifie les ports d'écoute utilisés par le DRAC 5 pour une connexion serveur. Tableau 1-3 identifie les ports que le DRAC 5 utilise comme client. Ces informations sont nécessaires lors de l'ouverture de pare-feu pour accéder à distance à un DRAC 5.

Tableau 1-2. Ports d'écoute de serveur du DRAC 5

Numéro de port	Fonction
22*	Secure Shell (SSH)
23*	Telnet
80*	HTTP
161	Agent SNMP
443*	HTTPS
623	RMCP/RMCP+
3668*	Serveur de média virtuel
3669*	Service de média virtuel sécurisé
5900*	Clavier/Souris de la redirection de console
5901*	Vidéo de la redirection de console
* Port configurable	

Tableau 1-3. Ports clients du DRAC 5

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)

Connexions d'accès à distance prises en charge

Tableau 1-4 répertorie les fonctionnalités de connexion.

Tableau 1-4. Connexions d'accès à distance prises en charge

Connexion	Fonctionnalités
NIC du DRAC 5	• Ethernet à 10/100 Mb/s • Prise en charge de DHCP • Interruptions SNMP et notifications d'événements par e-mail • Interface réseau dédiée pour l'interface Web du DRAC 5 • Prise en charge de la console telnet/ssh et des commandes CLI RACADM, y compris les commandes de démarrage, de réinitialisation, de mise sous tension et d'arrêt du système
Port série	• Prise en charge de la console série et des commandes CLI racadm, y compris les commandes de démarrage, de réinitialisation, de mise sous tension et d'arrêt du système • Prise en charge de la redirection de console texte seulement vers un terminal ou un émulateur de terminal VT-100

Fonctionnalités standard du DRAC 5

Le DRAC 5 dispose des fonctionnalités suivantes :

- Authentification bifactorielle, assurée par l'ouverture de session par carte à puce. L'authentification bifactorielle est basée sur ce que possèdent les utilisateurs (la carte à puce) et sur ce qu'ils connaissent (le code PIN).
- Authentification des utilisateurs via Microsoft 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 d'ID d'utilisateur et de mot de passe par l'interface Web ou la CLI RACADM
- Enregistrement de système de noms de domaine dynamique (DNS)
- Gestion et surveillance du système à distance via une interface Web, une connexion série, une RACADM distante ou une connexion telnet.
- Prise en charge de l'authentification Active Directory : centralise tous les ID d'utilisateurs et mots de passe du DRAC 5 dans Active Directory à l'aide du schéma standard et du schéma étendu.
- Redirection de console : fournit les fonctions de clavier, vidéo et souris à distance.
- Média virtuel : permet à un système géré d'accéder à un lecteur de média sur la station de gestion.
- Accès aux journaux des événements système : permet d'accéder au journal des événements système (SEL), au journal du DRAC 5 et à l'écran de la dernière panne 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 du DRAC 5 à partir de Dell OpenManage Server Administrator ou d'IT Assistant.
- Alerte du RAC : signale les problèmes de nud géré potentiels via des messages par e-mail ou une interruption SNMP à l'aide des paramètres **Dédié**, **Partagé avec basculement** ou **Partagé** de la NIC.
- Configuration locale et distante : permet une configuration locale et distante à l'aide de l'utilitaire de ligne de commande RACADM.
- Gestion de l'alimentation à distance : fournit des fonctionnalités de gestion de l'alimentation à distance à partir d'une console de gestion, comme l'arrêt et la réinitialisation.
- Prise en charge d'IPMI.
- Gestion standardisée avec IPMI sur réseau local et SM-CLP.
- Capteurs de surveillance de la consommation de puissance. Le DRAC 5 utilise ces données pour représenter la consommation de puissance du système par des graphiques et données statistiques.
- 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.

Autres documents utiles

En plus de ce *Guide d'utilisation*, les documents suivants fournissent des informations supplémentaires sur la configuration et l'utilisation du DRAC 5 dans votre système :

- L'aide en ligne du DRAC 5 donne des informations sur l'utilisation de l'interface Web.
- Le *Guide d'utilisation de Dell OpenManage IT Assistant* donne des informations à propos de IT Assistant.
- Le *Guide d'utilisation de Dell OpenManage Server Administrator* donne des informations sur l'installation et l'utilisation de Server Administrator.
- Le *Guide de référence SNMP de Dell OpenManage Server Administrator* traite de la base d'informations de gestion de Server Administrator SNMP (MIB). La MIB définit les variables qui étendent la MIB standard pour couvrir les capacités des agents de gestion de systèmes.
- Le *Guide d'utilisation des utilitaires de contrôleur de gestion de la carte mère de Dell OpenManage* fournit des informations sur la configuration du contrôleur de gestion de la carte mère (BMC), en configurant votre système géré à l'aide de l'utilitaire de gestion du contrôleur BMC et des informations supplémentaires sur le BMC.
- Le *Guide d'utilisation des progiciels Dell Update Package* fournit des informations sur l'obtention et l'utilisation des progiciels Dell Update Package dans le cadre de votre stratégie de mise à jour du système.
- La *Matrice d'assistance logicielle des systèmes Dell* fournit des informations concernant les différents systèmes Dell, les systèmes d'exploitation pris en charge par ces systèmes et les composants Dell OpenManage pouvant être installés sur ces systèmes.

En outre, la documentation système suivante fournit des informations supplémentaires sur le système sur lequel le DRAC 5 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 soit dans ce document, soit à part.
- Le *Guide d'installation du rack* ou les *Instructions d'installation du rack* fournis avec votre solution rack décrivent comment installer votre système dans un rack.
- Le document *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 à la page su sommaire

Retour à la page su sommaire

Utilisation et configuration du média virtuel

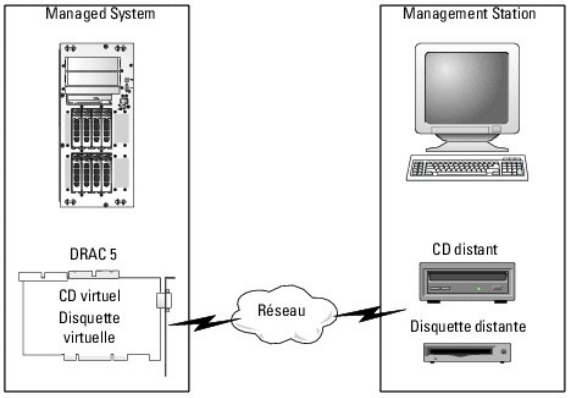
Dell™ Remote Access Controller 5 Guide d'utilisation de la version 1.45 du micrologiciel

---

Présentation

La fonctionnalité Média virtuel fournit au système géré un lecteur de CD virtuel qui peut utiliser des médias standards à partir de n'importe quel endroit sur le réseau. Figure 10-1 illustre l'architecture globale d'un média virtuel.

Figure 10-1. Architecture globale d'un média virtuel



Grâce au média virtuel, les administrateurs peuvent démarrer à distance leurs systèmes 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 disquette virtuels.

REMARQUE : Le média virtuel exige une bande passante réseau disponible d'au moins 128 Kb/s.

Le système géré est configuré avec une carte DRAC 5. Les lecteurs de CD et de disquette virtuels sont deux périphériques électroniques intégrés au DRAC 5 et contrôlés par le micrologiciel du DRAC 5. Ces deux périphériques sont toujours présents sur le système d'exploitation et le BIOS du système géré, que le média virtuel soit connecté ou déconnecté.

La station de gestion fournit le média physique ou le fichier image sur le réseau. La première fois que vous lancez le navigateur du RAC et que vous accédez à la page Média virtuel, le plug-in du média virtuel est téléchargé à partir du serveur Web du DRAC 5 et est automatiquement installé sur la station de gestion. Pour que la fonctionnalité Média virtuel fonctionne correctement, le plug-in du média virtuel doit être installé sur la station de gestion.

Quand le média virtuel est connecté, toutes les demandes d'accès au lecteur de CD ou de disquette virtuel à partir du système géré sont dirigées vers la station de gestion via le réseau. La connexion du média virtuel est identique à l'insertion de médias dans les périphériques virtuels. Lorsque le média virtuel n'est pas connecté, les périphériques virtuels sur le système géré se comportent comme deux lecteurs exempts de média.

Tableau 10-1 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 10-1. 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 au format ISO9660
Image de lecteur de disquette 1.44	Lecteur de CD-ROM USB avec média de CD-ROM.

Installation du plug-in du média virtuel

Le plug-in du navigateur du média virtuel doit être installé sur votre station de gestion pour pouvoir utiliser la fonctionnalité Média virtuel. Après avoir ouvert l'interface utilisateur du DRAC 5 et lancé la page Média virtuel, le navigateur télécharge automatiquement le plug-in, si nécessaire. Si le plug-in est correctement installé, la page Média virtuel affiche une liste de disquettes et de disques optiques qui se connectent au lecteur virtuel.

Station de gestion Windows

Pour exécuter la fonctionnalité Média virtuel sur une station de gestion exécutant le système d'exploitation Microsoft® Windows®, installez une version prise en charge d'Internet Explorer® avec le plug-in de contrôle ActiveX. Définissez la sécurité du navigateur sur **Moyen** ou un paramètre inférieur pour autoriser Internet Explorer à télécharger et à installer les contrôles ActiveX signés.

En outre, vous devez posséder des droits d'administrateur pour pouvoir installer et utiliser la fonctionnalité Média virtuel. Avant d'installer le contrôle ActiveX, Internet Explorer peut afficher un avertissement de sécurité. Pour terminer la procédure d'installation du contrôle ActiveX, acceptez le contrôle ActiveX lorsqu'Internet Explorer affiche un avertissement de sécurité.

Station de gestion Linux

Pour exécuter la fonctionnalité Média virtuel sur une station de gestion exécutant le système d'exploitation Linux, installez une version prise en charge de Mozilla ou de Firefox. Si le plug-in du média virtuel n'est pas installé ou si une nouvelle version est disponible, une boîte de dialogue s'affiche au cours de la procédure d'installation et vous demande de confirmer l'installation du plug-in sur la station de gestion. Assurez-vous que l'ID d'utilisateur exécutant le navigateur a des droits d'écriture dans l'arborescence de répertoires du navigateur. Si l'ID d'utilisateur n'a pas de droits d'écriture, vous ne pouvez pas installer le plug-in du média virtuel.

Consultez la *Matrice de prise en charge des logiciels des systèmes Dell* située sur le site Web de support de Dell à l'adresse **support.dell.com** pour plus d'informations.

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.

À l'aide du média virtuel, vous pouvez « virtualiser » une image de disquette ou un lecteur, en permettant à une image de disquette, un lecteur de disquette ou un lecteur optique sur votre console de gestion de devenir un lecteur disponible sur le système distant.

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.

Exécution du média virtuel à l'aide de l'interface utilisateur Web

Connexion du média virtuel

1. Ouvrez un navigateur Web pris en charge sur votre station de gestion. Pour obtenir une liste des navigateurs Web pris en charge, consultez la *Matrice de prise en charge des logiciels des systèmes Dell* sur le site Web Dell Support à l'adresse **support.dell.com**.

PRÉCAUTION : La redirection de console et le média virtuel prennent uniquement en charge les navigateurs Web 32 bits. L'utilisation de navigateurs Web 64 bits peut générer des résultats inattendus ou des défaillances.

2. Connectez-vous au DRAC 5 et ouvrez une session. Voir « Accès à l'interface Web pour de plus amples informations ».

3. Cliquez sur l'onglet **Média**, puis sur **Média virtuel**.

   La page **Média virtuel** apparaît avec les lecteurs client qui peuvent être virtualisés.

   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 un seul lecteur optique et un seul lecteur de disquette en même temps, ou un seul lecteur.

   REMARQUE : Les lettres du lecteur de périphérique virtuel sur le système géré ne coïncident pas avec celles du lecteur physique sur la station de gestion.

4. Si on vous le demande, suivez les instructions affichées à l'écran pour installer le plug-in du média virtuel.

5. Dans la case **Attribut**, effectuez les étapes suivantes :

   a. Dans la colonne **Valeur**, assurez-vous que la valeur d'état **Connecter/Déconnecter** est définie sur **Connecté**.

      Si la valeur est **Déconnecté**, effectuez les étapes suivantes :

      - Dans l'onglet **Média**, cliquez sur **Configuration**.
      - Dans la colonne **Valeur**, assurez-vous que la case **Connecter le média virtuel** est cochée.
      - Cliquez sur **Appliquer les modifications**.
      - Dans l'onglet **Média virtuel**, cliquez sur **Média virtuel**.
      - Dans la colonne **Valeur**, assurez-vous que la valeur d'état **Connecter/Déconnecter** est définie sur **Connecté**.

   b. Assurez-vous que la valeur **État actuel** est **Pas connecté**. Si le champ **Valeur** affiche Connecté, vous devez vous déconnecter de l'image ou du lecteur avant de vous reconnecter. Cet état indique l'état actuel de la connexion du média virtuel sur l'interface Web actuelle uniquement.

   c. Vérifiez que la valeur S**ession active** est **Disponible**. Si le champ **Valeur** affiche **En cours d'utilisation**, vous devez attendre que la session existante du média virtuel soit achevée ou vous devez y mettre fin en accédant à l'onglet Gestion de sessions dans Accès distant et en interrompant la session active du média virtuel. Une seule session active du média virtuel n'est autorisée à la fois. Cette session aurait pu être créée par une interface Web ou un utilitaire VM-CLI quelconque.

   d. Cochez la case **Cryptage activé** pour établir une connexion cryptée entre le système distant et votre station de gestion (si nécessaire).

6. Si vous virtualisez une image de disquette ou une image ISO, sélectionnez **Fichier image de disquette** ou **Fichier d'image ISO** et saisissez ou accédez au fichier image que vous voulez virtualiser.

   Si vous virtualisez un lecteur de disquette ou un lecteur optique, sélectionnez le bouton à côté des lecteurs que vous voulez virtualiser.

7. Cliquez sur **Connecter**.

   Si la connexion est authentifiée, l'état de la connexion devient **Connecté** et une liste de tous les lecteurs connectés est affichée. Toutes les images de disquette disponibles et les lecteurs que vous avez sélectionnés deviennent disponibles sur la console du système géré, bien qu'il s'agisse de lecteurs réels.

   REMARQUE : La lettre de lecteur virtuel attribuée (pour les systèmes Microsoft Windows) ou le fichier spécial de périphérique (pour les systèmes Linux) peut ne pas être identique à la lettre de lecteur sur votre console 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.

Déconnexion du média virtuel

Cliquez sur **Déconnecter** pour déconnecter toutes les images et lecteurs virtualisés de la station de gestion. **Toutes** les images ou lecteurs virtualisés sont tous déconnectés et ne sont plus disponibles sur le système géré.

Connexion et déconnexion de la fonctionnalité Média virtuel

La fonctionnalité Média virtuel du DRAC 5 est fondée sur la technologie USB et peut profiter des fonctionnalités USB Plug and Play. Le DRAC 5 permet aussi de connecter et de déconnecter les périphériques virtuels du bus USB. Lorsque les périphériques sont déconnectés, le système d'exploitation ou le BIOS ne peut pas voir les lecteurs connectés. Lorsque les périphériques virtuels sont connectés, les lecteurs sont visibles. À la différence du DRAC 4, où les lecteurs pouvaient seulement être activés ou désactivés lors du redémarrage du système, les périphériques virtuels du DRAC 5 peuvent être connectés ou déconnectés à tout moment.

Les périphériques virtuels peuvent être connectés ou déconnectés à l'aide d'un navigateur Web, d'une racadm locale/distante et d'un port série/Telnet. Pour configurer le média virtuel à l'aide d'un navigateur Web, accédez à la page **Média**, puis à la page **Configuration**, où vous pouvez modifier les paramètres et les appliquer. Vous pouvez aussi spécifier le **Numéro de port de média virtuel** et le **Numéro de port SSL de média virtuel**. De plus, vous pouvez activer ou désactiver la fonctionnalité Disque flash virtuel et Un seul démarrage. Consultez « cfgVirtualBootOnce (lecture/écriture) » pour des informations sur la fonction Un seul démarrage. Si cette propriété est définie sur un périphérique pris en charge, au redémarrage du serveur hôte, la fonction tentera de démarrer depuis le périphérique sélectionné, si le média approprié est installé dans le périphérique.

Auto-connexion du média virtuel

La version 1.30 et autres versions ultérieures du micrologiciel du DRAC 5 prennent en charge la fonctionnalité d'auto-connexion du média virtuel. Lorsque vous activez cette fonctionnalité, le DRAC 5 connecte automatiquement un périphérique virtuel au système uniquement lorsqu'un périphérique est virtualisé (connecté) sur un client pris en charge.

Le DRAC 5 déconnectera les périphériques de média virtuel une fois la session du média virtuel déconnectée

Connexion, auto-connexion et déconnexion du média virtuel à l'aide du navigateur Web

Pour connecter la fonctionnalité Média virtuel, procédez comme suit :

1. Cliquez sur **Système** -> **Média** -> **Configuration**

2. Cochez la case **Valeur** pour **Connecter le média virtuel**
3. Cliquez sur **Appliquer les modifications**.

Pour déconnecter la fonctionnalité Média virtuel, procédez comme suit :

1. Cliquez sur **Système** -> **Média** -> **Configuration**
2. Décochez la case **Valeur** pour **Connecter le média virtuel**
3. Cliquez sur **Appliquer les modifications**.

Connexion, auto-connexion et déconnexion du média virtuel à l'aide de la RACADM

Pour connecter la fonctionnalité Média virtuel, ouvrez une invite de commande, tapez la commande suivante, puis appuyez sur <Entrée> :

```
racadm config -g cfgRacVirtual -o cfgVirMediaAttached 1
```

Pour déconnecter le média virtuel, ouvrez une invite de commande, tapez la commande suivante, puis appuyez sur <Entrée> :

```
racadm config -g cfgRacVirtual -o cfgVirMediaAttached 0
```

Pour auto-connecter le média virtuel, ouvrez une invite de commande, tapez la commande suivante, puis appuyez sur <Entrée> :

```
racadm config -g cfgRacVirtual -o cfgVirMediaAttached 2
```

Démarrage à partir d'un média virtuel

Sur les systèmes pris en charge, 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 modifier le paramètre du BIOS :

1. Démarrez le système 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 système géré redémarre.

   Le système géré essaie de démarrer à partir d'un périphérique de démarrage en fonction de l'ordre de démarrage. Si un périphérique virtuel est connecté et qu'un média de démarrage est présent, le système démarre sur le périphérique virtuel. Autrement, le système ignore le périphérique (semblable à 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 de système d'exploitation scriptée à l'aide du média virtuel peut prendre moins de 15 minutes. Pour plus d'informations, voir « Déploiement de votre système d'exploitation à l'aide de l'utilitaire VM-CLI ».

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 « » afin de garantir que le BIOS est configuré pour démarrer à partir du lecteur de CD à partir duquel vous effectuez l'installation.Démarrage à partir d'un média virtuel
3. Suivez les instructions à l'écran pour terminer l'installation.

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 auto-montés 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 au niveau d'une station de gestion, le média est disponible sur le système en cliquant sur le lecteur et en parcourant son contenu.

Systèmes Linux

Sur les systèmes Linux, les lecteurs de média virtuel ne sont pas configurés avec une lettre de lecteur. Selon le logiciel installé sur votre système, les lecteurs de média virtuel ne peuvent pas être auto-montés. Si vos lecteurs ne sont pas auto-montés, montez-les manuellement.

Utilisation du disque flash virtuel

Le DRAC 5 fournit un disque flash virtuel permanent de 16 Mo de mémoire flash qui réside dans le système de fichiers du DRAC 5 qui peut être utilisé pour le stockage permanent et est accessible par le système. Lorsqu'il est activé, le disque flash virtuel est configuré comme le troisième lecteur virtuel et apparaît dans l'ordre de démarrage du BIOS, ce qui permet à un utilisateur de démarrer à partir du disque flash virtuel.

REMARQUE : Pour démarrer à partir du disque flash virtuel, l'image de disque flash virtuel doit être une image de démarrage.

À la différence d'un CD ou d'un lecteur de disquette qui exige une connexion client externe ou un périphérique fonctionnel dans le système hôte, l'implémentation du disque flash virtuel exige seulement la fonctionnalité Disque flash virtuel permanent du DRAC 5. La mémoire flash de 16 Mo apparaît comme un lecteur USB non formaté et amovible dans l'environnement hôte.

Suivez les instructions suivantes lors de l'implémentation du disque flash virtuel :

- La connexion ou la déconnexion du disque flash virtuel effectue une ré-énumération USB, qui connecte et déconnecte tous les périphériques du média virtuel, respectivement (par exemple, lecteur de CD et lecteur de disquette).
- Lorsque vous activez ou désactivez le disque flash virtuel, l'état de connexion du lecteur de CD/disquette du média virtuel ne change pas.

PRÉCAUTION : Les procédures de déconnexion et de connexion perturbent les opérations de lecture et d'écriture actives du média virtuel.

Activation du disque flash virtuel

Pour activer le disque flash virtuel, ouvrez une invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

```
racadm config -g cfgRacVirtual -o cfgVirMediaKeyEnable 1
```

Désactivation du disque flash virtuel

Pour activer le disque flash virtuel, ouvrez une invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

```
racadm config -gcfgRacVirtual -o cfgVirMediaKeyEnable 0
```

Stockage des images dans un disque flash virtuel

Le disque flash virtuel peut être formaté à partir de l'hôte géré. Si vous exécutez le système d'exploitation Windows, cliquez-droite sur l'icône de lecteur et sélectionnez **Format**. Si vous exécutez Linux, les outils système tels que **format** et **fdisk** vous permettent de partitionner et de formater l'USB.

Avant de télécharger une image à partir du navigateur Web du RAC sur le disque flash virtuel, assurez-vous que le fichier image fait entre 1,44 et 16 Mo (inclus) et que le disque flash virtuel est désactivé. Après avoir téléchargé l'image et réactivé le disque flash virtuel, le système et le BIOS reconnaissent le disque flash virtuel.

Configuration d'un disque flash virtuel de démarrage

1. Insérez une disquette de démarrage dans le lecteur de disquette ou insérez un CD de démarrage dans le lecteur optique.
2. Redémarrez votre système et démarrez sur le lecteur de média sélectionné.
3. Ajoutez une partition au disque flash virtuel et activez la partition.

Utilisez **fdisk** si le disque flash virtuel émule le disque dur. Si le disque flash virtuel est configuré comme lecteur B:, le disque flash virtuel est émulé par la disquette et ne nécessite pas de partition pour configurer le disque flash virtuel comme lecteur de démarrage.

4. À l'aide de la commande **format**, formatez le lecteur avec le commutateur **/s** pour transférer les fichiers système vers le disque flash virtuel.

   Par exemple :

   `format /s x`

   où *x* est la lettre de lecteur attribuée au disque flash virtuel.

5. Arrêtez le système et retirez la disquette ou le CD de démarrage du lecteur approprié.

6. Mettez le système sous tension et vérifiez que le système démarre à partir du disque flash virtuel à l'invite `C:\` ou `A:\`.

Utilisation de l'utilitaire d'interface de ligne de commande du média virtuel

L'utilitaire d'interface de ligne de commande du média virtuel (VM-CLI) est une interface de ligne de commande scriptable qui fournit des fonctionnalités de média virtuel de la station de gestion au DRAC 5 dans le système distant.

L'utilitaire VM-CLI fournit les fonctionnalités suivantes :

- Prise en charge de plusieurs sessions actives simultanément.

  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-ins du média virtuel
- L'arrêt automatique lorsque l'option de démarrage unique du micrologiciel du DRAC est activée.
- Les communications sécurisées vers le DRAC 5 à l'aide du protocole Secure Sockets Layer (SSL)

Avant d'exécuter l'utilitaire, assurez-vous que vous avez des privilèges d'utilisateur de média virtuel sur le DRAC 5 dans le système distant.

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 VM-CLI.

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 VM-CLI.

Pour les systèmes Linux, vous pouvez accéder à l'utilitaire VM-CLI 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 VM-CLI, l'administrateur utilise la commande **visudo**. Les utilisateurs sans privilèges Administrateur peuvent ajouter la commande **sudo** comme préfixe à la ligne de commande VM-CLI (ou au script VM-CLI) afin d'accéder au DRAC 5 dans le système distant et d'exécuter l'utilitaire.

Installation de l'utilitaire

L'utilitaire VM-CLI 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 le diagnostic, la gestion du stockage, le service d'accès à distance et l'utilitaire RACADM. Ce DVD contient aussi des fichiers lisez-moi, qui fournissent les dernières informations sur les produits logiciels de gestion de systèmes.

De plus, le DVD *Dell Systems Management Tools and Documentation* inclut **vmdeploy**, un modèle de script qui illustre comment utiliser les utilitaires VM-CLI et RACADM pour déployer le logiciel sur plusieurs systèmes distants. Pour plus d'informations, voir « Déploiement de votre système d'exploitation à l'aide de l'utilitaire VM-CLI ».

Options de ligne de commande

L'interface VM-CLI est identique sur les systèmes Windows et Linux. L'utilitaire utilise des options qui sont en accord avec les options de l'utilitaire RACADM. Par exemple, une option pour spécifier l'adresse IP du DRAC 5 exige la même syntaxe pour les utilitaires RACADM et VM-CLI.

Le format d'une commande VM-CLI est comme suit :

`racvmcli` *`[paramètre] [options_d'environnement_de_système_d'exploitation]`*

REMARQUE : Vous devez avoir des privilèges **Administrateur** pour exécuter la commande `racvmcli`.

Toute la syntaxe de la ligne de commande est sensible à la casse. Pour plus d'informations, voir « Paramètres VM-CLI ».

Si le système distant accepte les commandes et si le DRAC 5 autorise la connexion, la commande continue de s'exécuter jusqu'à ce qu'un des événements suivants se produise :

- La connexion VM-CLI est interrompue pour une raison ou une autre.
- 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 VM-CLI

Adresse IPdu DRAC 5

`-r <adresse-IP-du-RAC>[:<port-SSL-du-RAC>]`

où <*adresse-IP-du-RAC*> est une adresse IP unique valide ou le nom DDNS (Dynamic Domain Naming System - Système dynamique d'attributions de noms de domaine) du DRAC 5 (si pris en charge).

Ce paramètre fournit l'adresse IP et le port SSL du DRAC 5. L'utilitaire VM-CLI a besoin de ces informations pour établir une connexion de média virtuel avec le DRAC 5 cible. Si vous saisissez une adresse IP ou un nom DDNS non valide, un message d'erreur apparaît et la commande est terminée.

Si <*port-SSL-du-RAC*> est omis, le port 443 (le port par défaut) est utilisé. le port SSL optionnel n'est pas obligatoire sauf si vous changez le port SSL par défaut du DRAC 5.

Nom d'utilisateur du DRAC 5

`-u <nom-d'utilisateur-du-DRAC>`

Ce paramètre fournit le nom d'utilisateur DRAC 5 qui exécutera le média virtuel.

Le <*nom-d'utilisateur-du-DRAC*> doit comporter les attributs suivants :

- Nom d'utilisateur valide
- Droit d'utilisateur de média virtuel du DRAC

Si l'authentification du DRAC 5 échoue, un message d'erreur s'affiche et la commande est interrompue.

Mot de passe d'utilisateur du DRAC

`-p <mot-de-passe-d'utilisateur-du-DRAC>`

Ce paramètre fournit le mot de passe de l'utilisateur du DRAC 5 indiqué.

Si l'authentification du DRAC 5 échoue, un message d'erreur s'affiche et la commande est interrompue.

Périphérique de disquette/disque ou fichier image

`-f {<nom-du-périphérique> | <fichier-image>}`

où <*nom-du-périphérique*> est une lettre de lecteur valide (pour les systèmes Windows) ou un nom de fichier de périphérique valide, notamment le numéro de partition du système de fichiers montable, si applicable (pour les systèmes Linux) ; et <*fichier-image*> est le nom de fichier et le chemin d'accès d'un fichier image valide.

Ce paramètre spécifie le périphérique ou le fichier qui fournit le média de disquette/disque virtuel.

Par exemple, un fichier image est spécifié comme :

`-f c:\temp\myfloppy.img` (système Windows)

`-f/tmp/myfloppy.img` (système Linux)

Si le fichier n'est pas protégé contre l'écriture, le média virtuel peut écrire sur le fichier image. Configurez le système d'exploitation pour protéger contre l'écriture un fichier image de disquette qui ne doit pas être écrasé.

Par exemple, un périphérique est spécifié comme :

`-f a:\` (système Windows)

`-f /dev/sdb4 # 4ème partition sur le périphérique` /dev/sdb (système Linux)

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.

De plus, 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-du-périphérique> | <fichier-image>}`

où `<nom-du-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'accès 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 Windows)

`-c/dev/cdrom` (systèmes Linux)

De plus, 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 VM-CLI. 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 VM-CLI. 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, l'utilitaire VM-CLI utilise un canal crypté SSL pour transférer des données entre la station de gestion et le DRAC 5 dans le système distant. Si ce paramètre n'est pas inclus dans la ligne de commande, le transfert de données n'est pas crypté.

Options d'environnement du système d'exploitation VM-CLI

Les fonctionnalités du système d'exploitation suivantes peuvent être utilisées sur la ligne de commande VM-CLI :

- 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 VM-CLI.

  REMARQUE : L'utilitaire VM-CLI 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 VM-CLI 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 de poursuivre le script après le démarrage d'un nouveau processus pour la commande VM-CLI (le cas échéant, le script serait bloqué jusqu'à ce que le programme VM-CLI soit interrompu). Lorsque plusieurs instances VM-CLI sont démarrées de cette manière et qu'une ou plusieurs instances de commande doivent être interrompues manuellement, utilisez les équipements spécifiques au système d'exploitation pour énumérer et interrompre les processus.

Codes de retour VM-CLI

0 = aucune erreur

1 = connexion impossible

2 = erreur de ligne de commande VM-CLI

3 = connexion du micrologiciel du RAC coupée

Les messages de texte seulement en anglais sont aussi distribués vers la sortie d'erreur standard chaque fois que l'on rencontre des erreurs.

Déploiement de votre système d'exploitation à l'aide de l'utilitaire VM-CLI

L'utilitaire d'interface de ligne de commande de média virtuel (VM-CLI) est une interface de ligne de commande qui fournit les fonctionnalités de média virtuel de la station de gestion au DRAC 5 dans le système distant. À l'aide de VM-CLI et de méthodes cryptées, vous pouvez déployer votre système d'exploitation sur plusieurs systèmes distants dans votre réseau.

Cette section fournit des informations sur l'intégration de l'utilitaire VM-CLI dans votre réseau d'entreprise.

Avant de commencer

Avant d'utiliser l'utilitaire VM-CLI, assurez-vous que vos systèmes distants cibles et votre réseau d'entreprise répondent aux exigences mentionnées dans les sections suivantes.

Exigences du système distant

- Une carte DRAC 5 est installée dans chaque système distant
- Le périphérique virtuel dans chaque système distant est le premier périphérique dans l'ordre de démarrage du BIOS.

Custom Factory Integration de Dell

Lorsque vous commandez votre système Dell™ à l'aide des options CFI (Custom Factory Integration) de Dell, Dell peut préconfigurer votre système avec une carte DRAC 5 qui comprend un nom DDNS et un BIOS système préconfiguré qui est activé pour le média virtuel. Grâce à cette configuration, votre système peut être démarré à partir de ses périphériques de média virtuel lorsqu'il est installé dans votre réseau d'entreprise.

Pour plus d'informations, consultez le site Web de Dell à l'adresse **www.dell.com**.

Configuration réseau requise

Vous devez disposer d'un partage réseau contenant ce qui suit :

- Fichiers de système d'exploitation
- Pilotes requis
- Fichier(s) image de démarrage du système d'exploitation

  Le fichier image doit être une image de disquette 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 fichier image vers un système de test à l'aide de l'interface utilisateur Web du DRAC 5, puis redémarrez le système.

Les sections suivantes fournissent des informations spécifiques pour créer des fichiers image pour les systèmes Windows et Linux.

Création d'un fichier image pour les systèmes Linux

Utilisez l'utilitaire de duplicateur de données 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/fd0 of=myfloppy.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 les scripts utilisés pour les procédures de déploiement de système d'exploitation

   Par exemple, pour déployer le système d'exploitation Microsoft® 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, exécutez les étapes suivantes :

   - 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 la RACADM et l'interface de ligne de commande de média virtuel (VM-CLI) dans votre application de déploiement de système d'exploitation existante. Utilisez le modèle de script de déploiement comme guide lors de l'intégration des utilitaires du DRAC 5 dans votre application de déploiement de système d'exploitation existante.
   - Utilisez le script **vmdeploy** existant pour déployer votre système d'exploitation.

Déploiement du système d'exploitation

Utilisez l'utilitaire VM-CLI et le script **vmdeploy** inclus avec l'utilitaire pour déployer le système d'exploitation dans vos systèmes distants.

Avant de commencer, vérifiez le modèle de script **vmdeploy** inclus avec l'utilitaire VM-CLI. Le script offre des exigences détaillées 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. Identifiez les systèmes distants qui seront déployés.
2. Enregistrez les noms et les adresses IP du DRAC 5 des systèmes distants cibles.
3. Effectuez la procédure suivante pour chaque système distant cible :
   a. Configurez un processus VM-CLI qui inclut les paramètres suivants pour le système cible :
      - Adresse IP ou nom DDNS du DRAC 5
      - Nom de fichier image de déploiement de démarrage
      - Nom d'utilisateur du DRAC 5
      - Mot de passe utilisateur du DRAC 5
   b. À l'aide de la RACADM, configurez l'option **Un seul démarrage** du DRAC 5 cible.
   c. À l'aide de la RACADM, redémarrez le système DRAC 5.

Questions les plus fréquentes

Je remarque parfois que ma connexion client de média virtuel se coupe. Pourquoi ?

En cas de dépassement du délai d'attente du réseau, le micrologiciel du DRAC 5 interrompt la connexion, en déconnectant le lien entre le serveur et le lecteur virtuel. Pour rétablir la connexion au lecteur virtuel, utilisez la fonctionnalité du média virtuel.

Quels sont les systèmes d'exploitation pris en charge par le DRAC 5 ?

Consultez la *Matrice de prise en charge des logiciels des systèmes Dell* située sur le site Web de support de Dell à l'adresse **support.dell.com** pour une liste des systèmes d'exploitation pris en charge.

Quels sont les navigateurs Web pris en charge par le DRAC 5 ?

Consultez la *Matrice de prise en charge des logiciels des systèmes Dell* située sur le site Web de support de Dell à l'adresse **support.dell.com** pour une liste des 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.
- En cas de dépassement du délai d'attente du réseau, le micrologiciel du DRAC 5 interrompt la connexion, en déconnectant le lien entre le serveur et le lecteur virtuel. Pour rétablir la connexion au lecteur virtuel, utilisez la fonctionnalité du média virtuel.

Que dois-je faire si je n'arrive pas à installer correctement Windows 2000 avec le Service Pack 4 ?

Si vous utilisez le média virtuel et le CD du système d'exploitation Windows 2000 pour installer Windows 2000 avec le Service Pack 4, votre système peut momentanément perdre sa connexion au lecteur de CD pendant la procédure d'installation et le système d'exploitation peut ne pas être installé correctement. Pour résoudre ce problème, téléchargez le fichier **usbstor.sys** à partir du site Web de support de Microsoft à l'adresse **support.microsoft.com** et exécutez le programme uniquement sur les systèmes qui ont rencontré ce problème. Pour plus d'informations, consultez l'article 823086 de la base de connaissances Microsoft.

Pourquoi ne puis-je pas installer Windows 2000 localement ou à distance ?

Ce problème se produit généralement si le disque flash virtuel est activé et ne contient pas d'image valide ; par exemple, si le disque flash virtuel contient une image corrompue ou aléatoire, vous ne pouvez pas installer Windows 2000 localement ou à distance. Pour résoudre ce problème, installez une image valide sur le disque flash virtuel ou désactivez le disque flash virtuel s'il n'est pas utilisé pendant la procédure d'installation.

Pourquoi la connexion au média virtuel est-elle interrompue lorsqu'elle est configurée en mode NIC partagé ?

L'installation de pilotes de réseau et de chipset sur le serveur peut interrompre la connexion au média virtuel en cas de configuration en mode NIC partagé. L'installation de pilotes de réseau ou de chipset provoque la réinitialisation de LOM, qui provoque à son tour l'expiration des paquets réseau ainsi que l'expiration et l'interruption de la connexion au média virtuel. Pour contourner ce problème, copiez les pilotes de votre lecteur virtuel sur le disque dur local du serveur. Pour empêcher que toute connexion au média virtuel interrompue n'interfère avec la procédure d'installation de votre pilote, démarrez directement l'installation du pilote à partir du serveur.

Une installation du système d'exploitation Windows 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 du DRAC 5 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.

Je visualise le contenu d'un lecteur de disquette ou d'une clé mémoire USB. Si j'essaie d'établir une connexion au média virtuel en utilisant le même lecteur, je reçois un message d'échec de connexion et on me demande de réessayer. Pourquoi ?

L'accès simultané aux lecteurs de disquette virtuels n'est pas autorisé. Fermez l'application utilisée pour visualiser le contenu du lecteur avant d'essayer de virtualiser le lecteur.

Comment puis-je configurer mon périphérique virtuel comme périphérique de démarrage ?

Sur le système géré, accédez au programme de configuration du BIOS, puis au 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. 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 ?

Le DRAC 5 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
- Disque flash virtuel intégré au DRAC 5
- 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 ?

Seules les clés USB avec le DOS Windows 98 peuvent démarrer à partir de la disquette virtuelle. Pour configurer votre propre clé USB de démarrage, démarrez sur un disque de démarrage Windows 98 et copiez les fichiers système à partir du disque de démarrage 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.

Vous pouvez également utiliser l'utilitaire de démarrage de Dell pour créer une clé USB de démarrage. Cet utilitaire n'est compatible qu'avec les clés USB de Dell. Pour télécharger l'utilitaire, ouvrez un navigateur Web pris en charge, naviguez vers le site Web de support de Dell à l'adresse **support.dell.com** et recherchez le fichier « R122672.exe ».

Ai-je besoin de privilèges Administrateur pour installer le plug-in ActiveX ?

Vous devez disposer de privilèges Administrateur ou Utilisateur privilégié sur les systèmes Windows pour pouvoir installer le plug-in du média virtuel.

Quels privilèges faut-il pour installer et utiliser le plug-in du média virtuel sur une station de gestion Red Hat Linux ?

Vous devez disposer de privilèges d'écriture dans l'arborescence des répertoires du navigateur pour pouvoir installer le plug-in du média virtuel.

Je n'arrive pas à trouver mon lecteur de disquette 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 monter le lecteur de disquette virtuel, recherchez le nud de périphérique que Linux affecte au lecteur de disquette virtuel. Procédez aux étapes suivantes 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 « Dell Virtual Floppy »

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.

Quels types de système de fichiers sont pris en charge sur mon lecteur de disquette virtuel ou sur le disque flash virtuel ?

Votre lecteur de disquette virtuel ou disque flash virtuel prend en charge les systèmes de fichiers FAT16 ou FAT32.

Quand j'ai effectué une mise à jour de micrologiciel à distance à l'aide de l'interface Web du DRAC 5, mes lecteurs virtuels sur le serveur ont été supprimés. Pourquoi ?

Les mises à jour de micrologiciel entraînent la réinitialisation du DRAC 5, une interruption de la connexion à distance et le démontage des lecteurs virtuels. Les lecteurs réapparaîtront une fois la réinitialisation du DRAC terminée.

En activant ou en désactivant le disque flash virtuel, j'ai remarqué que tous mes lecteurs virtuels ont disparu puis sont réapparus. Pourquoi ?

La désactivation ou l'activation du disque flash virtuel entraîne une réinitialisation USB et déconnecte puis reconnecte tous les lecteurs virtuels au bus USB.

Comment faire pour installer un navigateur Web sur ma station de gestion qui dispose d'un système de fichiers en lecture seule ?

Si vous exécutez Linux et que votre station de gestion a un système de fichiers en lecture seule, un navigateur peut être installé sur un système client sans nécessiter de connexion à un DRAC 5. En utilisant le progiciel d'installation de plug-in natif, le navigateur peut être installé manuellement pendant la phase de configuration du client.

△ **PRÉCAUTION : Dans un environnement client en lecture seule, si le micrologiciel du DRAC 5 est mis à jour avec une version plus récente du plug-in, le plug-in du média virtuel installé devient alors inopérationnel. C'est parce que les fonctionnalités de plug-in plus anciennes ne peuvent pas fonctionner lorsque le micrologiciel contient une version de plug-in plus récente. Vous êtes dans ce cas invité à installer le plug-in. Comme le système de fichiers est en lecture seule, l'installation échouera et les fonctionnalités de plug-in ne seront pas disponibles.**

Pour vous procurer le progiciel d'installation du plug-in :

1. Ouvrez une session sur un DRAC 5 existant

2. Dans la barre d'adresses du navigateur, remplacez l'URL :

   `https://<IP_RAC>/cgi-bin/webcgi/main`

   par :

   `https://<IP_RAC>/plugins/ # N'oubliez pas d'inclure la barre oblique.`

3. Identifiez les deux sous-répertoires vm et vkvm. Accédez au sous- répertoire approprié, cliquez-droite sur le fichier rac5XXX.xpi, puis sélectionnez **Enregistrer la cible du lien sous...**

4. Sélectionnez un emplacement pour enregistrer le fichier du progiciel d'installation du plug-in.

Pour installer le progiciel d'installation du plug-in :

1. Copiez le progiciel d'installation sur le partage de système de fichiers natif du client qui est accessible par le client.
2. Ouvrez une instance du navigateur sur le système client.
3. Saisissez le chemin d'accès du fichier vers le progiciel d'installation du plug-in dans la barre d'adresses du navigateur. Par exemple :

   file:///tmp/rac5vm.xpi

4. Le navigateur guide l'utilisateur à travers les différentes étapes d'installation du plug-in.

Une fois installé, le navigateur ne demandera plus l'installation de ce plug-in, tant que le micrologiciel du DRAC 5 cible ne contient pas une version plus récente du plug-in.

Retour à la page su sommaire

Retour à la page su sommaire

Configuration des fonctionnalités de sécurité

Dell™ Remote Access Controller 5 Guide d'utilisation de la version 1.45 du micrologiciel

Le DRAC 5 dispose des fonctionnalités de sécurité suivantes :

- Options Sécurité avancée pour l'administrateur du DRAC :
  - 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 du DRAC 5.
  - Les fonctionnalités de désactivation de la configuration locale permettent à l'administrateur du DRAC *distant* de désactiver de manière sélective la capacité de configuration du DRAC 5 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 l'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 au DRAC 5

Options de sécurité pour l'administrateur du DRAC

Désactivation de la configuration locale du DRAC 5

Les administrateurs peuvent désactiver la configuration locale via l'interface utilisateur graphique (GUI) du DRAC 5 en sélectionnant **Accès distant**→ **Configuration**→ **Services**. Lorsque la case **Désactiver la configuration locale du DRAC à l'aide de l'option ROM** est cochée, l'utilitaire Remote Access Configuration (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 du DRAC à l'aide de RACADM**, les utilisateurs locaux ne peuvent pas configurer le DRAC 5 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 la GUI, 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 le DRAC 5 pendant le redémarrage du système.

```
racadm config -g cfgRacTune -o

cfgRacTuneCtrlEConfigDisable 1
```

REMARQUE : Cette option est prise en charge uniquement sur l'utilitaire Remote Access Configuration Utility version 1.13 et version ultérieure. 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 DVD *Dell Server Updates* ou sur le site Web Dell Support 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 le DRAC 5 à l'aide de la racadm locale ou des utilitaires de Dell OpenManage Server Administrator.

```
racadm config -g cfgRacTune -o cfgRacTuneLocalConfigDisable 1
```

PRÉCAUTION : Ces fonctionnalités limitent considérablement la capacité de l'utilisateur local à configurer le DRAC 5 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 GUI ou une interface de ligne de commande du DRAC 5 hors bande 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 le DRAC 5 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 du DRAC 5 local et n'autorisent que les utilisateurs du service de répertoires Microsoft Active Directory® à ouvrir une session sur le DRAC 5 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 DRAC 5 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 du DRAC 5 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 du DRAC 5

Les administrateurs peuvent désactiver de manière sélective le KVM distant du DRAC 5, 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 du DRAC 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 locale, 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 du DRAC 5. Par exemple, les administrateurs peuvent ne pas vouloir qu'un utilisateur du DRAC 5 distant voit les paramètres du BIOS qu'ils configurent sur un système, auquel 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 du DRAC 5 via SSL et des certificats numériques

Cette sous-section fournit des informations sur les fonctionnalités de sécurité des données suivantes qui sont intégrées dans votre DRAC 5 :

- « Secure Sockets Layer (SSL) »
- « Requête de signature de certificat (CSR) »
- « Accès au menu principal SSL »
- « Génération d'une nouvelle requête de signature de certificat »
- « Téléchargement d'un certificat de serveur »
- « Téléchargement d'un certificat de serveur »

Secure Sockets Layer (SSL)

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

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. Le DRAC 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 du DRAC inclut un certificat numérique SSL autosigné Dell (ID de serveur). Pour garantir un haut niveau de sécurité sur Internet, remplacez le certificat SSL de serveur Web en envoyant une demande au DRAC pour générer une nouvelle requête de signature de certificat (CSR).

Requête de signature de certificat (CSR)

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 télécharger 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 CSR et vous envoie le certificat, vous devez le télécharger dans le micrologiciel du contrôleur DRAC. Les informations de CSR stockées dans le micrologiciel du contrôleur DRAC 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 les options de la page **Menu principal SSL** (voir Tableau 11-1) pour générer une CSR à envoyer à une CA. Les informations de la CSR sont stockées dans le micrologiciel du DRAC 5. Tableau 11-2 décrit les boutons disponibles à la page **Menu principal SSL**.

Tableau 11-1. Options du menu principal SSL

Champ	Description
Générer une nouvelle requête de signature de certificat (CSR)	Cliquez sur **Suivant** pour ouvrir la page **Génération de la requête de signature de certificat** qui permet de générer une CSR à envoyer à une CA pour demander un certificat Web sécurisé. **PRÉCAUTION : 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.**
Télécharger le certificat de serveur	Cliquez sur **Suivant** pour télécharger un certificat existant qui appartient à votre société et qu'elle utilise pour contrôler l'accès au DRAC 5. **PRÉCAUTION : Seuls les certificats X509 encodés en base 64 sont acceptés par le DRAC 5. Les certificats encodés DER ne sont pas acceptés. Téléchargez un nouveau certificat pour remplacer le certificat par défaut que vous avez reçu avec le DRAC 5.**
Afficher le certificat de serveur	Cliquez sur **Suivant** pour afficher un certificat de serveur existant.

Tableau 11-2. Boutons du menu principal SSL

Bouton	Description
Imprimer	Imprime la page **Menu principal SSL**.
Suivant	Navigue jusqu'à la page suivante.

Génération d'une nouvelle requête de signature de certificat

REMARQUE : Chaque nouvelle CSR supplante la CSR qui se trouve déjà sur le micrologiciel. Pour qu'une autorité de certification (CA) puisse accepter votre CSR, la CSR du micrologiciel doit correspondre au certificat renvoyé par la CA. Sinon, le DRAC 5 ne téléchargera pas le certificat.

1. Sur la page **Menu principal SSL**, sélectionnez **Générer une nouvelle requête de signature de certificat (CSR)** et cliquez sur **Suivant**.
2. Sur la page **Générer une requête de signature de certificat (CSR)**, tapez une valeur pour chaque valeur d'attribut CSR.

Tableau 11-3 décrit les options de la page **Générer une requête de signature de certificat (CSR)**.

3. Cliquez sur **Générer** pour enregistrer ou afficher la CSR.

4. Cliquez sur le bouton approprié de la page **Générer une requête de signature de certificat (CSR)** pour continuer. Tableau 11-4 décrit les boutons disponibles dans la page **Générer une requête de signature de certificat (CSR)**.

Tableau 11-3. 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 et les points sont valides. Les espaces ne sont pas 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 11-4. 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)**.
Retour au menu principal Sécurité	Retourne à la page **Menu principal SSL**.
Générer	Génère une CSR.

Téléchargement d'un certificat de serveur

1. Sur la page **Menu principal SSL**, sélectionnez **Télécharger le certificat de serveur** et cliquez sur **Suivant**.

   La page **Téléchargement d'un certificat** apparaît.

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 téléchargez. 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.

Affichage d'un certificat de serveur

1. Sur la page **Menu principal SSL**, sélectionnez **Afficher le certificat de serveur** et cliquez sur **Suivant**.

   Tableau 11-5 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 11-5. 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)

Quatre sessions SSH uniquement sont prises en charge à la fois. Le délai d'expiration de la session est contrôlé par la propriété `cfgSsnMgtSshIdleTimeout` comme décrit dans « Définitions des groupes et des objets de la base de données de propriétés du DRAC 5 ».

Vous pouvez activer SSH sur le DRAC 5 avec la commande :

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

Vous pouvez changer le port SSH avec la commande :

```
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 de propriétés du DRAC 5 ».

La mise en oeuvre SSH du DRAC 5 prend en charge plusieurs schémas de cryptographie, comme illustré dans le tableau 11-6.

Tableau 11-6. 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 des services

REMARQUE : Pour modifier ces paramètres, vous devez avoir le droit **Configurer le DRAC 5**. 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 11-7)
   - Tableau 11-8 Serveur Web ()
   - SSH (Tableau 11-9)
   - Telnet (Tableau 11-10)
   - RACADM distante (Tableau 11-11)
   - Agent SNMP (Tableau 11-12)
   - Agent de récupération de système automatique (Tableau 11-13)

   Utilisez l'**agent de récupération de système automatique** pour activer la fonctionnalité **Écran de la dernière panne** du DRAC 5.

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 le DRAC 5.

4. Cliquez sur **Appliquer les modifications**.

5. Cliquez sur le bouton approprié de la page **Services** pour continuer. Reportez-vous à la section Tableau 11-14.

Tableau 11-7. Paramètres de configuration locale

Paramètre	Description
Désactiver la configuration locale du DRAC avec l'option ROM	Désactive la configuration locale du DRAC 5 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 du DRAC avec RACADM	Désactive la configuration locale du DRAC 5 à l'aide de la RACADM locale.

Tableau 11-8. Paramètres de Web Server

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	Délai en secondes pendant lequel une connexion peut rester inactive. La session est annulée quand le délai d'expiration est atteint. Les modifications apportées au paramètre du délai d'expiration n'affectent pas la session actuelle. Lorsque vous modifiez le paramètre du délai d'expiration, vous devez fermer puis rouvrir une session pour appliquer le nouveau paramètre. La plage du délai d'expiration est comprise entre 60 et 1 920 secondes.
Numéro de port HTTP	Port utilisé par le DRAC pour une connexion serveur. Le paramètre par défaut est **80**.
Numéro de port HTTPS	Port utilisé par le DRAC pour une connexion serveur. Le paramètre par défaut est **443**.

Tableau 11-9. Paramètres SSH

Paramètre	Description
Activé	Active ou désactive SSH. Coché = Activé ; Décoché = Désactivé.
Nombre maximal de sessions	Nombre maximal de sessions simultanées autorisées pour ce système. Jusqu'à quatre sessions sont prises en charge.
Sessions actives	Nombre de sessions actuelles sur le système, inférieur ou égal au **Nombre maximal de sessions**.
Délai d'attente	Délai d'expiration Secure Shell en secondes. Plage = 60 à 1 920 secondes. Saisissez 0 seconde pour désactiver la fonctionnalité Délai d'expiration. Le paramètre par défaut est 300.
Numéro de port	Port utilisé par le DRAC pour une connexion serveur. Le paramètre par défaut est 22.

Tableau 11-10. Paramètres Telnet

Paramètre	Description
Activé	Active ou désactive Telnet. Coché = Activé ; Décoché = Désactivé.
Nombre maximal de sessions	Nombre maximal de sessions simultanées autorisées pour ce système. Jusqu'à quatre sessions sont prises en charge.
Sessions actives	Nombre de sessions actuelles sur le système, inférieur ou égal au **Nombre maximal de sessions**.
Délai d'attente	Délai d'expiration Secure Shell en secondes. Plage = 60 à 1 920 secondes. Saisissez 0 seconde pour désactiver la fonctionnalité Délai d'expiration. Le paramètre par défaut est 0.
Numéro de port	Port utilisé par le DRAC pour une connexion serveur. Le paramètre par défaut est 23.

Tableau 11-11. Paramètres RACADM distante

Paramètre	Description
Activé	Active ou désactive la RACADM distante. Coché = Activé ; Décoché = Désactivé.
Nombre maximal de sessions	Nombre maximal de sessions simultanées autorisées pour ce système. Jusqu'à quatre sessions sont prises en charge.
Sessions actives	Nombre de sessions actuelles sur le système, inférieur ou égal au **Nombre maximal de sessions**.

Tableau 11-12. 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 11-13. Paramètre de l'agent de récupération de système automatique

Paramètre	Description
Activé	Active l'agent de récupération de système automatique.

Tableau 11-14. 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 supplémentaires du DRAC 5

Pour empêcher tout accès non autorisé à votre système distant, le DRAC 5 fournit les fonctionnalités suivantes :

- Filtrage des adresses IP (IPRange) : définit une plage spécifique d'adresses IP auxquelles peut accéder le DRAC 5.
- 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 du DRAC 5. 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 au DRAC 5 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 au DRAC 5. 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 de propriétés du DRAC 5 » pour une liste complète des propriétés **cfgRacTune**.

Tableau 11-15. 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 DRAC 5. 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 le DRAC 5.
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), utilisent 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 quand un nombre excessif d'échecs d'ouverture de session se produit à partir d'une adresse IP particulière et bloque (ou empêche) l'adresse d'ouvrir une session sur le DRAC 5 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 : identification d'échange ssh : connexion fermée par l'hôte distant.

Voir « Définitions des groupes et des objets de la base de données de propriétés du DRAC 5 » pour une liste complète des propriétés **cfgRacTune**.

Tableau 11-16 répertorie les paramètres définis par l'utilisateur.

Tableau 11-16. 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.
crgRacTuneIpBlkPenaltyTime	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 du DRAC 5

REMARQUE : Vous devez avoir le droit **Configurer le DRAC 5** 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**.

   Tableau 11-17 décrit les paramètres de la page **Sécurité réseau**.
5. Cliquez sur le bouton approprié de la page **Sécurité réseau** pour continuer. Voir Tableau 11-18 pour une description des boutons de la page **Sécurité réseau**.

Tableau 11-17. Paramètres de la page Sécurité réseau

Paramètres	Description
Plage IP activée	Active la fonctionnalité de contrôle de plage IP, qui définit une plage spécifique d'adresses IP pouvant accéder au DRAC 5.
Adresse de la plage IP	Détermine l'adresse de sous-réseau IP acceptée.
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 11-18. 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 à la page su sommaire

Retour à la page su sommaire

Utilisation de l'interface de ligne de commande SM-CLP du DRAC 5

Dell™ Remote Access Controller 5 Guide d'utilisation de la version 1.45 du micrologiciel

Cette section fournit des informations sur le protocole de ligne de commande Server Management (SM-CLP) du groupe de travail Server Management (SMWG) qui est intégré au DRAC 5.

REMARQUE : Cette section suppose que vous connaissez l'initiative SMASH (Systems Management Architecture for Server Hardware) et les spécifications SMWG 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**.

La SM-CLP du DRAC 5 est un protocole régi par DMTF et SMWG pour fournir des normes aux implémentations de la CLI de gestion de systèmes. La SM-CLP SMWG est un sous-composant de l'ensemble des efforts SMASH effectués par DMTF.

Prise en charge de SM-CLP du DRAC 5

Le DRAC 5 est le premier produit RAC qui fournit la prise en charge du protocole de ligne de commande basé sur la norme SM-CLP. La SM-CLP est hébergée par le micrologiciel du contrôleur du DRAC 5 et prend en charge les interfaces telnet, SSH et série. L'interface SM-CLP du DRAC 5 est basée sur la spécification SM-CLP, version 1.0, fournie par l'organisation DMTF.

Les sections suivantes fournissent un aperçu de la fonctionnalité SM-CLP qui est hébergée par le DRAC 5.

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, l'utilisateur peut effectuer des opérations à l'aide des verbes énumérés dans Tableau 12-1 et Tableau 12-2.

Tableau 12-1. Verbes CLI pris en charge pour le système

Verbe	Définition
cd	Navigue dans MAP à l'aide de l'environnement.
delete	Supprime une instance d'objet.
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.

Tableau 12-2. Verbes CLI pris en charge pour les ventilateurs, les batteries, l'intrusion, les performances matérielles, les blocs d'alimentation, les températures et les tensions

Verbe	Définition
cd	Navigue dans MAP à l'aide de l'environnement.
help	Affiche l'aide pour une cible spécifique.
show	Affiche les propriétés, les verbes et les sous-cibles de la cible.
exit	Quitte la session d'environnement SM-CLP.
version	Affiche les attributs de version d'une cible.

Utilisation de SM-CLP

1. SSH (ou telnet) au DRAC 5 avec les bonnes références.
2. À l'invite de commande, tapez `smclp`.

   L'invite SMCLP (->) est affichée.

Opérations de gestion et cibles SM-CLP

Opérations de gestion

La SM-CLP du DRAC 5 permet aux utilisateurs de gérer ce qui suit :

- Gestion de l'alimentation du serveur : met sous tension, arrête ou redémarre le système
- Gestion du journal des événements système (SEL) : affiche ou efface les enregistrements du journal SEL

Options

Tableau 12-3 répertorie les options SM-CLP prises en charge.

Tableau 12-3. Options SM-CLP prises en charge

Option SM-CLP	Description
-all	Donne l'ordre au verbe d'effectuer toutes les fonctionnalités possibles.
-display	Affiche les données définies par l'utilisateur.
-examine	Donne l'ordre au processeur de commandes de valider la syntaxe de commande sans exécuter la commande.
-help	Affiche l'aide du verbe de commande.
-version	Affiche la version du verbe de commande.

Cibles

Tableau 12-4 fournit une liste des cibles fournies par la SM-CLP pour prendre en charge ces opérations.

Tableau 12-4. Cibles SM-CLP

Cible	Définition
/system1	Cible du système géré.
/system1/logs1	Cible des collections de journal
/system1/logs1/log1	Cible du journal des événements système (SEL) sur le système géré.
/system1/logs1/log1/ record1	Instance d'enregistrement SEL individuelle sur le système géré.
/system1/pwrmgtsvc1	Le service de gestion de l'alimentation pour le système.
/system1/pwrmgtsvc1/ pwrmgtcap1	Capacités du service de gestion de l'alimentation pour le système.
/system1/fan1	Une cible de ventilateur sur le système géré.
/system1/fan1/ pateurtach1	Une seule cible de capteur sur la cible de ventilateur sur le système géré.
/system1/batteries1	Une cible de batterie sur le système géré.
/system1/batteries1/ capteur1	Une seule cible de capteur sur la cible de batterie sur le système géré.
/system1/intrusion1	Une cible d'intrusion de châssis sur le système géré.
/system1/intrusion1/ capteur1	Une seule cible de capteur sur la cible d'intrusion de châssis sur le système géré.
/system1/hardwareperformance1	Une cible de performances matérielles sur le système géré.
system1/hardwareperformance1/sensor1	Une seule cible de capteur sur la cible de performances matérielles sur le système géré.
/system1/powersupplies1	Une cible de bloc d'alimentation sur le système géré.
/system1/powersupplies1/sensor1	Une seule cible de capteur sur la cible de bloc d'alimentation sur le système géré.
/system1/temperatures1	Une cible de température sur le système géré.
/system1/temperatures1/tempsensor1	Une seule cible de capteur sur la cible de température sur le système géré.
/system1/voltages1	Une cible de tension sur le système géré.

/system1/voltages1/voltsensor1	Une seule cible de capteur sur la cible de tension sur le système géré.
/system1/chassis1	Une seule cible de châssis du système.

Format de sortie SM-CLP

Le DRAC 5 prend actuellement en charge la sortie basée sur le texte comme décrit dans les spécifications de la SM-CLP.

Exemples de SM-CLP du DRAC 5

Les sous-sections suivantes fournissent des exemples de scénario concernant l'utilisation de la SM-CLP pour effectuer les opérations suivantes :

- Gestion de l'alimentation du serveur
- Gestion du journal SEL
- Navigation de la cible MAP
- Affichage des propriétés système

Gestion de l'alimentation du serveur

Tableau 12-5 fournit des exemples d'utilisation de la SM-CLP pour effectuer des opérations de gestion de l'alimentation sur un système géré.

Tableau 12-5. Opérations de gestion de l'alimentation du serveur

Opération	Syntaxe
Ouverture d'une session sur le RAC à l'aide de l'interface telnet/SSH	>ssh 192.168.0.120 >login: root -password
Démarrage de l'environnement de gestion SM-CLP	- >smclp DRAC 5 SM-CLP System Management Shell, version 1.0 Copyright (c) 2004-2008 Dell, Inc. Tous droits réservés ->
Mettre le serveur hors tension	- ->stop /system1 system1 a été correctement arrêté
Mettre le serveur sous tension à partir de l'état hors tension	- ->start /system1 system1 a été correctement démarré
Redémarrer le serveur	->reset /system1 system1 a été correctement réinitialisé

Gestion du journal SEL

Tableau 12-6 fournit des exemples d'utilisation de la SM-CLP pour effectuer des opérations SEL sur le système géré.

Tableau 12-6. Opérations de gestion du journal SEL

Opération	Syntaxe
Affichage du journal SEL	->show /system1/logs1/log1 /system1/logs1/log1 Targets: Record1 Record2 Record3 Record4 Record5 Properties: InstanceID = IPMI:BMC1 SEL Log MaxNumberOfRecords = 512 CurrentNumberOfRecords = 5 Name = IPMI SEL EnabledState = 2 OperationalState = 2 HealthState = 2 Caption = IPMI SEL

	Description = IPMI SEL ElementName = IPMI SEL Commands: cd show help exit version
Affichage de l'enregistrement du journal SEL	->show /system1/logs1/log1/record4 system1/logs1/log1/record4 Properties: LogCreationClassName = CIM_RecordLog CreationClassName = CIM_LogRecord LogName = IPMI SEL RecordID = 1 MessageTimeStamp = 20050620100512.000000-000 Description = FAN 7 RPM: fan sensor, detected a failure ElementName = IPMI SEL Record Commands: cd show help exit version
Effacement du journal SEL	->delete /system1/logs1/log1/record* All records deleted successfully

Gestion des batteries

Tableau 12-7 donne un exemple d'utilisation de SM-CLP pour effectuer des opérations sur les batteries.

Tableau 12-7. Opérations de gestion des batteries

Opération	Syntaxe
Affichage de l'état des batteries	->show system1/batteries1/sensor1 /system1/batteries1/sensor1: Properties: SystemCreationClassName = CIM_ComputerSystem SystemName = F196P1S CreationClassName = CIM_Sensor DeviceID = BATTERY 1 SensorType = 1 PossibleStates = {"Good" "Bad" "Unknown"} CurrentState = good ElementName = System Board CMOS Battery OtherSensorTypeDescription = CMOS battery sensor. EnabledState = 1 Verbs: cd exit help show version

Navigation de la cible MAP

Tableau 12-8 fournit des exemples d'utilisation du verbe **cd** pour naviguer dans MAP. Dans tous les exemples, la cible par défaut initiale est supposée être /.

Tableau 12-8. Opérations de navigation de la cible MAP

Opération	Syntaxe

Naviguer vers la cible système et redémarrez	`->cd system1`
	`->reset`
	
	REMARQUE : La cible par défaut actuelle est /.

Naviguer vers la cible SEL et afficher les enregistrements du journal	`->cd system1`
	`->cd logs1/log1`
	`->show`

	`->cd system1/logs1/log1` `->show`
Afficher la cible actuelle	`->cd .`
Monter d'un niveau	`->cd ..`
Quitter l'environnement	`->exit`

Propriétés système

Le tableau 12-9 énumère les propriétés système qui sont affichées lorsque l'utilisateur tape ce qui suit :

```
show /system1
```

Ces propriétés sont extraites du profil système de base qui est fourni par l'organisme de normalisation et est fondé sur la classe **CIM_ComputerSystem** comme définie par le schéma CIM.

Pour des informations supplémentaires, consultez les définitions du schéma CIM de DMTF.

Tableau 12-9. Propriétés système

Objet	Propriété	Description
CIM_ComputerSystem	Nom	Identifiant unique d'une instance système qui existe dans l'environnement d'entreprise. MaxLen = 256
	ElementName	Nom d'utilisateur convivial du système. MaxLen = 64
	NameFormat	Identifie la méthode de génération du nom. Valeurs : Autre, IP, Numérotation, HID, NWA, HWA, X25, RNIS, IPX, DCC, ICD, E.164, SNA, OID/OSI, WWN, NAA
	Dédié	Énumération indiquant si le système est un système spécial ou un système général. Valeurs : 0=Non dédié 1=Inconnu 2=Autre 3=Stockage 4=Routeur 5=Commutateur 6=Commutateur de couche 3 7= Commutateur CentralOffice 8=Concentrateur 9=Serveur d'accès 10=Pare-feu 11=Imprimer 12=E/S 13=Cache Web 14=Gestion

		15=Serveur de blocs
		16=Serveur de fichiers 17=Périphérique utilisateur mobile 18=Répéteur 19=Pont/Extendeur 20=Passerelle 21=Virtualisateur de stockage 22=Bibliothèque de médias 23=Nud d'extendeur 24=En-tête NAS 25=NAS auto-contenu 26=Onduleur 27=Téléphone IP 28=Contrôleur de gestion 29=Gestionnaire de châssis
	ResetCapability	Définit les méthodes de réinitialisation disponibles sur le système Valeurs : 1=Autre 2=Inconnu 3=Désactivé 4=Activé 5=Non mis en oeuvre
	CreationClassName	Superclasse d'où est extraite cette instance.
	EnabledState	Indique les états activé/désactivé du système. Valeurs : 0=Inconnu 1=Autre 2=Activé 3=Désactivé 4=Arrêt 5=Non applicable 6=Activé mais hors ligne 7=En cours de test 8=Déféré 9 =Acquiescement 10=Démarrage
	EnabledDefault	Indique la configuration de démarrage par défaut pour l'état activé du système. Par défaut, le système est « Activé » (valeur = 2). Valeurs : 2=Activé 3=Désactivé 4=Non applicable 5=Activé mais hors ligne 6=Aucune valeur par défaut
	RequestedState	Indique le dernier état demandé ou souhaité pour le système.

		Valeurs : 2=Activé 3=Désactivé 4=Arrêter 5=Pas de changement 6=Hors ligne 7=Test 8=Déféré 9 =Acquiescement 10=Redémarrer 11=Réinitialiser 12=Non applicable
	HealthState	Indique l'intégrité actuelle du système. Valeurs : 0=Inconnu 5=OK 10=Dégradé/Avertissement 15=Défaillance mineure 20=Défaillance majeure 30=Défaillance critique 35=Erreur irrécupérable
	OperationalStatus	Indique l'état actuel du système. Valeurs : 0=Inconnu 1=Autre 2=OK 3=Dégradé 4=Stressé 5=Défaillance prévue 6=Erreur 7=Erreur irrécupérable 8=Démarrage 9=Arrêt 10=Arrêté 11=En réparation 12=Pas de contact 13=Communication coupée 14=Interrompu 15=Inactif 16=Erreur de l'entité de prise en charge 17=Terminé 18=Mode d'alimentation
	Description	Une description textuelle du système.

Noms de propriété pour les capteurs de ventilateur, de température, de tension numérique, de consommation de puissance et d'intensité de courant

Noms de propriété pris en charge pour les capteurs de ventilateur, de température, de tension numérique, de consommation de puissance et d'intensité du courant

Tableau 12-10. Capteurs

Objet	Propriété	Description
CIM_NumericSensor	SystemCreationClassName	Le nom de la classe de création système : CIM_ComputerSystem
	SystemName	Le numéro de service du système, l'identifiant unique d'un système existant dans l'environnement d'une entreprise
	CreationClassName	Le nom de la classe de création : CIM_NumericSensor
	DeviceID	La référence unique pour le capteur dans le système fan1...n (pour capteur de Tachymètre) temp 1...n (pour capteur de température) numeric voltage 1...n (pour capteur numérique (tension) (Systèmes PMBus uniquement)) power consumption 1...n (pour la consommation de puissance (Systèmes PMBus uniquement)) amperage 1...n (pour l'intensité du courant (systèmes PMBus uniquement))
	BaseUnits	Les unités de mesure du capteur tr/min=Tachymètre (pour capteur Tachymètre) C=Température (pour capteur de température) V=Tension (pour capteur numérique) Watts=Consommation de puissance (pour Consommation de puissance) A= Ampères (pour intensité du courant)
	CurrentReading	La mesure actuelle du capteur.
	LowerThresholdNonCritical	La valeur du seuil minimal non critique
	UpperThresholdNonCritical	La valeur du seuil maximal non critique
	LowerThresholdCritical	La valeur du seuil inférieur critique
	UpperThresholdCritical	La valeur du seuil maximal critique
	SupportedThreshold	Le seuil supporté pour le capteur. { "LowerThresholdCritical" } (pour capteur Tachymètre) { "LowerThresholdNonCritical", "SeuilMaximalNonCritique", "UpperThresholdCritical", "LowerThresholdCritical" } (pour capteur de température) {} (pour capteur de tension (capteur numérique)) {"UpperThresholdNonCritical", "SeuilMaximalCritique"} (pour la consommation de puissance {} pour l'intensité du courant)
	Seuil configurable	Les niveaux de seuil que vous pouvez configurer pour un capteur. { } (pas de prise en charge de capteur pour paramétrer les valeurs de seuil)
	SensorTypes	Type de sensor : 5=Tachymètre (pour tachsensor) 2=Température (pour température) 3=Tension (pour tension) 1=Consommation de puissance (pour powerconsumption) 1=Intensité courant (pour intensité du courant)
	PossibleStates	Les états possibles du capteur. { "inconnu", "avertissement", "a échoué", "irrécupérable" }
	ÉtatActuel	L'état actuel comme indiqué par le capteur
	ElementName	Le nom du capteur
	OtherSensorTypeDescription	Si la propriété du type de capteur contient la valeur "1" (autres), cette propriété donne une description supplémentaire du capteur. "Power consumption sensor." pour consommation de puissance "Amperage sensor." pour intensité du courant
	EnabledState	Indique si le capteur est activé ou désactivé. 1=Activé

Noms de propriété pour Capteurs de bloc d'alimentation

Tableau 12-11. Noms de propriété pris en charge pour Capteurs de bloc d'alimentation

Objet	Propriété	Description
CIM_NumericSensor	SystemCreationClassName	Le nom de la classe de création système : CIM_ComputerSystem
	SystemName	Le numéro de service du système, l'identifiant unique d'un système existant dans l'environnement d'une entreprise
	CreationClassName	Le nom de la classe de création : CIM_PowerSupply
	DeviceID	La référence unique pour le capteur dans le système blocalim1...n
	TotalOutputPower	La puissance de sortie totale comme indiquée sur l'interface utilisateur DRAC
	ElementName	Nom du capteur spécifique.
	OperationalStatus	Condition opérationnelle actuelle de l'unité d'alimentation.
	HealthState	L'état d'intégrité du bloc d'alimentation.
	EnabledState	Indique si le capteur est activé ou désactivé. 1=Activé

Noms de propriété pour les capteurs d'intrusion, de batterie, de tension du courant et de performances matérielles

Tableau 12-12. Noms de propriété prise en charge pour les capteurs d'intrusion, de batterie, de tension du courant et de performances matérielles

Objet	Propriété	Description
CIM_NumericSensor	SystemCreationClassName	Le nom de la classe de création système : CIM_ComputerSystem
	SystemName	Le numéro de service du système, l'identifiant unique d'un système existant dans l'environnement d'une entreprise
	CreationClassName	Le nom de la classe de création : CIM_Sensor
	DeviceID	La référence unique pour le capteur dans le système Intrusion1...n (pour capteur d'intrusion) Battery1...n (pour capteur de batterie) Voltage1...n (pour capteur de tension) Hardware performance sensor1...n (pour capteur de performances matérielles)
	TypeCapteur	1=Autre 3=Tension (pour capteur de tension)
	PossibleStates	Les états possibles du capteur { "pas d'intrusion", "intrusion dans le châssis," "intrusion dans la baie du lecteur," "intrusion de la zone de la carte E/S," "intrusion dans la zone du processeur," "déconnexion du LAN," "connexion non autorisée," "intrusion dans la zone VENTILATEUR" } (pour le capteur d'intrusion) { "absent," "faible," "a échoué," "en bon état" } (pour le capteur de batterie) { "en bon état," "en mauvais état," "état inconnu" } (pour le capteur de tension) { "Normal," "Autres," "Protection thermique," "Capacité de refroidissement modifiée," "Capacité d'alimentation modifiée," "Configuration utilisateur" } (pour capteur de performances matérielles)
	ÉtatActuel	État actuel indiqué par le capteur.
	ElementName	Le nom du capteur
	OtherSensorTypeDescription	Si la propriété du type de capteur contient la valeur "1" (autres), cette propriété donne une description supplémentaire du capteur. "Chassis intrusion sensor" (pour capteur d'intrusion) "CMOS battery sensor" (pour capteur de batterie) "Hardware performance sensor" (pour performances matérielles)
	EnabledState	Indique si le capteur est activé ou désactivé. 1=Activé (pour tous les capteurs)

Noms de propriété pour les capteurs de kit de redondance du ventilateur et du bloc d'alimentation

Tableau 12-13. Noms de propriété pris en charge pour les capteurs de kit de redondance du ventilateur et du bloc d'alimentation

Objet	Propriété	Description
CIM_RedundancySet	InstanceID	Numéro d'instance
	RedundancyStatus	L'état de la redondance.
	TypeOfSet	3=Charge équilibrée (pour redondance ventilateur) 4=Modérée (pour redondance bloc d'alimentation)
	MinNumberNeeded	0=Inconnu
	ElementName	Le nom du capteur

Noms de propriété pour les capteurs de châssis

Tableau 12-14. Noms de propriété prise en charge pour les capteurs de châssis

Objet	Propriété	Description
CIM_Chassis	CreationClassName	Le nom de la classe de création : CIM_Chassis
	PackageType	Type de progiciel 3=Châssis
	ChassisPackageType	Type de progiciel de châssis 17=Châssis système principal
	Fabricant	Fabricant "Dell"
	Model	Le nom du modèle du système d'exploitation.
	ElementName	Nom de l'élément

Noms de propriété pour me service de gestion de l'alimentation

Tableau 12-15. Noms de propriété prise en charge pour le service de gestion de l'alimentation

Objet	Propriété	Description
CIM_PowerManagementService	CreationClassName	Le nom de la classe de création système : CIM_PowerManagementService
	Nom	Service d'alimentation IPMI
	ElementName	Service de gestion de l'alimentation du serveur Dell
	powerstate	État actuel de l'alimentation du système. 2=Allumé 6=Éteint Peut être configuré aux valeurs suivantes : 2=Allumer l'alimentation 6=Eteindre l'alimentation 5=Réinitialiser l'alimentaiton 9=Lancer un cycle d'alimentation du système

En utilisant le verbe défini, vous pouvez régler l''état de l'alimentation du système. par exemple, pour allumer le système si celui-ci est éteint :

```
set powerstate=2
```

Noms de propriété pour la fonction alimentation

Tableau 12-16. Noms de propriété prise en charge pour la fonction alimentation

Objet	Propriété	Description
CIM_PowerManagementCapabilities	InstanceID	Référence d'instance unique pour les fonctions d'alimentation
	PowerChangeCapabilities	3=État Alimentation Réglable
	ElementName	Service de gestion de l'alimentation du serveur Dell

	PowerStatesSupported	2=Allumer l'alimentation 6=Eteindre l'alimentation 5=Réinitialiser l'alimentaiton 9=Lancer un cycle d'alimentation du système

Retour à la page su sommaire

Retour à la page su sommaire

Surveillance et gestion des alertes

Dell™ Remote Access Controller 5 Guide d'utilisation de la version 1.45 du micrologiciel

Cette section explique comment surveiller le DRAC 5 et les procédures pour configurer votre système et le DRAC 5 pour recevoir des alertes.

Configuration du système géré pour la saisie de l'écran de la dernière panne

Pour que le DRAC 5 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'utilisation 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 hors tension.

Désactivation de l'option Redémarrage automatique de Windows

Pour que la fonctionnalité d'écran de la dernière panne de l'interface Web du DRAC 5 soit opérationnelle, désactivez l'option **Redémarrage automatique** des systèmes gérés qui exécutent les systèmes d'exploitation Microsoft Windows Server 2003 et Windows 2000 Server.

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.

Désactivation de l'option Redémarrage automatique dans Windows 2000 Server

1. Ouvrez le **Panneau de configuration** de Windows et double-cliquez sur l'icône **Système**.

2. Cliquez sur l'onglet **Avancé**.

3. Cliquez sur le bouton **Démarrage et récupération...**

4. Décochez la case **Redémarrage automatique**.

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, la réduction de puissance et le déclenchement d'une alerte (interruption des événements sur plate-forme [PET] et/ou e-mail).

Les événements sur pla-teforme pouvant être filtrés incluent :

- Panne de sonde de ventilateur
- Avertissement des sondes de batterie
- Panne de sonde de batterie
- Panne de la sonde de tension discrète
- Avertissement des sondes de température
- Panne de sonde de température
- Détection d'une intrusion dans le châssis
- Dégradation de la redondance
- Perte de la redondance
- Avertissement concernant un processeur
- Panne de processeur
- Processeur absent
- Avertissement concernant PS/VRM/D2D
- Panne de PS/VRM/D2D
- Bloc d'alimentation absent
- Erreur dans le journal du matériel
- Récupération automatique du système
- Avertissement de sonde de puissance système
- Panne de sonde de puissance système

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 (ex. : 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 via l'interface utilisateur Web

1. Ouvrez une session sur le système distant à l'aide d'un navigateur Web pris en charge. Voir « Accès à l'interface Web ».
2. Cliquez sur l'onglet **Gestion des alertes** puis sur **Événements sur plate- forme**.
3. Activez les alertes globales.
   a. Cliquez sur **Gestion des alertes** et sélectionnez **Événements sur plate- forme**.
   b. Cochez la case **Activer les alertes de filtre d'événements sur plate- forme**.
4. Dans **Configuration des filtres d'événements sur plate-forme**, cochez la case **Activer les alertes de filtre d'événements sur plate-forme** et cliquez sur **Appliquer les modifications**.
5. Dans **Liste des filtres d'événements sur plate-forme**, cliquez sur le filtre que vous voulez configurer.
6. Sur la page **Définir les événements sur plate-forme**, effectuez les sélections appropriées puis cliquez sur **Appliquer les modifications**.

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

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 17. 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 -i <index> -o cfgIpmiPefAction <action>
   ```

   où les bits des valeurs <*action*> sont les suivants :

   - bit de valeur <*action*> 0 - 1 = action d'activation d'alerte, 0 = désactivation d'alerte
   - bit de valeur <*action*> 1 - 1 = mise hors tension ; 0 = pas de mise hors tension
   - bit de valeur <*action*> 2 - 1 = redémarrage ; 0 = pas de redémarrage
   - bit de valeur <*action*> 3 - 1 = cycle d'alimentation ; 0 = pas de cycle d'alimentation
   - bit de valeur <*action*> 4 - 1 = réduction de puissance ; 0 = pas de réduction de puissance

   Par exemple, pour activer le PEF pour redémarrer le système, 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

1. Ouvrez une session sur le système distant à l'aide d'un navigateur Web pris en charge. Voir « Accès à l'interface Web ».
2. Assurez-vous d'avoir bien suivi les procédures dans « Configuration du PEF via l'interface utilisateur Web ».
3. Configurez votre règle PET.
   a. Dans l'onglet **Gestion des alertes**, cliquez sur **Paramètres d'interruptions**.
   b. Dans **Paramètres de configuration de la destination**, configurez le champ **Chaîne de communauté** avec les informations appropriées puis cliquez sur **Appliquer les modifications**.
4. Configurez votre adresse IP de destination PET.
   a. Dans la colonne **Numéro de destination**, cliquez sur un numéro de destination.
   b. Vérifiez si la case **Activer la destination** est cochée.
   c. Dans le champ **Adresse IP de destination**, tapez une adresse IP de destination PET valide.
   d. Cliquez sur **Appliquer les modifications**.
   e. Cliquez sur **Envoyer l'interruption test** pour tester l'alerte configurée (si nécessaire).

   REMARQUE : Votre compte utilisateur doit avoir le droit **Tester les alertes** pour effectuer cette procédure. Reportez-vous à la section Tableau 5-4.

   f. Répétez les étapes a à e pour les autres numéros de destination.

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 :

   ```
   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -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 :

   ```
   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertEnable -i 4 0
   ```

3. Configurez votre règle PET.

   À l'invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

   ```
   racadm config -g cfgIpmiPet -o cfgIpmiPetAlertDestIPAddr -i 1 <Adresse_IP>
   ```

   où `1` est l'index de destination PET et *<adresse_IP>* l'adresse IP de destination du système qui reçoit les alertes d'événement sur plate-forme.

4. Configurez la chaîne Nom de communauté.

   À l'invite de commande, tapez :

   ```
   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

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

2. Assurez-vous d'avoir bien suivi les procédures dans « Configuration du PEF via l'interface utilisateur Web ».

3. Configurez vos paramètres d'alerte par e-mail.
   a. Dans l'onglet **Gestion des alertes**, cliquez sur **Paramètres d'alertes par e-mail**.
   b. Sous les **paramètres Adresse du serveur SMTP (e-mail)**, configurez le champ **Adresse IP du serveur SMTP (e-mail)** avec les informations appropriées puis cliquez sur **Appliquer les modifications**.

4. Configurez votre destination d'alerte par e-mail.
   a. Dans la colonne **Numéro d'alerte par e-mail**, cliquez sur un numéro d'alerte par e-mail.
   b. Vérifiez si la case **Activer l'alerte par e-mail** est cochée.
   c. Dans le champ **Adresse e-mail de destination**, tapez une adresse e- mail valide.
   d. Dans le champ **Description de l'e-mail**, saisissez une description (si nécessaire).
   e. Cliquez sur **Appliquer les modifications**.
   f. Cliquez sur **Envoyer l'e-mail test** pour tester l'alerte par e-mail configurée (si nécessaire).

   REMARQUE : Votre compte utilisateur doit avoir le droit **Tester les alertes** pour effectuer cette procédure. Reportez-vous à la section Tableau 5-4.

   g. Répétez étape a à étape e pour les paramètres d'alerte par e-mail restants.

5. Activez les alertes globales.
   a. Cliquez sur **Gestion des alertes** et sélectionnez **Événements sur plate- forme**.
   b. Cochez la case **Activer les alertes de filtre d'événements sur plate- forme**.

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 d'e-mail et *<message_personnalisé>* le message personnalisé.

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 « **testemail** » pour configurer ces paramètres.

Questions les plus fréquentes

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 DRAC 5 est public. Lorsqu'IT Assistant envoie une requête de définition, l'agent DRAC 5 génère une erreur d'authentification SNMP car il accepte uniquement les requêtes de la **communauté = public**.

Vous pouvez changer le nom de communauté du DRAC 5 avec RACADM.

Pour afficher le nom de communauté du DRAC 5, utilisez la commande suivante :

```
racadm getconfig -g cfgOobSnmp
```

Pour définir le nom de communauté du DRAC 5, utilisez la commande suivante :

racadm config -g cfgOobSnmp -o cfgOobSnmpAgentCommunity <*nom de communauté*>

Pour éviter de générer des interruptions d'authentification SNMP, vous devez saisir des noms de communauté qui seront acceptés par l'agent. Comme le DRAC 5 n'accepte qu'un seul nom de communauté, vous devez utiliser le même nom de communauté **get** et **set** pour configurer les découvertes sous IT Assistant.

Retour à la page su sommaire

Retour à la page su sommaire

Configuration de l'interface de gestion de plate-forme intelligente (IPMI)

Dell™ Remote Access Controller 5 Guide d'utilisation de la version 1.45 du micrologiciel

---

Configuration d'IPMI

Cette section fournit des informations sur la configuration et l'utilisation de l'interface IPMI du DRAC 5. L'interface comprend :

- IPMI sur le LAN
- IPMI sur série
- Série sur LAN

Le DRAC 5 est compatible IPMI 2.0. Vous pouvez configurer l'IPMI du DRAC en utilisant :

- votre navigateur
- un utilitaire Open Source comme *ipmitool*
- l'environnement IPMI de Dell OpenManage, *ipmish*
- la RACADM

Pour plus d'informations sur l'utilisation de l'environnement IPMI, ipmish, consultez le *Guide d'utilisation du contrôleur BMC de Dell OpenManage*™ sur le site Web de support de Dell à l'adresse **support.dell.com**.

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

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

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'IPMI du DRAC 5 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.

Configuration d'IPMI à l'aide de la CLI RACADM

1. Ouvrez une session sur le système distant à l'aide d'une des interfaces RACADM. Voir « Utilisation de la RACADM à distance ».

2. Configurez IPMI sur LAN.

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

```
racadm config -g cfgIpmiLan -o cfgIpmiLanEnable 1
```

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

a. Mettez à jour les privilèges du canal IPMI.

À l'invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

```
racadm config -g cfgIpmiLan -o cfgIpmiLanPrivilegeLimit <niveau>
```

où <*niveau*> correspond à :

- 2 (utilisateur)
- 3 (opérateur)
- 4 (administrateur)

Par exemple, pour définir le privilège 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'IPMI du DRAC 5 prend en charge le protocole RMCP+. Pour plus d'informations, consultez les spécifications d'IPMI 2.0.

À l'invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

```
racadm config -g cfgIpmiLan -o cfgIpmiEncryptionKey <clé>
```

où *<clé>* est une clé de cryptage à 20 caractères au format hexadécimal valide.

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

   À l'invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

   ```
   racadm config -g cfgIpmiSol -o cfgIpmiSolEnable 1
   ```

   a. Mettez à jour le niveau de privilège minimum d'IPMI SOL.

PRÉCAUTION : 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.

À l'invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

```
racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege <niveau>
```

où <*niveau*> correspond à :

- 2 (utilisateur)
- 3 (opérateur)
- 4 (administrateur)

Par exemple, pour configurer les privilèges IPMI sur 2 (utilisateur), tapez la commande suivante :

```
racadm config -g cfgIpmiSol -o cfgIpmiSolMinPrivilege 2
```

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

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

À l'invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

```
racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate <débit_en_bauds>
```

où *<débit_en_bauds>* est égal à 9600, 19200, 57600 ou 115200 b/s.

Par exemple :

```
racadm config -g cfgIpmiSol -o cfgIpmiSolBaudRate 57600
```

c. Activez le SOL.

REMARQUE : Le SOL peut être activé ou désactivé pour chaque utilisateur individuel.

À l'invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

```
racadm config -g cfgUserAdmin -o cfgUserAdminSolEnable -i <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.

   À l'invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

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

   b. Configurez le débit en bauds 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.

À l'invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

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

d. Configurez le niveau de privilège minimum de canal IPMI série.

À l'invite de commande, tapez la commande suivante et appuyez sur <Entrée> :

```
racadm config -g cfgIpmiSerial -o cfgIpmiSerialChanPrivLimit <niveau>
```

où <*niveau*> correspond à :

- 2 (utilisateur)
- 3 (opérateur)
- 4 (administrateur)

Par exemple, pour configurer les privilèges 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.
- 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.

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 commande, tapez :

   ```
   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 de propriétés du DRAC 5 ».

Configuration de la communication série sur LAN

REMARQUE : Pour plus d'informations sur la communication série sur LAN, consultez le *Guide d'utilisation du contrôleur de gestion de la carte mère de Dell OpenManage*.

1. Développez l'arborescence du **système** et cliquez sur **Accès distant**.
2. Cliquez sur l'onglet **Configuration**, puis sur **Communication série sur LAN**.
3. Configurez les paramètres Communication série sur LAN.

   Tableau 14-1 fournit des informations sur les paramètres de la page **Configuration de la communication série sur LAN**.
4. Cliquez sur **Appliquer les modifications**.
5. Configurez les paramètres avancés, si nécessaire. Sinon, cliquez sur le bouton approprié de la page **Configuration de la communication série sur LAN** pour continuer (voir Tableau 14-2).

   Pour configurer les paramètres avancés :

   a. Cliquez sur **Paramètres avancés**.

   b. Sur la page **Paramètres avancés de la configuration de la communication série sur LAN**, configurez les paramètres avancés, si nécessaire. Reportez-vous à la section Tableau 14-3.

   c. Cliquez sur **Appliquer les modifications**.

   d. Cliquez sur le bouton approprié de la page **Paramètres avancés de la configuration de la communication série sur LAN** pour continuer. Voir Tableau 14-4 ou la description des boutons de la page **Paramètres avancés de la configuration de la communication série sur LAN**.

Tableau 14-1. Paramètres de la page Configuration de la communication série sur LAN

Paramètre	Description
Activer la connexion série sur le réseau local	Active la communication série sur LAN. Coché = Activé ; Décoché = Désactivé.
Débit en bauds	Vitesse de transmission des données IPMI. Sélectionnez **9600 b/s**, **19,2 kb/s**, **57,6 kb/s** ou **115,2 kb/s**.
Limite du niveau de privilège du canal	Définit le privilège d'utilisateur minimum de la communication IPMI série sur LAN : **Administrateur**, **Opérateur** ou **Utilisateur**.

Tableau 14-2. Boutons de la page Configuration de la communication série sur LAN

Bouton	Description
Imprimer	Imprime la page **Configuration de la communication série sur LAN**.
Actualiser	Actualise la page **Configuration de la communication série sur LAN**.
Paramètres avancés	Ouvre la page **Paramètres avancés de la configuration de la communication série sur LAN**.
Appliquer les modifications	Applique les paramètres de la page **Configuration de la communication série sur LAN**.

Tableau 14-3. Paramètres de la page Paramètres avancés de la configuration de la communication série sur LAN

Paramètre	Description
Intervalle d'accumulation des caractères	Quantité de temps que le BMC attend avant de transmettre un progiciel de données de caractère SOL partiel. Incréments de 5 ms de 1.
Seuil d'envoi des caractères	Le BMC envoie un progiciel de données de caractère SOL contenant les caractères dès que ce nombre de caractères (ou supérieur) a été accepté. Unités de 1.

Tableau 14-4. Boutons de la page Paramètres avancés de la configuration de la communication série sur LAN

Bouton	Description
Imprimer	Imprime la page **Paramètres avancés de la configuration de la communication série sur LAN**.
Actualiser	Actualise la page **Paramètres avancés de la configuration de la communication série sur LAN**.
Retour à la page Configuration de la communication série sur LAN	Retourne à la page **Configuration de la communication série sur LAN**.
Appliquer les modifications	Applique les paramètres de la page **Paramètres avancés de la configuration de la communication série sur LAN**.

Retour à la page su sommaire

Retour à la page su sommaire

Récupération et dépannage du système géré

Dell™ Remote Access Controller 5 Guide d'utilisation de la version 1.45 du micrologiciel

Cette section explique comment utiliser l'interface Web du DRAC 5 pour effectuer les tâches de récupération et de dépannage d'un système distant qui est tombé en panne.

- « Premières étapes de dépannage d'un système distant »
- « Gestion de l'alimentation d'un système distant »
- « Utilisation du journal des événements système (SEL) »
- « 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 ou est- il tombé en panne ou 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 (voir « Taux de rafraîchissement des résolutions d'écran prises en charge sur le système géré ») 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

Le DRAC 5 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.

Utilisez la page **Gestion de l'alimentation** pour effectuer ce qui suit :

- Effectuer un arrêt normal via le système d'exploitation lors du redémarrage et mettre sous tension puis hors tension le système.
- Afficher l'**état actuel de l'alimentation** du système, soit **ACTIVÉ** ou **DÉSACTIVÉ**.

Pour accéder à la page **Gestion de l'alimentation** à partir de l'arborescence **Système**, cliquez sur **Système** puis sur l'onglet **Gestion de l'alimentation**.

REMARQUE : Vous devez avoir le droit **Exécuter les commandes d'action du serveur** pour effectuer les actions de gestion de l'alimentation.

Sélection des actions de contrôle de l'alimentation depuis la GUI du DRAC 5

1. Sélectionnez l'une des **actions de contrôle de l'alimentation** suivantes.
   - **Mettre le système sous tension** : met le système sous tension (équivaut à appuyer sur le bouton d'alimentation quand le système est hors tension).
   - **Mettre le système hors tension** : met le système hors tension (équivaut à appuyer sur le bouton d'alimentation quand le système est sous tension).
   - **Réinitialiser le système** : réinitialise le système (équivaut à appuyer sur le bouton de réinitialisation) ; l'alimentation n'est pas coupée si vous utilisez cette fonction.
   - **Exécuter un cycle d'alimentation sur le système** : met hors tension, puis redémarre (à froid) le système.
2. Cliquez sur **Appliquer** pour effectuer l'action de gestion de l'alimentation (par exemple, provoquer un cycle d'alimentation sur le système).
3. Cliquez sur le bouton approprié de la page **Gestion de l'alimentation** pour continuer (voir Tableau 15-1).

Tableau 15-1. Boutons de la page Gestion de l'alimentation (en haut à droite)

Bouton	Action
Imprimer	Imprime la page **Gestion de l'alimentation**
Actualiser	Recharge la page **Gestion de l'alimentation**

Sélection des actions de contrôle de l'alimentation depuis la CLI du DRAC 5

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
- Remote Access Controller
- Contrôleur de gestion de la carte mère

Pour accéder aux informations système, développez l'arborescence **Système** et cliquez sur **Propriétés**.

Châssis principal du système

Tableau 15-2 et le tableau 15-3 décrit 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 du DRAC 5 doivent être installés sur le système géré.

Tableau 15-2. 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 d'hôte	Nom du système hôte.
Nom du système d'exploitation	Système d'exploitation fonctionnant sur le système.

Tableau 15-3. Champs Récupération automatique

Champ	Description
Action de récupération	Lorsqu'un « blocage système » est détecté, le DRAC 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 après la détection d'un « blocage système » à partir duquel le DRAC effectuera une action de récupération.
Compte à rebours actuel	Valeur actuelle, en secondes, du compte à rebours.

Remote Access Controller

Tableau 15-4 décrit les propriétés du Remote Access Controller.

Tableau 15-4. Champs Informations sur le RAC

Champ	Description
Nom	Nom abrégé.
Informations produit	Nom complet.
Version du matériel	Version de la carte Remote Access Controller ou « inconnue ».
Version du micrologiciel	Niveau de la version actuelle du micrologiciel du DRAC 5.
Mise à jour du micrologiciel	Date et heure de la dernière mise à jour du micrologiciel.
Heure du RAC	Paramètre d'horloge du système.

Contrôleur de gestion de la carte mère

Tableau 15-5 décrit les propriétés du contrôleur de gestion de la carte mère.

Tableau 15-5. Champs Informations sur le BMC

Champ	Description
Nom	« Contrôleur de gestion de la carte mère ».
Version d'IPMI	Version de l'interface de gestion de plate-forme intelligente (IPMI).
Nombre de sessions actives possibles	Nombre maximum de sessions pouvant être actives en même temps.
Nombre de sessions actives en cours	Nombre total de sessions actives.
Version du micrologiciel	Version du micrologiciel BMC.
Activé sur le LAN	Activé sur le LAN ou Désactivé sur le LAN.

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 15-6.
3. Cliquez sur le bouton approprié de la page **Journal des événements système** pour continuer (Reportez-vous à la section Tableau 15-7).

Tableau 15-6. Icônes des indicateurs d'état

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 15-7. Boutons de la page SEL

Bouton	Action
Imprimer	Imprime le **journal SEL dans l'ordre de tri qui apparaît dans la fenêtre.**
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.
Actualiser	Recharge la page du **journal SEL**.

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 de saisie POST et de démarrage du système d'exploitation

Cette fonction de DRAC 5 vous permet de lire une vidéo image par image des trois dernières occurences de démarrage du BIOS POST et du système d'exploitation.

Pour afficher les journaux de saisie POST et de démarrage du système d'exploitation :

1. Dans l'arborescence **Système**, cliquez sur **Système**.
2. Cliquez sur **l'onglet** Journaux, puis sur l'onglet **Saisie de démarrage**.
3. Sélectionnez le numéro de journal du POST ou le journal de la saisie de démarrage du système d'exploitation.

   La vidéo des journaux est lue sur le nouvel écran.
4. Cliquez sur **Arrêter** pour arrêter la vidéo.

Affichage de l'écran de la dernière panne système

PRÉCAUTION : 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 du DRAC. 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 panne la plus récente, qui comprend des informations sur les événements qui se sont produits avant la panne du système. Les informations sur la dernière panne système sont enregistrées dans la mémoire du DRAC 5 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 (consultez Tableau 15-8) en haut à droite de l'écran :

Tableau 15-8. Boutons de la page Écran de la dernière panne

Bouton	Action
Imprimer	Imprime la page **Écran de la dernière panne**.
Enregistrer	Ouvre une fenêtre contextuelle qui vous permet d'enregistrer l'écran de la dernière panne dans le répertoire de votre choix.
Supprimer	Supprime 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 à la page su sommaire

Retour à la page su sommaire

Récupération et dépannage du DRAc 5

Dell™ Remote Access Controller 5 Guide d'utilisation de la version 1.45 du micrologiciel

Cette section explique comment effectuer des tâches liées à la récupération et au dépannage d'un DRAC 5 en panne.

Vous pouvez utiliser un des outils suivants pour dépanner votre DRAC 5 :

- Journal du RAC
- Console de diagnostic
- Journal de suivi
- racdump
- coredump

Utilisation du journal du RAC

Le **journal du RAC** est un journal permanent conservé dans le micrologiciel du DRAC 5. Le journal contient une liste des actions d'utilisateur (ouverture et fermeture de session et modifications des règles de sécurité, par exemple) et des alertes envoyées par le DRAC 5. Les entrées les plus anciennes sont écrasées quand le journal est plein.

Pour accéder au journal du RAC depuis l'interface utilisateur (UI) du DRAC 5 :

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 16-1.

Tableau 16-1. Informations sur la page Journal du RAC

Champ	Description
Date/Heure	Date et heure (par exemple, 19 Déc 16:55:47). Lorsque le DRAC 5 démarre à l'initiale et qu'il ne parvient pas à communiquer avec le système géré, l'heure est affichée comme Démarrage du système.
Source	Interface qui a provoqué l'événement.
Description	Description brève de l'événement et nom d'utilisateur qui a ouvert une session sur le DRAC 5.

Utilisation des boutons de la page Journal du RAC

La page **Journal du RAC** contient les boutons répertoriés dans le tableau 16-2.

Tableau 16-2. 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 avez le 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 du DRAC 5.

```
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

Le DRAC 5 fournit un ensemble standard d'outils de diagnostic réseau (voir Tableau 16-3) semblables aux outils fournis avec les systèmes Microsoft® Windows® ou Linux. À l'aide de l'interface Web du DRAC 5, 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**.

Tableau 16-3 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 16-3. 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 qu'il est possible d'atteindre l'adresse IP de destination à partir du DRAC 5 avec le contenu actuel de la table 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 trace du DRAC 5. Pour plus d'informations, voir « gettracelog ».

Utilisation du journal de suivi

Le journal de suivi interne du DRAC 5 permet aux administrateurs de déboguer les alertes et les problèmes de mise en réseau du DRAC 5.

Pour accéder au journal de suivi depuis l'interface Web du DRAC 5 :

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 de plus amples informations, consultez la section « gettracelog ».

Le journal de suivi enregistre les informations suivantes :

- DHCP : fait 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 du DRAC 5, c'est-à-dire le micrologiciel DRAC 5 interne, et non le système d'exploitation du système géré.

REMARQUE : Le DRAC 5 ne renvoie pas d'ICMP (ping) si le 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 du DRAC 5.

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 coredumpdelete` peut être utilisée pour effacer toutes les données coredump actuellement stockées dans le RAC.

Pour plus d'informations, voir « coredump » et « coredumpdelete ».

Retour à la page su sommaire

Retour à la page su sommaire

Capteurs

Dell™ Remote Access Controller 5 Guide d'utilisation de la version 1.45 du micrologiciel

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 le DRAC 5 pour surveiller le capteur de matériel pour les batteries, les capteurs de ventilateurs, l'intrusion dans le châssis, les blocs d'alimentation, l'alimentation consommée, la température et les tensions.

Sondes de batterie

Les 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 :

- la condition des blocs d'alimentation, qu'ils entrent dans les valeurs de seuil normales ou qu'ils les dépassent.

  REMARQUE : Vous pouvez configurer les valeurs de seuil uniquement à partir de Dell™ OpenManage™ Server Administrator. Voir le *Guide d'utilisation de Dell OpenManage Server Administrator* pour de plus amples informations.

- redondance du bloc d'alimentation, c'est-à-dire la capacité du bloc d'alimentation redondant de remplacer le bloc d'alimentation primaire si celui-ci fonctionne mal.

  REMARQUE : S'il y n'y a qu'un seul bloc d'alimentation dans le système, la section Redondance du bloc d'alimentation ne sera pas affichée.

Sondes de performances matérielles

Le capteur de performances matérielles indique la condition de la performance de votre unité centrale de traitement (UCT), qu'elle soit dégradée ou non. La condition des capteurs de performances matérielles est dégradée lorsque l'UCT est restreinte.

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. Ces informations sont communiquées au DRAC 5 avec les capteurs du micrologiciel du contrôleur de gestion de la carte mère (baseboard management controller - BMC).

REMARQUE : Cette fonction est prise en charge uniquement sur les systèmes limités Dell PowerEdge™ *x*9*xx* and *xx*0*x*.

DRAC 5 offre des fonctionnalités avancées de surveillance de l'alimentation. Cela comprend :

- La représentation graphique du niveau de puissance du système en watts et de l'alimentation électrique en ampères sur une période de temps donnée.
- Les statistiques de consommation de puissance maximale, minimale et moyenne pour le système en watts et en BTU/h (British Thermal Unit per Hour ou unité thermique britannique par heure) au cours de la dernière heure, du dernier jour et de la dernière semaine à partir de l'heure courante du DRAC et ce, sous forme graphique.
- La puissance consommée par le système en watts et le courant moyen consommé par chaque alimentation électrique en ampères.

Informations graphiques

La page **Informations graphiques** affiche les graphiques du niveau de puissance du système en watts et de l'alimentation électrique en ampères sur une période de temps donnée. La page s'actualise automatiquement toutes les minutes.

REMARQUE : Les données sont récupérées par le DRAC 5 toutes les cinq minutes et sont perdues après la réinitialisation du DRAC, un cycle d'alimentation secteur ou une mise à jour de micrologiciel.

REMARQUE : Les graphiques peuvent contenir des trous lors de la mise hors tension du système ou lors de la réinitialisation du BMC. La raison en est que les capteurs d'alimentation sont indisponibles pendant cette période.

La consommation de puissance en watts affiche la période de temps au cours de laquelle les données de puissance sont recueillies. Vous pouvez définir la plage de l'axe des X à 1 heure, 1 jour ou 1 semaine à partir du menu déroulant disponible sur cette page. La période de temps court à partir de l'heure courante définie sur le DRAC. L'axe des Y affiche la puissance consommée par le système en watts.

La consommation de puissance en ampères affiche la période de temps au cours de laquelle les données du courant sont recueillies. Vous pouvez définir la plage de l'axe des X sur 1 heure, 1 jour ou 1 semaine à partir du menu déroulant disponible sur cette page. La période de temps court à partir de l'heure courante du DRAC. L'axe des Y affiche le courant consommé par les alimentations électriques en ampères. Si le système comprend plusieurs unités d'alimentation et que les mesures sont identiques, les graphiques actuels peuvent se chevaucher.

Informations sur la consommation de puissance

La page **Informations sur la consommation de puissance** affiche la puissance consommée par le système en watts et le courant moyen consommé par chaque alimentation électrique en ampères.

Cette page affiche également l'état des sondes, le nom des sondes, la puissance consommée, les seuils minimal et maximal pour la génération des alertes d'avertissement et de panne, l'emplacement de l'unité d'alimentation et le courant moyen consommé par chaque alimentation électrique en ampères.

Statistiques d'alimentation

La page **Statistiques d'alimentation** affiche la consommation électrique moyenne ainsi que les statistiques de consommation électrique maximale et minimale pour le système en watts et en BTU/h (British Thermal Unit per Hour ou unité thermique britannique par heure) au cours de la dernière heure, du dernier jour ou de la dernière semaine à partir de l'heure courante du DRAC. Les données sont récupérées par le DRAC 5 et sont réinitialisées si le DRAC doit être réinitialisé pour quelque raison que ce soit.

Sondes de température

Le capteur de température donne des informations concernant la température ambiante de la carte système. Les sondes de températures indiquent si la condition des sondes entre dans la valeur prédéfinie de seuil critique 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 à la page su sommaire

Retour à la page su sommaire

Familiarisation avec le DRAC 5

Dell™ Remote Access Controller 5 Guide d'utilisation de la version 1.45 du micrologiciel

Le DRAC 5 vous permet de surveiller, dépanner et réparer à distance un système Dell, même lorsque celui-ci est en panne. Le DRAC 5 est doté d'un vaste ensemble de fonctionnalités telles que la redirection de console, le média virtuel, le KVM virtuel, l'authentification par carte à puce, etc.

La station de gestion est le système à partir duquel un administrateur gère à distance un système Dell doté d'une carte DRAC. Les systèmes ainsi surveillés sont des systèmes gérés.

Pour utiliser cette carte DRAC, procédez comme suit :

1. Installez la carte DRAC 5 dans votre système Dell : le DRAC 5 peut avoir été pré-installé sur votre système ou disponible dans un kit séparé.

   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** pour des instructions précises sur la réalisation de cette procédure.

   Vous devez installer le logiciel du DRAC 5 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 le DRAC ne pourra pas capturer l'écran de la dernière panne.

2. Configurez les propriétés, les paramètres réseau et les utilisateurs du DRAC 5 : vous pouvez configurer le DRAC 5 à l'aide de l'utilitaire de configuration de l'accès à distance, de l'interface Web ou de la RACADM.

3. Configurez Microsoft® Active Directory® pour accéder au DRAC 5 afin de pouvoir ajouter et contrôler les privilèges d'utilisateur du DRAC 5 de vos utilisateurs existants dans votre logiciel Active Directory.

4. Configurez l'authentification par carte à puce : la carte à puce offre un niveau accru de sécurité à votre entreprise.

5. Configurez les points d'accès à distance, comme la redirection de console et le média virtuel.

6. Configurez les paramètres de sécurité.

7. Utilisez la gestion standardisée SM-CLP (Server Management-Command Line Protocol) pour gérer les systèmes sur votre réseau.

8. Configurez les alertes pour une gestion efficace des systèmes.

9. Configurez les paramètres de l'interface de gestion de plateforme intelligente de DRAC 5 (IPMI) pour utiliser les outils IPMI standardisés pour gérer les systèmes sur votre réseau.

Retour à la page su sommaire

Retour à la page su sommaire

Installation de base du DRAC 5

Dell™ Remote Access Controller 5 Guide d'utilisation de la version 1.45 du micrologiciel

Cette section fournit des informations pour installer et configurer le matériel et le logiciel de votre DRAC 5.

Avant de commencer

Rassemblez les éléments suivants, fournis avec votre système, avant d'installer et de configurer le logiciel du DRAC 5 :

- Matériel du DRAC 5 (déjà installé ou en kit en option)
- Procédures d'installation du DRAC 5 (situées dans ce chapitre)
- DVD *Dell Systems Management Tools* and Documentation

Installation du matériel du DRAC 5

REMARQUE : La connexion du DRAC 5 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.

Le DRAC 5 peut être préinstallé sur votre système ou disponible séparément sous forme de kit. Pour commencer à utiliser le DRAC 5 installé sur votre système, consultez « Présentation générale de l'installation et de la configuration du logiciel ».

Si votre système n'a pas de DRAC 5, consultez d'abord le document intitulé *Installation d'une carte d'accès à distance* qui fait partie de votre kit DRAC 5 ou le *Guide d'installation et de dépannage* de votre plate-forme pour obtenir les instructions d'installation du matériel.

REMARQUE : Consultez le *Guide d'installation et de dépannage* fourni avec votre système pour plus d'informations sur le retrait du DRAC 5. Étudiez également toutes les propriétés de RAC de Microsoft® Active Directory® associées au DRAC 5 retiré pour garantir une sécurité adéquate si vous utilisez un schéma étendu.

Configuration de votre système pour utiliser un DRAC 5

Pour configurer votre système pour utiliser un DRAC 5, utilisez l'utilitaire de configuration de l'accès à distance de Dell™ (anciennement connu sous le nom de module d'installation du BMC).

Pour exécuter l'utilitaire de configuration de l'accès à distance de Dell :

1. Allumez ou redémarrez le 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 finir de démarrer, puis redémarrez-le et réessayez.
3. Configurez le NIC.
   a. À l'aide de la touche fléchée vers le bas, sélectionnez **Sélection du NIC**.
   b. À l'aide des touches fléchées vers la gauche et la droite, sélectionnez l'une des sélections de NIC suivantes :
      - **Dédié** : sélectionnez cette option pour permettre au périphérique d'accès à distance d'utiliser l'interface réseau dédiée disponible sur le RAC (Remote Access Controller). 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 une carte DRAC est installée 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.
      - **Basculement** : 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 l'intégralité de la transmission des données sur le NIC 1.

4. Configurez les paramètres LAN du contrôleur de 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** 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**.

   Le système redémarre automatiquement.

REMARQUE : Lors de l'affichage de l'interface utilisateur Web sur un système Dell PowerEdge™ 1900 qui est configuré avec un NIC, la page Configuration du NIC affiche deux NIC (NIC1 et NIC2). Ce comportement est normal. Le système PowerEdge 1900 (et les autres systèmes Dell qui sont configurés avec un seul LAN sur carte mère) peut être configuré avec le regroupement de NIC. Les modes Partagé et Regroupement sont indépendants sur ces systèmes.

Consultez le *Guide d'utilisation des utilitaires de contrôleur de gestion de la carte mère de Dell OpenManage* pour plus d'informations sur l'utilitaire de configuration de l'accès à distance de Dell.

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 du DRAC 5. Configurez votre DRAC 5 à l'aide de l'interface Web, de la CLI RACADM ou de la console série/Telnet/SSH.

Pour plus d'informations sur les composants logiciels du DRAC 5, consultez « Installation du logiciel sur le système géré ».

Installation du logiciel de votre DRAC 5

Pour installer le logiciel de votre DRAC 5 :

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

Configuration de votre DRAC 5

Pour configurer votre DRAC 5 :

1. Sélectionnez un des outils de configuration suivants :
   - Une interface Web
   - CLI RACADM
   - Console série/Telnet/SSH

PRÉCAUTION : L'utilisation de plusieurs outils de configuration du DRAC 5 en même temps peut provoquer des résultats inattendus.

2. Configurez les paramètres réseau du DRAC 5. Voir « Configuration des propriétés du DRAC 5 ».
3. Ajoutez et configurez les utilisateurs du DRAC 5. Voir « Ajout et configuration des utilisateurs du DRAC 5 ».
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 Windows®. Voir « Désactivation de l'option Redémarrage automatique de Windows ».
6. Mettez le micrologiciel du DRAC 5 à jour. Voir « Connexion au système géré via le port série local ou une station de gestion Telnet (système client) ».
7. Accédez au DRAC 5 via un réseau. Voir « Connexion au système géré via le port série local ou une station de gestion Telnet (système client) ».

Installation du logiciel sur le système géré

L'installation du logiciel sur le système géré est facultative. Sans le logiciel Managed System, vous ne pourrez pas utiliser la RACADM localement et le DRAC ne pourra pas capturer 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 des instructions sur l'installation de ce logiciel, consultez votre *Guide d'installation rapide*.

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 Management Station du DRAC 5 et Managed System du DRAC 5 sur le même système.

PRÉCAUTION : Le dernier micrologiciel du DRAC prend uniquement en charge la dernière version de la RACADM. Vous pouvez rencontrer des erreurs si vous utilisez une version plus ancienne de la RACADM pour interroger un DRAC doté du dernier micrologiciel. Installez la version de la RACADM fournie avec votre dernier DVD Dell OpenManage.

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 inclut le kit Dell OpenManage Systems Management Software. Ce kit comprend, mais ne s'y limite pas, au DVD *Dell Systems Management Tools and Documentation*. Pour obtenir des informations sur l'installation du logiciel Server Administrator, consultez le *Guide d'utilisation de Server Administrator*.

Configuration de votre station de gestion Red Hat Enterprise Linux (version 4)

Le visualiseur KVM numérique de Dell nécessite une configuration supplémentaire pour fonctionner sur une station de gestion Red Hat Enterprise Linux (version 4). Lorsque vous installez le système d'exploitation Red Hat Enterprise Linux (version 4) sur votre station de gestion, procédez comme suit :

- Lorsqu'on vous demande d'ajouter ou de retirer des progiciels, installez le logiciel **Legacy Software Development** en option. Ce progiciel comprend les composants logiciels nécessaires pour exécuter le visualiseur KVM numérique de Dell sur votre station de gestion.
- Pour garantir que les fonctions du visualiseur KVM numérique de Dell fonctionnent correctement, ouvrez les ports suivants sur votre pare-feu :
  - Port du clavier et de la souris (le port par défaut est 5900)
  - Port vidéo (le port par défaut est 5901)

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 du DRAC 5

Utilisez l'une des méthodes suivantes pour mettre le micrologiciel de votre DRAC 5 à jour.

- Interface Web
- CLI RACADM
- Progiciels Dell Update Package

Avant de commencer

Avant de mettre à jour le micrologiciel de votre DRAC 5 à l'aide de la RACADM locale ou des progiciels Dell Update Package, procédez comme suit. Sinon, la mise à jour du micrologiciel échouera.

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 votre système fonctionne sous SUSE Linux Enterprise Server (version 10) pour Intel EM64T, démarrez le service **Raw**.
4. Assurez-vous que le disque flash virtuel du RAC n'est ni monté ni utilisé par le système d'exploitation, une autre application ou un autre utilisateur.
5. Débranchez et démontez le média virtuel.
6. Assurez-vous que USB est activé.

Téléchargement du micrologiciel du DRAC 5

Pour mettre à jour le micrologiciel de votre DRAC 5, téléchargez le dernier micrologiciel sur le site Web de support de Dell à l'adresse **support.dell.com** et enregistrez le fichier sur votre système local.

Les composants logiciels suivants sont inclus avec le progiciel de micrologiciel de votre DRAC 5 :

- Code du micrologiciel compilé du DRAC 5 et données
- Image d'extension de ROM
- Fichiers de données de l'interface Web, JPEG et des autres interfaces utilisateur
- Fichiers de configuration par défaut

Utilisez la page **Mise à jour de micrologiciel** pour mettre le micrologiciel du DRAC 5 à jour vers la version la plus récente. Lorsque vous exécutez la mise à jour de micrologiciel, la mise à jour conserve les paramètres actuels du DRAC 5.

Mise à jour du micrologiciel du DRAC 5 à l'aide de l'interface Web

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

   Voir « Accès à l'interface Web ».

2. Dans l'arborescence **Système**, cliquez sur **Accès à distance** puis sur l'onglet **Mettre à jour**.

3. Sur la page **Mise à jour de micrologiciel** sous l'onglet **Image de micrologiciel**, tapez le chemin d'accès à l'image de micrologiciel que vous avez téléchargée sur le site **support.dell.com** ou cliquez sur **Parcourir** pour accéder à l'image.

   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>`.

   Par défaut, le nom de l'image du micrologiciel est **firmimg.d5**.

4. Cliquez sur **Update (Mise à jour)**.

   La mise à jour peut prendre plusieurs minutes. Lorsqu'elle est terminée, une boîte de dialogue apparaît.

5. Cliquez sur **OK** pour fermer la session et être déconnecté automatiquement.

6. Une fois le DRAC 5 réinitialisé, cliquez sur **Ouvrir une session** pour ouvrir une session sur le DRAC 5.

Mise à jour du micrologiciel DRAC 5 à l'aide de racadm

Vous pouvez mettre à jour le micrologiciel DRAC 5 à l'aide de l'outil racadm CLI. Si vous avez installé Server Administrator sur le système géré, utilisez la racadm locale pour mettre à jour le micrologiciel.

1. Téléchargez l'image de micrologiciel DRAC 5 du site Web Dell Support à l'adresse **support.dell.com** dans le système géré

   Par exemple :

   ```
   C:\downloads\firmimg.d5
   ```

2. Exécutez la commande racadm suivante :

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

   Vous pouvez également mettre à jour le micrologiciel à l'aide de la racadm distante.

   Par exemple :

   racadm -r <*Adresse IP du DRAC5*> U <*nomd'utilisateur*> -p <*motdepasse*> fwupdate -p -u -d <*chemin*>

   où *chemin* est l'emplacement où vous avez enregistré **firmimg.d5** sur le système géré.

Mise à jour du micrologiciel DRAC 5 à l'aide des progiciels de mise à jour Dell pour les systèmes d'exploitation pris en charge Windows et Linux

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**. Voir le *Guide d'utilisation du progiciel de mise à jour Dell* pour de plus amples informations.

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. Pour obtenir une liste des navigateurs Web pris en charge, consultez la *Matrice de prise en charge des logiciels des systèmes Dell* sur le site Web Dell Support à l'adresse **support.dell.com**.

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

Si vous vous connectez à l'interface Web du DRAC 5 depuis une station de gestion qui se connecte à Internet via un serveur proxy, vous devez configurer le navigateur Web pour qu'il accède 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 sélectionnée, sélectionnez la case **Ne pas utiliser de serveur proxy pour les adresses locales**.

6. Cliquez sur **OK** deux fois.

Liste des domaines de confiance

Lorsque vous accédez à l'interface Web du DRAC 5 via le navigateur Web, vous devez ajouter l'adresse IP du DRAC 5 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 du DRAC 5.

Navigateurs Web 32 bits et 64 bits

L'interface Web du DRAC 5 n'est pas prise en charge sur les navigateurs Web 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 Web 32 bits pris en charge et ouvrez une session sur le DRAC 5.

Affichage de versions localisées de l'interface Web

Windows

L'interface Web du DRAC 5 est prise en charge sur les langues de système d'exploitation Windows suivantes :

- Anglais
- Français
- Allemand
- Espagnol
- Japonais
- Chinois simplifié

Pour afficher une version localisée de l'interface Web du DRAC 5 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 du visualiseur et un titre peuvent apparaître sous forme de caractères aléatoires. Ce problème est dû à l'encodage incorrect dans le système d'exploitation Red Hat Enterprise Linux (version 4) en chinois simplifié. Pour 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>. Le message suivant apparaît.

```
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 le DRAC 5.

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 du DRAC 5, voir « Configuration avancée du DRAC 5 ».

Retour à la page su sommaire

Retour à la page su sommaire

Configuration avancée du DRAC 5

Dell™ Remote Access Controller 5 Guide d'utilisation de la version 1.45 du micrologiciel

Cette section contient des informations sur la configuration avancée du DRAC 5 et est recommandée pour les utilisateurs avec des connaissances avancées de gestion des systèmes et désirant personnaliser l'environnement du DRAC en fonction de vos besoins spécifiques.

Avant de commencer

Vous devez avoir terminé l'installation et la configuration de base du matériel et du logiciel de votre DRAC 5. Pour plus d'informations, voir « Installation de base du DRAC 5 ».

Configuration des propriétés du DRAC 5

Vous pouvez configurer les propriétés du DRAC 5 (réseau, utilisateurs, etc.) depuis l'interface Web ou la RACADM.

Le DRAC 5 est doté d'une interface Web et de la RACADM (une interface de ligne de commande) qui vous permet de configurer les propriétés et les utilisateurs du DRAC 5, d'effectuer des tâches de gestion à distance et de dépanner un système distant (géré) qui a des problèmes. Pour la gestion quotidienne des systèmes, utilisez l'interface Web du DRAC 5. Ce chapitre décrit comment effectuer les tâches de gestion de systèmes courantes en utilisant l'interface Web du DRAC 5 et donne des liens vers des informations connexes.

Toutes les tâches de configuration de l'interface Web peuvent aussi se faire via la RACADM.

Configuration du DRAC 5 via l'interface utilisateur Web

Consultez l'aide en ligne de votre DRAC 5 pour des informations contextuelles sur chaque page de l'interface Web.

Accès à l'interface Web

Pour accéder à l'interface Web du DRAC 5 :

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

   Pour obtenir une liste des navigateurs Web pris en charge, consultez la *Matrice de prise en charge des logiciels des systèmes Dell* sur le site Web Dell Support à l'adresse **support.dell.com**.

2. Dans le champ **Adresse**, tapez l'élément suivant et appuyez sur <Entrée> :

   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 du DRAC 5 et *numéro de port* le numéro de port HTTPS.

   La fenêtre **Ouvrir une session** du DRAC 5 apparaît.

REMARQUE : Quand vous utilisez la version 6 SP2 ou la version 7 d'Internet Explorer pour ouvrir une session d'interface utilisateur Web du DRAC 5 et que le client est sur un réseau privé, mais sans accès à Internet, il peut y avoir un délai d'attente allant jusqu'à 30 secondes. Pour résoudre ce

problème :

1. Désactiver le filtre anti-hameçonnage.

   https://phishingfilter.microsoft.com/faq.aspx.

2. Désactivez l'extraction de CRL :

   a. Cliquez sur **Outils**→ **Options**→ onglet **Avancé** → **Sécurité**.

   b. Désélectionnez **Check for publisher's certificate revocation**.

Ouverture de session

Vous pouvez ouvrir une session en tant qu'utilisateur du DRAC 5 ou utilisateur de Microsoft® Active Directory®. Par défaut, le nom d'utilisateur est **root** et le mot de passe est **calvin**.

Avant de vous connecter au DRAC 5, vérifiez que vous avez le droit **Ouvrir une session sur le DRAC 5**. Demandez à votre administrateur DRAC ou de réseau de confirmer vos privilèges d'accès.

Pour ouvrir une session :

1. Dans le champ **Nom d'utilisateur**, tapez :
   - Votre nom d'utilisateur DRAC 5.

     Par exemple, <*nom d'utilisateur*>

     Le nom d'utilisateur DRAC 5 pour les utilisateurs locaux est sensible à la casse
   - Votre nom d'utilisateur Active Directory.

     Par exemple, <*domaine*>\<*nom d'utilisateur*>, <*domaine*>/<*nom d'utilisateur*> ou <*utilisateur*>@<*domaine*>.

     Exemples de nom d'utilisateur Active Directory : **dell.com\john_doe** ou **john_doe@dell.com**.

     Le nom d'utilisateur Active Directory n'est pas sensible à la casse.
2. Dans le champ **Mot de passe**, tapez votre mot de passe utilisateur DRAC 5 ou Active Directory.

   Ce champ est sensible à la casse.
3. Cliquez sur **OK** ou appuyez sur <Entrée>.

Fermeture de session

1. Dans le coin supérieur droit de la fenêtre de l'interface Web du DRAC 5, 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 reste 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 restera active jusqu'à ce que son délai d'expiration soit atteint.

REMARQUE : La fermeture de l'interface Web du DRAC 5 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**.

Activation et configuration du système géré pour utiliser une console série ou Telnet

Les sous-sections suivantes expliquent comment activer et configurer une console série/telnet/ssh sur le système géré.

Utilisation de la commande série connect com2

Lorsque vous utilisez la commande série **connect com2**, assurez-vous que les éléments suivants sont correctement configurés :

- Le paramètre **Communications série**→ **Port série** dans le programme **Configuration du BIOS**.
- Les paramètres de configuration du DRAC.

Lorsqu'une session telnet est établie sur le DRAC 5 et que ces paramètres sont incorrects, **connect com2** peut afficher un écran vide.

Configuration du programme de configuration du BIOS pour une connexion série sur le système géré

Effectuez les étapes suivantes pour configurer la redirection des sorties vers un port série dans le programme **Configuration du BIOS**.

REMARQUE : Vous devez configurer le programme **Configuration du système** en association avec la commande **connect com2**.

1. Allumez ou redémarrez le système.
2. Appuyez sur <F2> immédiatement après le message suivant :

   ```
   <F2> = System Setup
   ```

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**

   Redirection après démarrage : **désactivée**

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

Utilisation de l'interface série d'accès à distance

Lorsque vous établissez une connexion série sur le périphérique RAC, les interfaces suivantes sont disponibles :

- Interface série IPMI Voir « Utilisation de l'interface série d'accès à distance IPMI ».
- Interface série RAC

Interface série RAC

Le RAC prend aussi en charge une interface de console série (ou *console série RAC*) qui fournit une CLI RAC, qui n'est pas définie par IPMI. Si votre système inclut une carte RAC avec l'option **Console série** activée, la carte RAC annule les paramètres série IPMI et affiche l'interface série CLI RAC.

Pour activer l'interface du terminal série RAC, configurez la propriété **cfgSerialConsoleEnable** sur **1** (TRUE).

Par exemple :

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

Pour plus d'informations, voir « cfgSerialConsoleEnable (lecture/écriture) ».

Tableau 4-1 fournit les paramètres de l'interface série.

Tableau 4-1. Paramètres de l'interface série

Mode IPMI	Console série RAC	Interface
De base	Désactivé	Mode de base
De base	Activé	CLI RAC
Terminal	Désactivé	Mode terminal IPMI
Terminal	Activé	CLI RAC

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=ttyS1,57600
   ```

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

Tableau 4-2 fournit un exemple de fichier **/etc/grub.conf** qui illustre les modifications décrites dans cette procédure.

Tableau 4-2. 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=ttyS1,57600
   initrd /boot/initrd-2.4.9-e.3smp.img
title Red Hat Linux Advanced Server-up (2.4.9-e.3)
   root (hd0,00)
   kernel /boot/vmlinuz-2.4.9-e.3 ro root=/dev/sda1 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=ttyS1,57600
   ```

   Tableau 4-2 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
```

Tableau 4-3 illustre un exemple de fichier avec la nouvelle ligne.

Tableau 4-3. 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
```

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

Tableau 4-4. 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
```

Activation de la console série/Telnet/SSH du DRAC 5

Vous pouvez activer la console série/telnet/ssh localement ou à distance.

Activation de la console série/Telnet/SSH localement

REMARQUE : Vous (l'utilisateur actuel) devez disposer du droit **Configurer le DRAC 5** pour pouvoir effectuer les étapes décrites dans cette section.

Pour activer la console série/telnet/ssh depuis le système géré, tapez les commandes de la RACADM locale suivantes à partir d'une invite de commande :

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

racadm config -g cfgSerial -o cfgSerialTelnetEnable 1

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

Activation à distance de la console série/Telnet/SSH

Pour activer la console série/telnet/ssh à distance, tapez les commandes de la **RACADM** distante suivantes à partir d'une invite de commande :

```
racadm -u <nomd'utilisateur> -p <motdepasse> -r <adresse IP du DRAC 5> config -g cfgSerial -o cfgSerialConsoleEnable 1

racadm -u <nomd'utilisateur> -p <motdepasse> -r <adresse IP du DRAC 5> config -g cfgSerial -o cfgSerialConsoleEnable 1

racadm -u <nomd'utilisateur> -p <motdepasse> -r <adresse IP du DRAC 5> config -g cfgSerial -o cfgSerialTelnetEnable 1
```

REMARQUE : Quand vous utilisez la version 6 SP2 ou la version 7 d'Internet Explorer pour ouvrir une session d'un système géré sur un réseau privé, mais sans accès à Internet, il peut y avoir un délai allant jusqu'à 30 secondes en utilisant les commandes de la RACADM distante.

Utilisation de la commande RACADM pour configurer les paramètres de la console série ou Telnet

Cette sous-section présente les étapes de configuration des paramètres de configuration par défaut de la redirection de console série/telnet/ssh.

Pour configurer les paramètres, tapez la commande **config** RACADM avec le groupe, la propriété et les valeurs de propriété appropriés au paramètre à configurer.

Vous pouvez taper les commandes RACADM localement ou à distance. Si vous utilisez les commandes RACADM à distance, vous devez inclure le nom d'utilisateur, le mot de passe et l'adresse IP du DRAC 5 du système géré.

Utilisation de la RACADM localement

Pour taper les commandes RACADM localement, tapez la commande suivante à partir d'une invite de commande sur le système géré :

```
racadm config -g <groupe> -o <propriété> <valeur>
```

Pour afficher la liste des propriétés, tapez la commande suivante à partir d'une invite de commande sur le système géré :

```
racadm getconfig -g <groupe>
```

Utilisation de la RACADM à distance

Pour utiliser les commandes RACADM à distance, tapez la commande suivante à partir d'une invite de commande sur une station de gestion :

```
racadm -u <nom d'utilisateur> -p <mot de passe> -r <adresse IP du DRAC 5> config -g <groupe> -o <propriété> <valeur>
```

Assurez-vous que votre serveur Web est configuré avec une carte DRAC 5 avant d'utiliser la RACADM à distance. Sinon, la RACADM expire et le message suivant apparaît :

```
Impossible de se connecter au RAC à l'adresse IP spécifiée.
```

Pour activer votre serveur Web à l'aide de l'interface Secure Shell (SSH), Telnet ou RACADM locale, tapez la commande suivante à partir d'une invite de commande sur une station de gestion :

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

Affichage des paramètres de configuration

Tableau 4-5 fournit les actions et les commandes associées pour afficher vos paramètres de configuration. Pour exécuter les commandes, ouvrez une invite de commande sur le système géré, tapez la commande et appuyez sur <Entrée>.

Tableau 4-5. Affichage des paramètres de configuration

Action	Commande
Énumérer les groupes disponibles.	racadm getconfig -h
Afficher les paramètres actuels pour un groupe particulier.	racadm getconfig -g <*groupe*> Par exemple, pour afficher une liste de tous les paramètres du groupe **cfgSerial**, tapez la

	commande suivante : racadm getconfig -g cfgSerial
Afficher les paramètres actuels pour un groupe particulier à distance.	racadm -u <*utilisateur*> -p <*mot de passe*> -r <*adresse IP du DRAC 5*> getconfig -g cfgSerial Par exemple, pour afficher une liste de tous les paramètres du groupe **cfgSerial** à distance, tapez : racadm -u root -p calvin -r 192.168.0.1 getconfig -g cfgSerial

Configuration du numéro du port Telnet

Tapez la commande suivante pour changer le numéro du port telnet du DRAC 5.

`racadm config -g cfgRacTuning -o cfgRacTuneTelnetPort` *<nouveau numéro de port>*

Utilisation d'une console série ou Telnet

Vous pouvez exécuter les commandes série dans le tableau 4-19 à distance à l'aide de la RACADM ou de l'invite de commande de la console série/telnet/ssh.

Ouverture de session sur le DRAC 5

Une fois le logiciel d'émulation du terminal et le BIOS du nud géré de votre station de gestion configurés, effectuez les étapes suivantes pour ouvrir une session sur le DRAC 5 :

1. Connectez-vous au DRAC 5 avec votre logiciel d'émulation de terminal de votre station de gestion.
2. Tapez votre nom d'utilisateur DRAC 5 et appuyez sur <Entrée>.

   Vous venez d'ouvrir une session sur le DRAC 5.

Démarrage d'une console texte

Lorsque vous avez ouvert une session sur le DRAC 5 avec le logiciel d'émulation de terminal de votre station de gestion via telnet ou SSH, vous pouvez rediriger la console texte du système géré en utilisant **connect com2**, qui est une commande telnet/SSH. Un seul client **connect com2** est pris en charge à la fois.

Pour vous connecter à la console texte du système géré, ouvrez une invite de commande DRAC 5 (affichée via une session telnet ou SSH) et tapez :

```
connect com2
```

À partir d'une session série, vous pouvez vous connecter à la console série du système géré en appuyant sur <Échap><Maj><Q>, ce qui connecte directement le port série du système géré au port COM2 des serveurs et évite le DRAC 5. Pour reconnecter le DRAC 5 au port série, appuyez sur <Échap><Maj><9>. Les débits en bauds du port COM2 du nud géré et du port série du DRAC 5 doivent être identiques.

La commande `connect -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.

REMARQUE : Lorsque vous utilisez l'option **-h**, le type d'émulation de terminal serveur et client (ANSI ou VT100) doit être identique ; sinon, la sortie peut être tronquée. De plus, définissez la ligne du terminal client sur **25**.

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>*

Configuration des modes série et terminal

Configuration du mode série IPMI et RAC

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 4-6 pour une description des paramètres série IPMI.

4. Configurez les paramètres série du RAC.

   Voir Tableau 4-7 pour une description des paramètres série du RAC.

5. Cliquez sur **Appliquer les modifications**.

6. Cliquez sur le bouton approprié de la page **Configuration série** pour continuer. Consultez Tableau 4-8 pour obtenir une description des paramètres de la page Configuration série.

Tableau 4-6. Paramètres série IPMI

Paramètre	Description
Paramètre du mode de connexion	• Mode de base de connexion directe : mode de base série IPMI • Mode terminal de connexion directe : mode terminal 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 4-7. Paramètres série du RAC

Paramètre	Description
Activé	Active ou désactive la console série RAC. Coché = Activé ; Décoché = Désactivé
Nombre maximal de sessions	Nombre maximal de sessions simultanées autorisées pour ce système.
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**, **28,8 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 du DRAC à exécuter lors d'une ouverture de session valide.

Tableau 4-8. Paramètres de la page Configuration série

Bouton	Description
Imprimer	Imprime la page **Configuration série**.
Actualiser	Actualise la page **Configuration série**.
Appliquer les modifications	Applique les modifications série IPMI et RAC.
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 **Configuration série**, cliquez sur **Paramètres du mode terminal**.

4. Configurez les paramètres du mode terminal.

   Voir Tableau 4-9 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 4-10 pour une description des boutons de la page Paramètres du mode terminal.

Tableau 4-9. 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 : • **Le contrôleur BMC sort un caractère <retarr.><esp.><retarr.> lorsque <retarr.> ou <suppr.> est reçu**. • **Le contrôleur BMC 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 4-10. 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**.
Retour à la page Configuration du port série	Retourne à la page **Configuration du port série**.
Appliquer les modifications	Applique les modifications apportées aux paramètres du mode terminal.

Connexion au système géré via le port série local ou une station de gestion Telnet (système client)

Le système géré permet de communiquer entre le DRAC 5 et le port série de votre système de façon à pouvoir mettre hors et sous tension le système géré ou le réinitialiser, et à pouvoir accéder aux journaux.

La console série est accessible depuis le DRAC 5 via le connecteur série externe du système géré. Il ne peut y avoir qu'un système client série (station de gestion) actif à un moment donné. Les consoles telnet et SSH sont disponibles sur le DRAC 5 via les modes DRAC (voir « Modes DRAC »). Un maximum de quatre systèmes client telnet et quatre clients SSH peuvent se connecter à la fois. La connexion de la station de gestion à la console série ou telnet du système géré nécessite un logiciel d'émulation de terminal sur la station de gestion. Pour plus d'informations, voir « Configuration du logiciel d'émulation de terminal de la station de gestion ».

Les sous-sections suivantes expliquent comment connecter votre station de gestion au système géré à l'aide des méthodes suivantes :

- Un port série externe du système géré à l'aide du logiciel de terminal et d'un DB-9 ou d'un câble null modem
- Une connexion telnet à l'aide du logiciel terminal via le NIC du DRAC 5 du système géré ou le NIC partagé

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. 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 4-11.

REMARQUE : Le câble DB-9 peut aussi être utilisé pour la redirection de console texte du BIOS.

Tableau 4-11. 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 DRAC 5 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 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`

Vérifiez que la fenêtre de Minicom affiche une invite de commande comme, par exemple, `[DRAC 5\root]#`. L'invite de commande apparaît si votre connexion est réussie et si 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 4-12 pour configurer une version quelconque de Minicom.

Tableau 4-12. 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.

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 4-13.

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 4-13. Paramètres du port COM de la station de gestion

Description du paramètre	Paramètre requis
Bits par seconde	57600
Bits de données	8
Parité	Aucun.
Bits d'arrêt	1
Contrôle du débit	Matériel

Vérifiez que la fenêtre d'HyperTerminal affiche une invite de commande comme, par exemple, `[DRAC 5\root]#`. L'invite de commande apparaît si votre connexion est réussie et si vous pouvez vous connecter à la console du système géré avec la commande série **connect com2**.

Configuration de Linux XTerm pour la redirection de console Telnet

Observez les instructions suivantes en effectuant les étapes de cette section :

- Lorsque vous utilisez la commande **connect com2** via une console telnet pour afficher les écrans Configuration du système, définissez le type de terminal sur **ANSI** dans le programme de configuration du système et pour la session telnet.
- 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.

Pour exécuter la console telnet avec Linux :

1. Démarrez une nouvelle session Xterm.

   À l'invite de commande, tapez `xterm &`

2. Cliquez dans l'angle inférieur droit de la fenêtre XTerm et redimensionnez la fenêtre sur 80 x 25.

3. Connectez-vous au DRAC 5 dans le système géré.

   À l'invite Xterm, tapez `telnet <adresse IP du DRAC 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. 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**.

1. Activez **Telnet** dans **Services du composant Windows.**

2. Connectez-vous au DRAC 5 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 du DRAC 5 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 de session telnet, tapez :

   `telnet`

   Si vous exécutez une session telnet, appuyez sur <Ctrl><]>.

3. À l'invite, tapez :

   `set bsasdel`

   Le message suivant apparaît :

   `Retour arrière sera envoyé en tant que delete.`

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 d'une console série ou Telnet

Les commandes **série** et **telnet** ainsi que la CLI RACADM peuvent être tapées dans une console série ou telnet et exécutées sur le serveur localement ou à distance. La CLI RACADM locale ne peut être utilisée que par un utilisateur root.

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

Si votre station de gestion exécute Windows XP ou Windows 2003, vous pouvez rencontrer un problème avec les caractères dans une session telnet DRAC 5. Ce problème peut provoquer le gel de l'ouverture de session où la touche de retour ne répond pas et le message de saisie du mot de passe n'apparaît 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* ».

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 affaire 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. Le DRAC 5 prend en charge la version 2 de SSH avec authentification par mot de passe. SSH est activé sur le DRAC 5 quand vous installez ou mettez à jour votre micrologiciel du DRAC 5.

Vous pouvez utiliser PuTTY ou OpenSSH sur la station de gestion pour vous connecter au DRAC 5 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 le DRAC 5.

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).

Quatre sessions SSH uniquement sont prises en charge à la fois. Le délai d'expiration de la session est contrôlé par la propriété `cfgSsnMgtSshIdleTimeout` comme décrit dans « Définitions des groupes et des objets de la base de données de propriétés du DRAC 5 ».

Pour activer SSH sur le DRAC 5, 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 de propriétés du DRAC 5 ».

La mise en oeuvre SSH du DRAC 5 prend en charge plusieurs schémas de cryptographie, comme illustré dans le tableau 4-14.

Tableau 4-14. 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 des paramètres réseau du DRAC 5

PRÉCAUTION : Si vous modifiez les paramètres réseau de votre DRAC 5, la connexion réseau en cours risque d'être coupée.

Configurez les paramètres réseau du DRAC 5 avec l'un des outils suivants :

- Interface Web : voir « Configuration du NIC du DRAC 5 »
- CLI RACADM : voir « cfgLanNetworking »
- Utilitaire Dell Remote Access Configuration : voir « Configuration de votre système pour utiliser un DRAC 5 »

REMARQUE : Si vous déployez le DRAC 5 dans un environnement Linux, voir « Installation de la RACADM ».

Accès au DRAC 5 via un réseau

Une fois le DRAC 5 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

Tableau 4-15 décrit chaque interface du DRAC 5.

Tableau 4-15. Interfaces du DRAC 5

Interface	Description
Une interface Web	Fournit un accès à distance au DRAC 5 à l'aide d'une interface utilisateur graphique. L'interface Web est intégrée au micrologiciel du DRAC 5 et accessible via l'interface NIC d'un navigateur Web pris en charge sur la station de gestion. Pour obtenir une liste des navigateurs Web pris en charge, consultez la *Matrice de prise en charge des logiciels des systèmes Dell* sur le site Web Dell Support à l'adresse **support.dell.com**.

la RACADM	Fournit un accès à distance au DRAC 5 à l'aide d'une interface de ligne de commande. La RACADM utilise l'adresse IP du système géré pour exécuter des commandes RACADM (option de capacité d'accès à distance de la racadm [-r]).
	
	REMARQUE : La capacité d'accès à distance de la racadm est prise en charge uniquement sur les stations de gestion.
	
	REMARQUE : Lorsque vous utilisez la capacité d'accès à distance de la racadm, vous devez posséder le droit 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`

Console Telnet	Fournit l'accès via le DRAC 5 au port RAC du serveur et aux interfaces de gestion de matériel via le NIC du DRAC 5 et assure 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 le DRAC 5 aux fonctionnalités de gestion de base du système distant. L'interface inclut IPMI sur LAN, IPMI sur communication série et Communication série sur LAN. Consultez le *Guide d'utilisation du contrôleur de gestion de la carte mère de Dell OpenManage* pour plus d'informations.

REMARQUE : Par défaut, le nom d'utilisateur du DRAC 5 est root et le mot de passe est calvin.

Vous pouvez accéder à l'interface Web du DRAC 5 via le NIC du DRAC 5 en utilisant un navigateur Web pris en charge, Server Administrator ou IT Assistant.

Pour obtenir une liste des navigateurs Web pris en charge, consultez la *Matrice de prise en charge des logiciels des systèmes Dell* sur le site Web Dell Support à l'adresse **support.dell.com**.

Pour accéder à l'interface d'accès à distance du DRAC 5 avec Server Administrator, 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 des informations supplémentaires, consultez le Guide d'utilisation de Server Administrator.

Configuration du NIC du DRAC 5

Configuration des paramètres du réseau et du LAN IPMI

REMARQUE : Vous devez avoir le droit **Configurer le DRAC 5** 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 (DRAC 5, par exemple) doit fournir ce jeton pendant la négociation DHCP. Pour les RAC, DRAC 5 fournit l'option d'identification de client à l'aide d'un numéro d'interface d'un octet (0) suivi par une adresse MAC de six octets.

REMARQUE : Si le DRAC du système géré est configuré en mode **Partagé** ou **Partagé avec basculement** et que le DRAC est connecté à un commutateur avec l'option STP (Spanning Tree Protocol) activée, les clients réseau connaîtront un retard de connectivité de 20 à 30 secondes lors d'une modification de l'état du lien LOM de la station de gestion pendant la convergence STP.

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**, configurez les paramètres NIC du DRAC 5.

   Tableau 4-16 et Tableau 4-17 décrit les **Paramètres réseau** et **Paramètres IPMI** de la page **Configuration réseau**.
4. Lorsque vous avez terminé, cliquez sur **Appliquer les modifications**.
5. Cliquez sur le bouton approprié de la page **Configuration réseau** pour continuer. Reportez-vous à la section Tableau 4-18.

Tableau 4-16. Paramètres réseau

Paramètre	Description
Sélection de NIC	Affiche le mode NIC sélectionné (**Dédié**, **Partagé avec basculement** ou **Partagé**). Le paramètre par défaut est **Dédié**.
MAC Address	Affiche l'adresse MAC du DRAC 5.
Activer le NIC	Active le NIC du DRAC 5 et active les autres commandes de ce groupe. Le paramètre par défaut est **Activé**.
Utiliser DHCP (pour l'adresse IP du NIC)	Permet à Dell OpenManage™ Server Administrator d'obtenir l'adresse IP NIC du DRAC 5 à partir du serveur de protocole de configuration dynamique des hôtes (DHCP). Le fait de cocher la case désactive les commandes **Adresse IP statique**, **Passerelle statique** et **Masque de sous-réseau statique**. Le paramètre par défaut est **Désactivé**.
Adresse IP statique	Spécifie ou modifie l'adresse IP statique du NIC du DRAC 5. Pour modifier ce paramètre, décochez la case **Utiliser DHCP (pour l'adresse IP du NIC)**.
Passerelle statique	Spécifie ou modifie la passerelle statique du NIC du DRAC 5. Pour modifier ce paramètre, décochez la case **Utiliser DHCP (pour l'adresse IP du NIC)**.
Masque de sous-réseau statique	Spécifie ou modifie le masque de sous-réseau statique du NIC du DRAC 5. Pour modifier ce paramètre, décochez la case **Utiliser DHCP (pour l'adresse IP du NIC)**.
Utiliser DHCP pour obtenir des adresses de serveur DNS	Obtient les adresses de serveur DNS principales et secondaires du serveur de DHCP au lieu des paramètres statiques. Le paramètre par défaut est **Désactivé**.
Serveur DNS préféré statique	Utilise l'adresse IP de serveur DNS principale uniquement lorsque l'option **Utiliser DHCP pour obtenir des adresses de serveur DNS** n'est **pas sélectionnée**.
Autre serveur DNS statique	Utilise l'adresse IP du serveur DNS secondaire si **Utiliser DHCP pour obtenir des adresses de serveur DNS** n'est **pas sélectionné**. Si vous n'avez pas d'autre serveur DNS, vous pouvez saisir 0.0.0.0 pour l'adresse IP.
Enregistrer le DRAC auprès du DNS	Enregistre le nom du DRAC 5 auprès du serveur DNS. Le paramètre par défaut est **Désactivé**.
Nom du DRAC DNS	N'affiche le nom du DRAC 5 que si **Enregistrer le DRAC 5 auprès du DNS** est sélectionné. Par défaut, le nom du DRAC 5 est RAC-*numéro de service*, *numéro de service* étant le numéro de service du serveur Dell (RAC-EK00002, par exemple).
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 **Inscrire le DRAC 5 sur DNS** est sélectionnée, vous pouvez changer le nom de domaine DNS dans le champ **Nom de domaine DNS**.

	Le paramètre par défaut est **Désactivé**.
Nom de domaine DNS	Par défaut, le nom de domaine DNS est **MYDOMAIN**. Si la case **Utiliser DHCP pour le nom de domaine DNS** est cochée, cette option est grisée et ne peut pas être modifiée.
Négociation automatique	Indique que le DRAC 5 définit automatiquement le **mode duplex** et la **vitesse du réseau** en communicant avec le routeur ou le concentrateur le plus proche (**Activé**) ou vous permet de définir le **mode duplex** et la **vitesse du réseau** manuellement (**Désactivé**).
Vitesse du réseau	Définit une vitesse du réseau de 100 Mo ou 10 Mo selon votre environnement réseau. Cette option n'est pas disponible si **Négociation automatique** est défini sur **Activé**.
Mode duplex	Définit le mode duplex sur intégral ou semi selon votre environnement réseau. Cette option n'est pas disponible si **Négociation automatique** est défini sur **Activé**.

Tableau 4-17. Paramètres LAN IPMI

Paramètre	Description
Activer IPMI sur le réseau local	Active le canal LAN IPMI.
Limite du niveau de privilège du canal	Configure le niveau de privilège maximum de l'utilisateur qui peut être accepté sur le canal LAN. Sélectionnez l'une des options suivantes : Administrateur, Opérateur ou Utilisateur.
Clé de cryptage	Configure le format de caractère de la clé de cryptage : 0 à 20 caractères hexadécimaux (aucun blanc autorisé). Le paramètre par défaut est *0000000000000000000*.
Activer l'ID du VLAN	Active l'ID du VLAN. Si cette option est activée, seul le trafic d'ID du VLAN correspondant est accepté.
ID du VLAN	Champ ID du VLAN des champs 802.1g.
Priorité	Champ Priorité des champs 802.1g.

Tableau 4-18. Boutons de la page Configuration réseau

Bouton	Description
Imprimer	Imprime la page **Configuration réseau**
Actualiser	Recharge la page **Configuration réseau**
Paramètres avancés	Affiche la page **Sécurité réseau**.
Appliquer les modifications	Enregistre les modifications apportées à la configuration réseau. **REMARQUE :** Les modifications apportées aux paramètres d'adresse IP du NIC ferment toutes les sessions utilisateur et imposent aux utilisateurs de se reconnecter à l'interface Web du DRAC 5 à l'aide des paramètres d'adresse IP mis à jour. Toutes les autres modifications nécessitent la réinitialisation du NIC, qui peut provoquer une perte brève de connectivité.

Pour plus d'informations, voir « Configuration des paramètres de sécurité réseau à l'aide de la GUI du DRAC 5 ».

Utilisation de la RACADM à distance

REMARQUE : Configurez l'adresse IP du DRAC 5 avant d'utiliser la fonction d'accès à distance à la racadm. Pour plus d'informations sur la configuration de votre DRAC 5 et une liste des documents connexes, voir « Installation de base du DRAC 5 ».

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 l'option de capacité d'accès à distance, vous avez besoin d'un nom d'utilisateur (option -**u**) et d'un mot de passe (option -**p**) valides, ainsi que de l'adresse IP du DRAC 5.

REMARQUE : Si le système depuis lequel vous accédez au système distant ne comporte pas de certificat de DRAC dans sa réserve de certificats par défaut, un message apparaît lorsque vous tapez une commande racadm.

```
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` , la 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.

EORROR: Unable to connect to RAC 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 au RAC à l'adresse IP spécifiée.)

REMARQUE : La capacité d'accès à distance de la racadm est prise en charge uniquement sur les stations de gestion. Consultez la Matrice de prise en charge des logiciels des systèmes Dell située sur le site Web de support de Dell à l'adresse support.dell.com pour plus d'informations.

REMARQUE : Lorsque vous utilisez la capacité d'accès à distance de la 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 du RAC> -u <nom d'utilisateur> -p <mot de passe> <sous-commande> <options de la sous-commande>

racadm -i -r <adresse IP du RAC> <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 du RAC a été remplacé par un port personnalisé autre que le port par défaut (443), la syntaxe suivante doit être utilisée :

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

racadm -i -r <adresse IP du RAC>:<port> <sous-commande> <options de la sous-commande>
```

Options de la RACADM

Tableau 4-19 énumère les options de la commande **racadm**.

Tableau 4-19. 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*> si le numéro de port du DRAC 5 n'est pas le port par défaut (443)
-i	Ordonne à la **racadm** de demander de manière interactive à l'utilisateur son nom d'utilisateur et son mot de passe.
-u <*usrName*>	Spécifie le nom d'utilisateur qui est utilisé pour authentifier la transaction de commande. Si l'option **-u** est utilisée, l'option **-p** doit être utilisée et l'option **-i** (interactive) n'est pas autorisée.
-p <*mot de passe*>	Spécifie le mot de passe utilisé pour authentifier la transaction de commande. Si l'option **-p** est utilisée, l'option **-i** n'est pas autorisée.
-S	Indique que la **racadm** 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 fonction de capacité d'accès à distance de la 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

Tableau 4-20 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 4-20. Sous-commandes RACADM

Commande	Description
help	Répertorie les sous-commandes du DRAC 5.
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 du DRAC 5. Une entrée unique est effectuée pour indiquer l'utilisateur et l'heure à laquelle le journal a été effacé.
config	Configure le RAC.
getconfig	Affiche les propriétés de configuration du RAC actuelles.
coredump	Affiche le dernier vidage de mémoire du DRAC 5.
coredumpdelete	Supprime le vidage de mémoire stocké sur le DRAC 5.
fwupdate	Exécute ou affiche l'état des mises à jour du micrologiciel du DRAC 5.
getssninfo	Affiche des informations sur les sessions actives.
getsysinfo	Affiche des informations générales concernant le DRAC 5 et le système.
getractime	Affiche l'heure du DRAC 5.
ifconfig	Affiche la configuration IP du RAC actuelle.
netstat	Affiche la table de routage et les connexions actuelles.
ping	Vérifie qu'il est possible d'atteindre l'adresse IP de destination à partir du DRAC 5 avec le contenu actuel de la table 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 d'état du DRAC 5 pour le débogage.
racreset	Réinitialise le DRAC 5.
racresetcfg	Restaure la configuration par défaut du DRAC 5.
serveraction	Effectue des opérations de gestion de l'alimentation sur le système géré.
getraclog	Affiche le journal du RAC.
clrsel	Efface toutes les entrées du journal des événements système.
gettracelog	Affiche le journal trace du DRAC 5. Si elle est utilisée avec -i, la commande affiche le nombre d'entrées du journal de suivi du DRAC 5.
sslcsrgen	Génère et télécharge la CSR SSL.
sslcertupload	Télécharge un certificat de CA ou un certificat du serveur sur le DRAC 5.
sslcertdownload	Télécharge un certificat de CA.
sslcertview	Affiche un certificat de CA ou un certificat de serveur du DRAC 5.
testemail	Contraint le DRAC 5 à envoyer un e-mail test sur le NIC du DRAC 5 pour vérifier la configuration de l'e-mail.
testtrap	Contraint le DRAC 5 à envoyer une interruption SNMP sur le NIC du DRAC 5 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 (16 Mo).

Questions fréquemment posées sur les messages d'erreur de la RACADM

Une fois le DRAC 5 réinitialisé (avec la commande racadm racreset), j 'envoie une commande et le message suivant s'affiche :

racadm <nom de la commande> Transport: ERROR: (RC=-1)

Qu'est-ce que ce message signifie ?

Vous devez attendre que le DRAC 5 soit complètement 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 radcam 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 du DRAC de mon système, puis bascule ma carte DRAC 5 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 cartes DRAC 5

Utilisez la RACADM pour configurer une ou plusieurs cartes DRAC 5 avec des propriétés identiques. Lorsque vous effectuez une requête sur une carte DRAC 5 spécifique à l'aide de son ID de groupe et de son ID d'objet, la RACADM crée le fichier de configuration **racadm.cfg** à partir des informations collectées. En exportant le fichier vers une ou plusieurs cartes DRAC 5, vous pouvez configurer vos contrôleurs avec des propriétés identiques en un minimum de temps.

REMARQUE : Certains fichiers de configuration contiennent des informations uniques sur le DRAC 5 (comme l'adresse IP statique) qu'il faut modifier avant l'exportation du fichier vers d'autres cartes DRAC 5.

Pour configurer plusieurs cartes DRAC 5, effectuez les procédures suivantes :

1. Utilisez la RACADM pour effectuer une requête sur le DRAC 5 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 RAC 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 RAC cible.

   Dans l'invite de commande, tapez :

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

4. Réinitialisez le RAC cible qui a été configuré.

   Dans l'invite de commande, tapez :

   ```
   racadm reset
   ```

La sous-commande **getconfig -f racadm.cfg** nécessite la configuration du DRAC 5 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 DRAC 5. 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 qui ne reconnaît aucun type de formatage et qui peut corrompre la base de données RACADM.

Création d'un fichier de configuration du DRAC 5

Le fichier de configuration du DRAC 5 **<***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 le DRAC 5 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 au DRAC 5 si une erreur est trouvée dans le fichier **.cfg**. L'utilisateur doit corriger *toutes* les erreurs avant qu'une 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 le DRAC 5.

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 DRAC 5 pour ce groupe. Les objets dans ce groupe sont de simples modifications lorsque le DRAC 5 est configuré. Si un objet modifié représente un nouvel index, l'index est créé sur le DRAC 5 pendant 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 DRAC 5 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 toutes les cartes DRAC 5 avec des propriétés identiques.

  Utilisez la sous-commande **racresetcfg** pour restaurer les valeurs par défaut du DRAC 5, puis exécutez 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 le NIC du DRAC 5 à leurs paramètres par défaut et supprimer tous les utilisateurs et toutes les configurations utilisateur. Pendant que l'utilisateur root est disponible, les paramètres par défaut des autres utilisateurs sont également 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 *<nomdefichier>*.cfg, puis exécuter une commande racadm config -f *<nomdefichier>*.cfg sur un autre DRAC 5 sans ajouter de caractères d'échappement.

  Exemple :

  ```
  #

  # This is a comment

  [cfgUserAdmin]

  cfgUserAdminPageModemInitString=<Modem init # not a comment>
  ```

- 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 de propriétés du DRAC 5 ».

  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 NULL (identifiée par deux caractères """) ordonne au DRAC 5 de supprimer l'index du groupe indiqué.

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 <mon exemple>.cfg`, la commande crée un fichier **.cfg** pour la configuration du DRAC 5 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 du DRAC 5

Lorsque vous modifiez l'adresse IP du DRAC 5 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.

```
#

# Object Group "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.10.110

cfgNicGateway=10.35.10.1
```

Ce fichier est mis à jour comme suit :

```
#

# Object Group "cfgLanNetworking"

#

[cfgLanNetworking]

cfgNicIpAddress=10.35.9.143

# comment, the rest of this line is ignored

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 réseau du DRAC 5

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'option ROM au démarrage lorsque vous êtes invité à taper <Ctrl><e>. Pour plus d'informations sur la configuration des propriétés du réseau avec l'option ROM, voir « Configuration des propriétés réseau du DRAC 5 ».

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 **cfgNicEnable** est défini sur **0**, le LAN du DRAC 5 est désactivé même si DHCP est activé.

Modes DRAC

Le DRAC 5 peut être configuré dans un des trois modes suivants :

- Dédié
- Partagé
- Partagé avec basculement

Tableau 4-21 fournit une description de chaque modet.

Tableau 4-21. Configurations du NIC du DRAC 5

Mode	Description
Dédié	Le DRAC utilise son propre NIC (connecteur RJ-45) et l'adresse MAC du contrôleur BMC pour le trafic réseau.
Partagé	Le DRAC utilise Broadcom LOM1 sur le planar.
Partagé avec basculement	Le DRAC utilise Broadcom LOM1 et LOM2 comme groupe pour le basculement. Le groupe utilise l'adresse MAC du contrôleur BMC.

Questions les plus fréquentes

Lorsque j'accède à l'interface Web du DRAC 5, un message de sécurité s'affiche ; il m'informe que le nom d'hôte du certificat SSL ne correspond pas au nom d'hôte du DRAC 5.

Le DRAC 5 est doté d'un certificat de serveur DRAC 5 par défaut qui assure la sécurité du réseau pour l'interface Web et les fonctionnalités de la racadm distante. Lorsque ce certificat est utilisé, le navigateur Web affiche un avertissement de sécurité car le certificat par défaut est attribué au **certificat par défaut du DRAC 5**, lequel ne correspond pas au nom d'hôte du DRAC 5 (l'adresse IP, par exemple).

Pour corriger ce problème de sécurité, téléchargez un certificat de serveur DRAC 5 attribué à l'adresse IP du DRAC 5. Lorsque vous générez la requête de signature de certificat (CSR) qui servira à émettre le certificat, il faut que le nom commun (CN) de la CSR corresponde à l'adresse IP du DRAC 5 (192.168.0.120, par exemple) ou au nom DRAC DNS enregistré.

Pour vous assurer que la CSR correspond au nom DRAC DNS enregistré :

1. Dans l'arborescence du **système**, cliquez sur **Accès distant**.
2. Cliquez sur l'onglet **Configuration** puis sur **Réseau**.
3. Dans la page **Paramètres réseau** :
   a. Cochez la case **Enregistrer le DRAC auprès du DNS**.
   b. Dans le champ **Nom DRAC DNS**, entrez le nom du DRAC.
4. Cliquez sur **Appliquer les modifications**.

Voir « Sécurisation des communications du DRAC 5 via SSL et des certificats 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 DRAC 5, 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 du DRAC 5 Web 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 du DRAC 5
- Quand la propriété **cfgRacTuneHttpsPort** est modifiée (y compris lorsqu'une commande config -f <*fichier config*> la modifie)
- Quand on utilise **racresetcfg**
- Quand le DRAC 5 est réinitialisé
- Quand un nouveau certificat de serveur SSL est téléchargé

Mon serveur DNS n'enregistre pas mon DRAC 5. Pourquoi ?

Certains serveurs DNS ne peuvent enregistrer que des noms de 31 caractères ou moins.

Lorsque j'accède à l'interface Web du DRAC 5, un message de sécurité s'affiche ; il m'informe que le certificat SSL a été émis par une autorité de certification (CA) qui n'est pas fiable.

Le DRAC 5 est doté d'un certificat de serveur DRAC 5 par défaut qui assure la sécurité du réseau pour l'interface Web et les fonctionnalités de la racadm distante. Ce certificat n'a pas été émis par une CA de confiance. Pour résoudre ce problème de sécurité, téléchargez un certificat de serveur DRAC 5 émis par une CA de confiance (Thawte ou Verisign, par exemple). Consultez la section « Sécurisation des communications du DRAC 5 via SSL et des certificats numériques » pour obtenir de plus amples informations sur l'émission de certificats.

Retour à la page su sommaire

Retour à la page su sommaire

Ajout et configuration des utilisateurs du DRAC 5

Dell™ Remote Access Controller 5 Guide d'utilisation de la version 1.45 du micrologiciel

Pour gérer votre système avec le DRAC 5 et maintenir la sécurité du système, créez des utilisateurs uniques avec des droits d'administration spécifiques (ou *avec une 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.

Pour ajouter et configurer les utilisateurs du DRAC 5 :

REMARQUE : Vous devez avoir le droit Configurer le DRAC 5 pour effectuer les étapes suivantes.

1. Développez l'arborescence du **système** et cliquez sur **Accès à distance**.
2. Cliquez sur l'onglet **Configuration**, puis sur **Utilisateurs**.

   La page **Utilisateurs** apparaît, indiquant, pour chaque utilisateur, l'**État**, **le Nom d'utilisateur, le Privilège du RAC**, le **Privilège IPMI LAN**, **le Privilège IPMI série** et la **Communication série sur LAN**.
3. Dans la colonne **ID d'utilisateur**, cliquez sur un ID d'utilisateur.
4. Dans la page **Menu principal de l'utilisateur**, vous pouvez configurer des utilisateurs, télécharger un certificat d'utilisateur, consulter un certificat d'utilisateur existant, télécharger 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. Reportez-vous à la section étape 5 pour plus d'informations.

   Voir Tableau 5-1 si vous sélectionnez les options sous la section **Configuration de la carte à puce**.
5. Sur la page **Configuration de l'utilisateur**, configurez les propriétés et les privilèges de l'utilisateur.

   Tableau 5-2 décrit les paramètres **Généralités** pour configurer un nom d'utilisateur et un mot de passe DRAC nouveau ou existant.

   Tableau 5-3 décrit les **Privilèges d'utilisateur IPMI** pour la configuration des privilèges LAN de l'utilisateur.

   Tableau 5-4 décrit les **droits Groupe d'utilisateurs** pour les paramètres **Privilèges d'utilisateur IPMI** et **Privilèges d'utilisateur DRAC**.

   Tableau 5-5 décrit les droits **Groupe DRAC**. Si vous ajoutez un privilège d'utilisateur DRAC à Administrateur, Utilisateur privilégié ou Invité, le **groupe DRAC** bascule sur le groupe **Personnalisé**.
6. Lorsque vous avez terminé, cliquez sur **Appliquer les modifications**.
7. Cliquez sur le bouton approprié de la page **Configuration de l'utilisateur** pour continuer. Reportez-vous à la section Tableau 5-6.

Tableau 5-1. Options de la section Configuration de la carte à puce

Option	Description
Télécharger le certificat de l'utilisateur	Vous permet de télécharger le certificat de l'utilisateur sur le DRAC et de l'importer dans le profil de l'utilisateur.
Consulter le certificat de l'utilisateur	Affiche la page Certificat de l'utilisateur qui a été téléchargée sur le DRAC.
Télécharger le certificat CA de confiance	Vous permet de télécharger le certificat CA de confiance sur le DRAC 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 le DRAC. Le certificat CA de confiance est émis par la CA qui est autorisée à délivrer des certificats aux utilisateurs.

Tableau 5-2. Propriétés générales

Propriété	Description
ID d'utilisateur	Spécifie l'un des 16 ID d'utilisateur prédéfinis. Si vous modifiez des informations pour l'utilisateur root, ce champ est statique. Vous ne pouvez pas modifier le nom d'utilisateur root.
Activer l'utilisateur	Permet à l'utilisateur d'accéder au DRAC 5. Lorsque cette option n'est pas sélectionnée, le nom d'utilisateur ne peut pas être modifié.
Nom d'utilisateur	Spécifie un nom d'utilisateur DRAC 5 comprenant jusqu'à 16 caractères. Chaque utilisateur doit avoir un nom d'utilisateur unique.

	REMARQUE : Les noms d'utilisateur sur le DRAC 5 local ne peuvent pas contenir le caractère **@ (arobase), \ (barre oblique inversée), " (guillemet), / (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.
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	Spécifie ou modifie le mot de passe de l'utilisateur du DRAC 5.
Confirmer le nouveau mot de passe	Vous devez saisir de nouveau le mot de passe de l'utilisateur du DRAC 5 pour le confirmer.

Tableau 5-3. 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 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 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 la communication IPMI série sur LAN. Lorsque cette option est sélectionnée, ce privilège est activé.

Tableau 5-4. Privilèges d'utilisateur du DRAC

Propriété	Description
Groupe DRAC	Spécifie le privilège maximum de l'utilisateur du DRAC sur un des groupes d'utilisateurs suivants : **Administrateur**, **Utilisateur privilégié**, **Invité**, **Aucun** ou **Personnalisé**. Voir Tableau 5-5 pour connaître les droits **Groupe DRAC**.
Ouvrir une session sur le DRAC	Permet à l'utilisateur d'ouvrir une session sur le DRAC.
Configurer le DRAC	Permet à l'utilisateur de configurer le DRAC.
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 du DRAC.
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.

Tableau 5-5. Droits Groupe DRAC

Groupe d'utilisateurs	Droits accordés
Administrateur	**Ouvrir une session sur le DRAC**, **Configurer le DRAC**, **Configurer les utilisateurs**, **Effacer les journaux**, **Exécuter les commandes de contrôle du serveur**, **Accéder à la redirection de console**, **Accéder au média virtuel**, **Tester les alertes**, **Exécuter des commandes de diagnostic**
Utilisateur privilégié	**Ouvrir une session sur le DRAC**, **Effacer les journaux**, **Exécuter les commandes de contrôle du serveur**, **Accéder à la redirection de console**, **Accéder au média virtuel**, **Tester les alertes**
Invité	**Ouvrir une session sur le DRAC**
Personnalisé	Sélectionne n'importe quelle combinaison parmi les droits suivants : **Ouvrir une session sur le DRAC**, **Configurer le DRAC**, **Configurer les utilisateurs**, **Effacer les journaux**, **Exécuter des commandes d'action du serveur**, **Accéder à la redirection de console**, **Accéder au média virtuel**, **Tester les alertes**, **Exécuter des commandes de diagnostic**
Aucun.	Aucun droit attribué

Tableau 5-6. Boutons de la page Configuration de l'utilisateur

Bouton	Action
Imprimer	Imprime la page **Configuration de l'utilisateur**
Actualiser	Recharge la page **Configuration de l'utilisateur**
Retour à la page Utilisateurs	Retourne à la **page Utilisateurs**.
Appliquer les modifications	Enregistre les modifications apportées à la configuration réseau.

Utilisation de l'utilitaire RACADM pour configurer les utilisateurs du DRAC 5

REMARQUE : Vous devez avoir ouvert une session en tant qu'utilisateur **root** pour exécuter les commandes RACADM sur un système Linux distant.

L'interface Web du DRAC 5 représente le moyen le plus rapide de configurer un DRAC 5. Si vous préférez la configuration par ligne de commande ou script ou si vous devez configurer plusieurs DRAC 5, utilisez RACADM qui est installé avec les agents DRAC 5 sur le système géré.

Pour configurer plusieurs DRAC 5 avec des paramètres de configuration identiques, effectuez 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 du DRAC 5 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 du DRAC 5. Avant d'activer manuellement un utilisateur DRAC 5, vérifiez s'il existe des utilisateurs actuels. Si vous configurez un nouveau DRAC 5 ou 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 du DRAC 5.

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 numéro d'index différent sur chaque DRAC 5.

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 du DRAC 5.

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 par ce nom d'utilisateur.

REMARQUE : Lorsque vous activez ou désactivez manuellement un utilisateur avec la sous-commande **racadm config**, vous *devez* spécifier l'index avec l'option **-i**. L'objet **cfgUserAdminIndex** affiché dans l'exemple précédent contient un caractère « # ». De même, si vous utilisez la commande **racadm config -f racadm.cfg** pour spécifier un nombre de groupes/d'objets à écrire, l'index ne peut pas être spécifié. Un nouvel utilisateur est ajouté au premier index disponible. Ceci permet une plus grande flexibilité pour configurer plusieurs DRAC 5 avec les mêmes paramètres.

Ajout d'un utilisateur DRAC 5

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. Définissez les privilèges d'utilisateur.
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 cfgUserPrivilege 0x00000001

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 DRAC 5

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 null de guillemets ("") donne l'ordre au DRAC 5 de supprimer la configuration utilisateur à l'index indiqué et de réinitialiser les valeurs d'usine par défaut de la configuration utilisateur.

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 « **testemail** » pour configurer ces paramètres.

Activation d'un utilisateur DRAC 5 ayant 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 à la page su sommaire

Retour à la page su sommaire

Utilisation du DRAC 5 avec Microsoft Active Directory

Dell™ Remote Access Controller 5 Guide d'utilisation de la version 1.45 du micrologiciel

Un service de répertoire 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 déjà le logiciel de service Microsoft® Active Directory®, vous pouvez le configurer pour donner accès au DRAC 5, ce qui vous permet d'ajouter et de contrôler les privilèges utilisateur du DRAC 5 pour les utilisateurs existants dans votre logiciel Active Directory.

REMARQUE : L'utilisation d'Active Directory pour reconnaître les utilisateurs du DRAC 5 est prise en charge sur les systèmes d'exploitation Microsoft Windows® 2000, Windows Server® 2003 et Windows Server 2008.

Prérequis pour l'activation de l'authentification Active Directory pour le DRAC 5

Pour utiliser la fonctionnalité Authentification Active Directory du DRAC 5, vous devez déjà avoir déployé une infrastructure Active Directory. L'authentification Active Directory du DRAC 5 prend en charge l'authentification sur plusieurs arborescences dans une seule forêt. Voir « Configuration Active Directory prise en charge » pour des informations sur la configuration Active Directory prise en charge par rapport au niveau de fonction de domaine, des groupes, des objets, etc.

Consultez le site Web Microsoft pour des informations sur la configuration d'une infrastructure Active Directory si vous n'en avez pas déjà une.

Le DRAC 5 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 aurez également besoin d'activer le protocole Secure Socket Layer (SSL) sur tous les contrôleurs de domaine. 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 des utilisateurs sur le DRAC 5 au moyen de deux méthodes : vous pouvez utiliser une solution de *schéma standard*, qui utilise uniquement les objets du groupe Active Directory, ou vous pouvez utiliser la solution de *schéma étendu*, que Dell a personnalisée pour y ajouter des objets Active Directory définis par Dell. Pour plus d'informations sur ces solutions, consultez les sections ci-dessous.

Lorsque vous utilisez Active Directory pour configurer l'accès au DRAC 5, vous devez choisir la solution de schéma étendu ou la solution de schéma standard.

La solution de schéma standard comporte les avantages suivants :

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

La solution de schéma étendu présente les avantages suivants :

- Tous les objets de contrôle d'accès sont maintenus dans Active Directory.
- Flexibilité maximale lors de la configuration de l'accès des utilisateurs sur différentes cartes DRAC 5 avec différents niveaux de privilèges.

Présentation d'Active Directory avec le schéma standard

Comme illustré dans le figure 6-1, l'utilisation du schéma standard pour l'intégration d'Active Directory nécessite une configuration sur Active Directory et sur le DRAC 5. Du côté d'Active Directory, un objet de groupe standard est utilisé comme groupe de rôles. Un utilisateur pouvant accéder au DRAC 5 sera membre du groupe de rôles. Afin de donner à cet utilisateur l'accès à une carte DRAC 5 spécifique, le nom du groupe de rôles et son nom de domaine doivent être configurés sur la carte DRAC 5 spécifique. À l'inverse de la solution de schéma étendu, le rôle et le niveau de privilège sont définis sur chaque carte DRAC 5, et non dans Active Directory. Il est possible de configurer et de définir jusqu'à cinq groupes de rôles dans chaque DRAC 5. Tableau 6-12 présente le niveau de privilège des groupes de rôles et le tableau 6-1 illustre les paramètres par défaut des groupes de rôles.

Figure 6-1. Configuration du DRAC 5 avec Microsoft Active Directory et le schéma standard

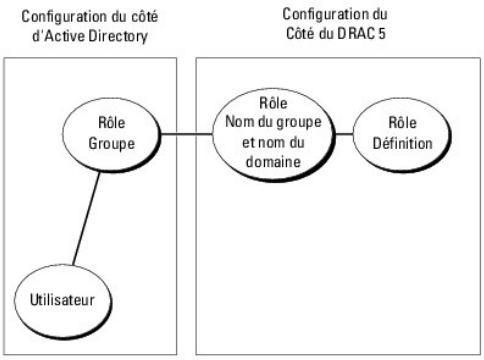


Tableau 6-1. Privilèges par défaut des groupes de rôles

Groupes de rôles	Niveau de privilège par défaut	Droits accordés	Masque binaire
Groupe de rôles 1	Administrateur	**Ouvrir une session sur le DRAC**, **Configurer le DRAC**, **Configurer les utilisateurs**, **Effacer les journaux**, **Exécuter les commandes de contrôle du serveur**, **Accéder à la redirection de console**, **Accéder au média virtuel**, **Tester les alertes**, **Exécuter des commandes de diagnostic**	0x000001ff
Groupe de rôles 2	Utilisateur privilégié	**Ouvrir une session sur le DRAC**, **Effacer les journaux**, **Exécuter les commandes de contrôle du serveur**, **Accéder à la redirection de console**, **Accéder au média virtuel**, **Tester les alertes**	0x000000f9
Groupe de rôles 3	Invité	Ouvrir une session sur le DRAC	0x00000001
Groupe de rôles 4	Aucun.	Aucun droit attribué	0x00000000
Groupe de rôles 5	Aucun.	Aucun droit attribué	0x00000000

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

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

- Avec l'interface utilisateur Web du DRAC 5. Voir « Configuration du DRAC 5 avec Active Directory avec le schéma standard et l'interface Web ».
- Avec l'outil CLI RACADM. Voir « Configuration du DRAC 5 avec Active Directory avec le schéma standard et la RACADM ».

Configuration d'Active Directory avec le schéma standard pour accéder au DRAC 5

Vous devez effectuer les étapes suivantes pour configurer Active Directory pour qu'un utilisateur d'Active Directory puisse accéder au DRAC 5 :

1. Sur un serveur Active Directory (contrôleur de domaine), ouvrez le snap-in Utilisateurs et ordinateurs Active Directory.
2. Créez un groupe ou sélectionnez un groupe existant. Le nom du groupe et le nom de ce domaine devront être configurés sur le DRAC 5 avec l'interface Web ou avec la RACADM (voir « Configuration du DRAC 5 avec Active Directory avec le schéma standard et l'interface Web » ou « Configuration du DRAC 5 avec Active Directory avec le schéma standard et la RACADM »).
3. Ajoutez l'utilisateur d'Active Directory en tant que membre du groupe Active Directory pour qu'il accède au DRAC 5.

Configuration du DRAC 5 avec Active Directory avec le schéma standard et l'interface Web

1. Ouvrez une fenêtre d'un navigateur Web pris en charge.
2. Ouvrez une session sur l'interface Web du DRAC 5.
3. Développez l'arborescence du **système** et cliquez sur **Accès distant**.
4. Cliquez sur l'onglet **Configuration** et sélectionnez **Active Directory**.
5. Sur la page **Menu principal d'Active Directory**, sélectionnez **Configurer Active Directory** et cliquez sur **Suivant**.
6. Dans la section Paramètres communs :

a. Sélectionnez la case à cocher **Activer Active Directory**.

b. Tapez le **nom de domaine racine**. Le **nom de domaine racine** est le nom de domaine racine pleinement qualifié de la forêt.

c. Tapez le **Délai d'attente** en secondes.

7. Cliquez sur **Utiliser le schéma standard** dans la section Sélection du schéma d'Active Directory.

8. Cliquez sur **Appliquer** pour enregistrer les paramètres Active Directory.

9. Dans la colonne **Groupes de rôles** de la section Paramètres du schéma standard, cliquez sur un **Groupe de rôles**.

   La page **Configurer un groupe de rôles** apparaît et comprend le **Nom du groupe**, **Domaine du groupe** et **Privilèges du groupe de rôles** d'un groupe de rôles.

10. Saisissez le **Nom du groupe**. Le nom du groupe identifie le groupe de rôles dans Active Directory associé à la carte DRAC 5.

11. Saisissez le **Domaine du groupe**. Le **Domaine du groupe** est le nom de domaine racine pleinement qualifié de la forêt.

12. Dans la page **Privilèges du groupe de rôles**, définissez les privilèges du groupe.

    Tableau 6-12 décrit les **Privilèges du groupe de rôles**.

    Tableau 6-13 décrit les **Droits du groupe de rôles**. Si vous modifiez des droits, le **privilège du groupe de rôles** actuel (administrateur, utilisateur privilégié ou utilisateur invité) devient celui d'un groupe personnalisé ou un privilège de groupe de rôles correspondant aux droits modifiés.

13. Cliquez sur **Appliquer** pour enregistrer les paramètres Groupe de rôles.

14. Cliquez sur **Retourner à la configuration et à la gestion d'Active Directory**.

15. Cliquez sur **Retourner au menu principal d'Active Directory**.

16. Téléchargez votre certificat CA racine de la forêt de domaines dans le DRAC 5.

    a. Cochez la case **Télécharger le certificat CA d'Active Directory**, puis cliquez sur **Suivant**.

    b. Sur la page **Téléchargement d'un certificat**, tapez le chemin d'accès du fichier du certificat ou naviguez vers le fichier du certificat.

    REMARQUE : La valeur **Chemin d'accès au fichier** affiche le chemin de fichier relatif du certificat que vous téléchargez. Vous devez entrer le chemin de fichier absolu, y compris le chemin et le nom de fichier complets et l'extension du fichier.

    Les certificats SSL des contrôleurs de domaine doivent avoir été signés par la CA racine. Vérifiez que le certificat CA racine est disponible sur votre station de gestion accédant au DRAC 5 (voir « Exportation du certificat CA racine du contrôleur de domaine sur le DRAC 5 »).

    c. Cliquez sur **Appliquer**.

    DRAC 5 Web Server redémarre automatiquement après que vous avez cliqué sur **Appliquer**.

17. Fermez la session, puis rouvrez une session sur le DRAC 5 pour terminer la configuration de la fonctionnalité Active Directory du DRAC 5.

18. Dans l'arborescence du **système**, cliquez sur **Accès distant**.

19. Cliquez sur l'onglet **Configuration**, puis sur **Réseau**.

    La page **Configuration du réseau** apparaît.

20. Si **Utiliser DHCP (pour l'adresse IP du NIC)** est sélectionné sous **Paramètres réseau**, sélectionnez Utiliser DHCP pour obtenir l'adresse du serveur DNS.

    Pour saisir manuellement l'adresse IP du serveur DNS, désélectionnez **Utiliser DHCP pour obtenir des adresses de serveur DNS** et tapez les adresses IP de serveur DNS principale et secondaire.

21. Cliquez sur **Appliquer les modifications**.

    La configuration de la fonctionnalité Active Directory avec le schéma standard du DRAC 5 est terminée.

Configuration du DRAC 5 avec Active Directory avec le schéma standard et la RACADM

Utilisez les commandes suivantes pour configurer la fonctionnalité Active Directory du DRAC 5 avec le schéma standard en utilisant la CLI RACADM au lieu de l'interface Web.

1. Ouvrez une invite de commande et tapez les commandes racadm suivantes :

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

racadm config -g cfgActiveDirectory -o cfgADType 2

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

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

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

racadm config -g cfgStandardSchema -i <index> -o cfgSSADRoleGroupPrivilege <nombre de masques binaires pour les droits d'utilisateur spécifiques>

racadm sslcertupload -t 0x2 -f <certificat CA racine ADS>

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

REMARQUE : Pour les valeurs numériques Masque binaire, voir Tableau B-4.

2. Si DHCP est activé sur le DRAC 5 et que vous voulez utiliser le DNS fourni par le serveur DHCP, tapez les commandes racadm suivantes :

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

3. Si DHCP est désactivé sur le DRAC 5 ou que vous voulez saisir manuellement l'adresse IP du DNS, tapez les commandes racadm suivantes :

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

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

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

Au lieu de demander au DRAC 5 de rechercher des serveurs Active Directory, vous pouvez spécifier les serveurs auxquels le DRAC 5 doit se connecter pour authentifier l'utilisateur. Consultez « Spécifier un serveur pour la configuration d'Active Directory » pour obtenir des informations sur les commandes RACADM à utiliser pour spécifier des serveurs.

Présentation d'Active Directory avec le schéma étendu

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

- Avec l'interface utilisateur Web du DRAC 5. Voir « Configuration du DRAC 5 avec Active Directory avec le schéma étendu et l'interface Web ».
- Avec l'outil CLI?RACADM. Voir « Configuration du DRAC 5 avec Active Directory avec le schéma étendu et la RACADM ».

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 qui 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 maintenir des ID uniques partout dans le monde, Microsoft maintient une base de données des identificateurs d'objets (OID) Active Directory de sorte que lorsque des sociétés ajoutent des extensions au schéma, elles sont certaines que celles-ci sont uniques et n'entrent pas en conflit les unes avec les 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 de répertoire.

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

La base de données OID d'Active Directory maintenue par Microsoft est disponible à l'adresse **http://msdn.microsoft.com/certification/ADAcctInfo.asp** en entrant notre extension Dell.

Présentation des extensions de schéma du RAC

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 RAC. Ce modèle offre à l'administrateur un maximum de flexibilité sur les différentes combinaisons d'utilisateurs, de privilèges du RAC et de périphériques RAC sur le réseau, sans ajouter trop de complexité.

Aperçu des objets Active Directory

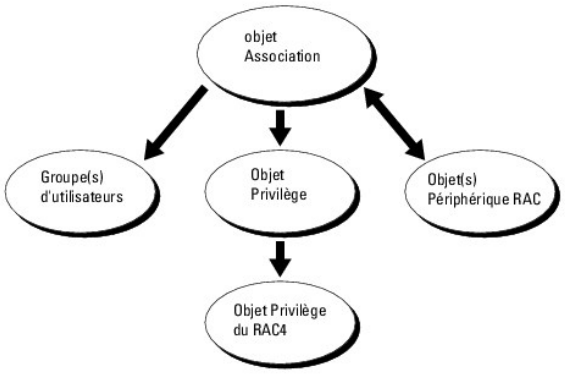
Pour chacun des RAC physiques présents sur le réseau que vous voulez intégrer à Active Directory en vue de l'authentification et de l'autorisation, vous devez créer au moins un objet Association et un objet Périphérique RAC. Vous pouvez créer plusieurs objets Association et chaque objet Association peut être lié à autant d'utilisateurs, de groupes d'utilisateurs ou d'objets Périphérique RAC que vous le souhaitez. Les utilisateurs et les objets Périphérique RAC peuvent être des membres de n'importe quel domaine dans l'entreprise.

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

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

Figure 6-2 illustre le fait que l'objet Association fournit la connexion nécessaire pour toute authentification et autorisation.

Figure 6-2. Configuration typique pour les objets Active Directory



REMARQUE : L'objet Privilège du RAC s'applique tant au DRAC 4 qu'au DRAC 5.

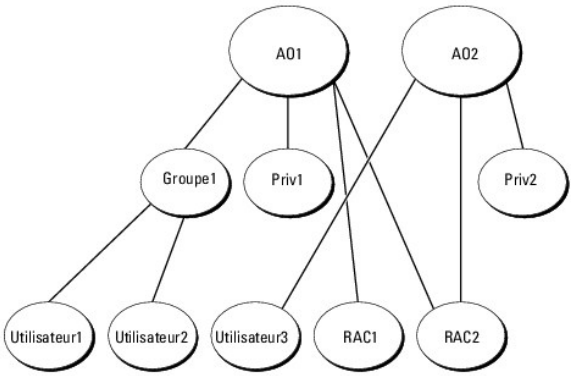
Vous pouvez créer autant d'objets Association que vous le voulez. Cependant, vous devez créer au moins un objet Association et vous devez avoir un objet Périphérique RAC pour chaque RAC (DRAC 5) sur le réseau que vous voulez intégrer avec Active Directory pour l'authentification et l'autorisation avec le RAC (DRAC 5).

L'objet Association inclut autant d'utilisateurs et/ou de groupes que d'objets Périphérique RAC. Toutefois, l'objet Association ne peut inclure qu'un objet Privilège par objet Association. L'objet Association connecte les « Utilisateurs » qui ont des « Privilèges » sur les RAC (DRAC 5).

En outre, vous pouvez configurer des objets Active Directory dans un domaine unique ou dans des domaines multiples. Par exemple, supposons que vous avez deux cartes DRAC 5 (RAC1 et RAC2) et trois utilisateurs Active Directory existants (Utilisateur1, Utilisateur2 et Utilisateur3). Vous voulez donner des privilèges d'administrateur à Utilisateur1 et à Utilisateur2 sur les deux cartes DRAC 5 et des privilèges d'ouverture de session à Utilisateur3 sur la carte RAC2. Figure 6-3 montre comment configurer les objets Active Directory dans ce scénario.

Lorsque vous ajoutez des groupes universels à partir de domaines séparés, créez un objet Association avec une étendue universelle. Les objets Association par défaut créés par l'utilitaire Dell Schema Extender sont des groupes locaux de domaines et ne fonctionnent pas avec les groupes universels d'autres domaines.

Figure 6-3. Définition d'objets Active Directory dans un domaine unique



Pour configurer les objets pour le scénario de domaine unique, effectuez les tâches suivantes :

1. Créez deux objets Association.

2. Créez deux objets Périphérique RAC, RAC1 et RAC2, pour représenter les deux cartes DRAC 5.

3. Créez deux objets Privilège, Priv1 et Priv2, dans lequel Priv1 a tous les privilèges (administrateur) et Priv2 a des privilèges d'ouverture de session.

4. Groupez Utilisateur1 et Utilisateur2 dans le Groupe1.

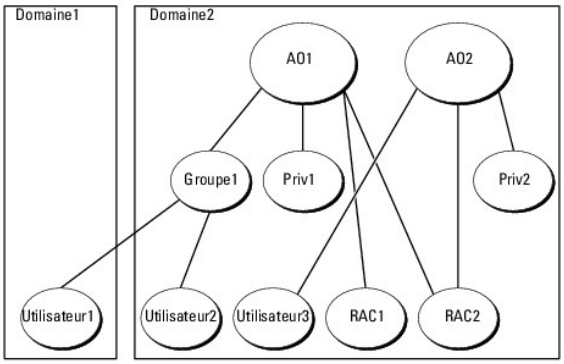
5. Ajoutez Groupe1 comme membre de l'objet Association 1 (AO1), Priv1 comme objets Privilège dans AO1, et RAC1 et RAC2 comme périphériques RAC dans AO1.

6. Ajoutez Utilisateur3 comme membre de l'objet Association 2 (AO2), Priv2 comme objets Privilège dans AO2 et RAC2 comme périphériques RAC dans AO2.

Voir « Ajout d'utilisateurs DRAC 5 et de leurs privilèges à Active Directory » pour des instructions détaillées.

Figure 6-4 fournit un exemple d'objets Active Directory dans de multiples domaines. Dans ce scénario, vous avez deux cartes DRAC 5 (RAC1 et RAC2) et trois utilisateurs Active Directory existants (Utilisateur1, Utilisateur2 et Utilisateur3). Utilisateur1 est dans le Domaine1 ; Utilisateur2 et Utilisateur3 sont dans le Domaine2. Dans ce scénario, configurez Utilisateur1 et Utilisateur2 avec les privilèges d'administrateur sur les deux cartes DRAC 5 et configurez Utilisateur3 avec les privilèges d'ouverture de session sur la carte RAC2.

Figure 6-4. Configuration des objets Active Directory dans des domaines multiples



Pour configurer les objets pour le scénario à domaines multiples, effectuez les tâches suivantes :

1. Assurez-vous que la fonction de forêt de domaines est en mode Natif ou Windows 2003.

2. Créez deux objets Association, AO1 (d'étendue universelle) et AO2, dans n'importe quel domaine.

   Figure 6-4 illustre les objets du Domaine2.

3. Créez deux objets Périphérique RAC, RAC1 et RAC2, pour représenter les deux cartes DRAC 5.

4. Créez deux objets Privilège, Priv1 et Priv2, dans lequel Priv1 a tous les privilèges (administrateur) et Priv2 a des privilèges d'ouverture de session.

5. Groupez Utilisateur1 et Utilisateur2 dans le Groupe1. L'étendue de groupe de Groupe1 doit être universelle.

6. Ajoutez Groupe1 comme membre de l'objet Association 1 (AO1), Priv1 comme objets Privilège dans AO1, et RAC1 et RAC2 comme périphériques RAC dans AO1.

7. Ajoutez Utilisateur3 comme membre de l'objet Association 2 (AO2), Priv2 comme objets Privilège dans AO2 et RAC2 comme périphériques RAC dans AO2.

Configuration d'Active Directory avec le schéma étendu pour accéder au DRAC 5

Pour pouvoir utiliser Active Directory pour accéder au DRAC 5, configurez le logiciel Active Directory et le DRAC 5 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 du DRAC 5 et leurs privilèges à Active Directory (voir « Ajout d'utilisateurs DRAC 5 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 du DRAC 5 à l'aide de l'interface Web du DRAC 5 ou de la RACADM (voir « Configuration du DRAC 5 avec Active Directory avec le schéma étendu et la RACADM » ou « Configuration du DRAC 5 avec Active Directory avec le schéma étendu et l'interface Web »).

Extension du schéma Active Directory

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 de 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 de DVD*:**\support\OMActiveDirectory Tools\RAC4-5\LDIF_Files**
- *Lecteur de DVD*:**\support\OMActiveDirectory Tools\RAC4-5\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

PRÉCAUTION : 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 6-2 à Tableau 6-7)
   - Attributs (Tableau 6-8)

   Consultez votre documentation Microsoft pour obtenir plus d'informations sur la façon d'activer et d'utiliser le snap-in du schéma Active Directory de la console MMC.

Tableau 6-2. Définitions de classe pour les classes ajoutées au schéma Active Directory

Nom de classe	Numéro d'identification d'objet attribué (OID)
dellRacDevice	1.2.840.113556.1.8000.1280.1.1.1.1
dellAssociationObject	1.2.840.113556.1.8000.1280.1.1.1.2
dellRACPrivileges	1.2.840.113556.1.8000.1280.1.1.1.3
dellPrivileges	1.2.840.113556.1.8000.1280.1.1.1.4
dellProduct	1.2.840.113556.1.8000.1280.1.1.1.5

Tableau 6-3. Classe dellRacDevice

OID	1.2.840.113556.1.8000.1280.1.1.1.1
Description	Représente le périphérique RAC de Dell. Le périphérique RAC doit être configuré comme dellRacDevice dans Active Directory. Cette configuration permet au DRAC 5 d'envoyer des requêtes LDAP (Lightweight Directory Access Protocol) à Active Directory.

Type de classe	Classe structurelle
SuperClasses	dellProduct
Attributs	**dellSchemaVersion** **dellRacType**

Tableau 6-4. Classe dellAssociationObject

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

Tableau 6-5. 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 DRAC 5.
Type de classe	Classe auxiliaire
SuperClasses	Aucun.
Attributs	**dellIsLoginUser** **dellIsCardConfigAdmin** **dellIsUserConfigAdmin** **dellIsLogClearAdmin** **dellIsServerResetUser** **dellIsConsoleRedirectUser** **dellIsVirtualMediaUser** **dellIsTestAlertUser** **dellIsDebugCommandAdmin**

Tableau 6-6. 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 6-7. 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 6-8. Liste des attributs ajoutés au schéma Active Directory

Nom / description de l'attribut	OID attribué/Identificateur d'objet de syntaxe	Valeur unique
dellPrivilegeMember	1.2.840.113556.1.8000.1280.1.1.2.1	FALSE

Liste des objets dellPrivilege qui appartiennent à cet Attribut.	Nom distingué (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	
dellProductMembers Liste des objets dellRacDevices qui appartiennent à ce rôle. Cet attribut est le lien vers l'avant vers le lien vers l'arrière dellAssociationMembers. Numéro de lien : 12070	1.2.840.113556.1.8000.1280.1.1.2.2 Nom distingué (LDAPTYPE_DN 1.3.6.1.4.1.1466.115.121.1.12)	FALSE
dellIsLoginUser TRUE si l'utilisateur a des 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 des 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 des 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 des 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 des 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 des 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 des 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 des 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 des 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 dellRacDevice 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 objets dellAssociationObjectMembers qui appartiennent 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 Active Directory pour que l'administrateur puisse gérer les périphériques RAC (DRAC 5), les utilisateurs et les groupes d'utilisateurs, les associations de RAC et les privilèges de RAC.

Lorsque vous installez votre logiciel Systems Management à l'aide du DVD *Dell Systems Management Tools and Documentation*, vous pouvez étendre le snap-in en sélectionnant l'option **Dell Extension sur le snap-in Utilisateurs et ordinateurs Active Directory** pendant la procédure d'installation. Consultez le *Guide d'installation rapide du logiciel Dell OpenManage* pour des instructions supplémentaires sur l'installation du logiciel Systems Management.

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

Installation du pack administrateur

Vous devez installer le pack administrateur sur tous les systèmes qui gèrent les objets DRAC 5 d'Active Directory. Si vous n'installez pas le pack administrateur, vous ne pouvez pas visualiser l'objet RAC Dell dans le conteneur.

Pour plus d'informations, voir « 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 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**, tapez `MMC` et appuyez sur **Entrée**.

   Ceci ouvre la console de gestion Microsoft (MMC).

2. Dans la fenêtre **Console 1**, cliquez sur **Fichier** (ou sur **Console** sur les systèmes exécutant Windows 2000).

3. Cliquez sur **Ajouter/Supprimer un snap-in**.

4. Sélectionnez un snap-in **Utilisateurs et ordinateurs Active Directory** et cliquez sur **Ajouter**.

5. Cliquez sur **Fermer** et cliquez sur **OK**.

Ajout d'utilisateurs DRAC 5 et de leurs privilèges à Active Directory

Le snap-in Utilisateurs et ordinateurs Active Directory étendu par Dell vous permet d'ajouter des utilisateurs DRAC 5 et des privilèges en créant des objets RAC, Association et Privilège. Pour ajouter chaque type d'objet, effectuez les procédures suivantes :

- Créez un objet Périphérique RAC
- Créez un objet Privilège
- Créez un objet Association
- Ajoutez des objets à un objet Association

Création d'un objet Périphérique RAC

1. Dans la fenêtre **Racine de la console** MMC, cliquez-droite sur un conteneur.

2. Sélectionnez **Nouveau**→ **Objet RAC Dell**.

   La fenêtre **Nouvel objet** apparaît.

3. Tapez un nom pour le nouvel objet. Le nom doit être identique au nom du DRAC 5 que vous tapez dans étape a de « Configuration du DRAC 5 avec Active Directory avec le schéma étendu et l'interface Web ».

4. Sélectionnez **Objet Périphérique RAC**.

5. Cliquez sur **OK**.

Création d'un objet Privilège

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

1. Dans la fenêtre **Racine de la console** (MMC), cliquez-droite sur un conteneur.

2. Sélectionnez **Nouveau**→ **Objet RAC Dell**.

   La fenêtre **Nouvel objet** apparaît.

3. Tapez un nom pour le nouvel objet.

4. Sélectionnez **Objet Privilège**.

5. Cliquez sur **OK**.

6. Cliquez-droite sur l'objet Privilège que vous avez créé et sélectionnez **Propriétés**.

7. Cliquez sur l'onglet **Privilèges RAC** et sélectionnez les privilèges à attribuer à l'utilisateur (pour des informations supplémentaires, voir Tableau 5-4).

Création d'un objet Association

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

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

1. Dans la fenêtre **Racine de la console** (MMC), cliquez-droite sur un conteneur.

2. Sélectionnez **Nouveau→ Objet RAC 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**.

Ajout d'objets à un objet Association

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

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

Ajout d'utilisateurs ou de groupes d'utilisateurs

1. Cliquez-droite sur **l'objet Association** et sélectionnez **Propriétés**.

2. Sélectionnez l'onglet **Utilisateurs** et cliquez sur **Ajouter**.

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

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

Ajout de privilèges

1. Sélectionnez l'onglet **Objet 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 ou plusieurs périphériques RAC à l'association. Les périphériques associés spécifient les périphériques RAC connectés au réseau qui sont disponibles pour les utilisateurs ou les groupes d'utilisateurs définis. Vous pouvez ajouter plusieurs périphériques RAC à un objet Association.

Ajout de périphériques RAC ou de groupes de périphériques RAC

Pour ajouter des périphériques RAC ou des groupes de périphériques RAC :

1. Sélectionnez l'onglet **Produits** et cliquez sur **Ajouter**.

2. Tapez le nom du périphérique RAC ou du groupe de périphériques RAC et cliquez sur **OK**.

3. Dans la fenêtre **Propriétés**, cliquez sur **Appliquer**, puis sur **OK**.

Configuration du DRAC 5 avec Active Directory avec le schéma étendu et l'interface Web

1. Ouvrez une fenêtre d'un navigateur Web pris en charge.
2. Ouvrez une session sur l'interface Web du DRAC 5.
3. Développez l'arborescence du **système** et cliquez sur **Accès distant**.
4. Cliquez sur l'onglet **Configuration** et sélectionnez **Active Directory**.
5. Sur la page **Menu principal d'Active Directory**, sélectionnez **Configurer Active Directory** et cliquez sur **Suivant**.
6. Dans la section Paramètres communs :
   a. Sélectionnez la case à cocher **Activer Active Directory**.
   b. Tapez le **nom de domaine racine**. Le **nom de domaine racine** correspond au nom de domaine racine pleinement qualifié de la forêt.
   c. Tapez le **Délai d'attente** en secondes.
7. Cliquez sur **Utiliser le schéma étendu** dans la section Sélection du schéma d'Active Directory.
8. Dans la section Paramètres du schéma étendu :
   a. Tapez le **Nom du DRAC**. Ce nom doit être identique au nom courant du nouvel objet RAC que vous avez créé dans votre contrôleur de domaine (voir étape 3 de Création d'un objet Périphérique RAC).
   b. Tapez le N**om de domaine du DRAC** (par exemple, `drac5.com`). N'utilisez pas le nom NetBIOS. Le **Nom de domaine du DRAC** est le nom de domaine pleinement qualifié du sous-domaine où l'objet Périphérique RAC se trouve.
9. Cliquez sur **Appliquer** pour enregistrer les paramètres Active Directory.
10. Cliquez sur **Retourner au menu principal d'Active Directory**.
11. Téléchargez votre certificat CA racine de la forêt de domaines dans le DRAC 5.
    a. Cochez la case **Télécharger le certificat CA d'Active Directory**, puis cliquez sur **Suivant**.
    b. Sur la page **Téléchargement d'un certificat**, tapez le chemin d'accès du fichier du certificat ou naviguez vers le fichier du certificat.

    REMARQUE : La valeur **Chemin d'accès au fichier** affiche le chemin de fichier relatif du certificat que vous téléchargez. Vous devez entrer le chemin de fichier absolu, y compris le chemin et le nom de fichier complets et l'extension du fichier.

    Les certificats SSL des contrôleurs de domaine doivent avoir été signés par la CA racine. Tenez le certificat CA racine disponible sur votre station de gestion accédant au DRAC 5 (voir « Exportation du certificat CA racine du contrôleur de domaine sur le DRAC 5 »).

    c. Cliquez sur **Appliquer**.

    DRAC 5 Web Server redémarre automatiquement après que vous avez cliqué sur **Appliquer**.
12. Fermez la session, puis rouvrez une session sur le DRAC 5 pour terminer la configuration de la fonctionnalité Active Directory du DRAC 5.
13. Dans l'arborescence du **système**, cliquez sur **Accès distant**.
14. Cliquez sur l'onglet **Configuration**, puis sur **Réseau**.

    La page **Configuration du réseau** apparaît.
15. Si **Utiliser DHCP (pour l'adresse IP du NIC)** est sélectionné dans **Paramètres réseau**, alors sélectionnez **Utiliser DHCP pour obtenir l'adresse du serveur DNS**.

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

    La configuration de la fonctionnalité Active Directory avec le schéma étendu du DRAC 5 est terminée.

Configuration du DRAC 5 avec Active Directory avec le schéma étendu et la RACADM

Utilisez les commandes suivantes pour configurer la fonctionnalité Active Directory du DRAC 5 avec le schéma étendu en utilisant l'outil CLI RACADM au lieu de l'interface Web.

1. Ouvrez une invite de commande et tapez les commandes racadm suivantes :

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

   racadm config -g cfgActiveDirectory -o cfgADType 1

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

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

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

   racadm sslcertupload -t 0x2 -f <certificat CA racine ADS>

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

2. Si DHCP est activé sur le DRAC 5 et que vous voulez utiliser le DNS fourni par le serveur DHCP, tapez la commande racadm suivante :

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

3. Si DHCP est désactivé sur le DRAC 5 ou si vous voulez saisir l'adresse IP du DNS, tapez les commandes racadm suivantes :

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

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

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

Appuyez sur **Entrée** pour terminer la configuration de la fonctionnalité Active Directory du DRAC 5.

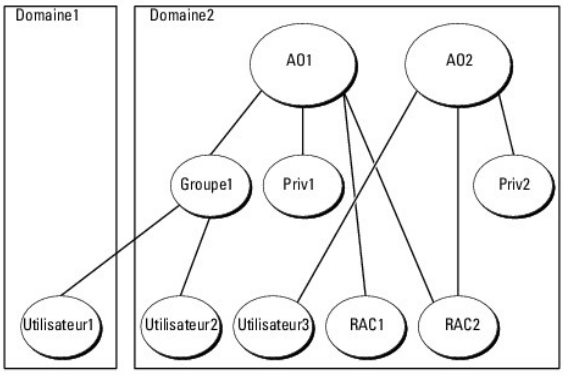
Au lieu de demander au DRAC 5 de rechercher des serveurs Active Directory, vous pouvez spécifier les serveurs auxquels le DRAC 5 doit se connecter pour authentifier l'utilisateur. Consultez « Spécifier un serveur pour la configuration d'Active Directory » pour obtenir des informations sur les commandes RACADM à utiliser pour spécifier des serveurs.

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.

Figure 6-5 fournit un exemple d'accumulation de privilèges à l'aide du schéma étendu.

Figure 6-5. Accumulation de privilèges pour un utilisateur



La figure illustre deux objets Association, A01 et A02. Ces objets Association peuvent faire partie du même domaine ou de domaines différents. Utilisateur1 est associé à RAC1 et à RAC2 via les deux objets Association. Par conséquent, Utilisateur1 a accumulé des privilèges résultant de l'association de l'ensemble des privilèges pour les objets Priv1 et Priv2.

Par exemple, Priv1 possède les privilèges Ouvrir une session, Média virtuel et Effacer les journaux et Privr2 a les privilèges Ouvrir une session, Configurer le DRAC et Tester les alertes. Utilisateur1 aura maintenant l'ensemble de privilèges Ouvrir une session, Média virtuel, Effacer les journaux, Configurer le DRAC et Tester les alertes, qui correspond à l'ensemble de privilèges associé de Priv1 et Priv2.

L'authentification du schéma étendu accumule ainsi 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.

Spécifier un serveur pour la configuration d'Active Directory

Si, pour rechercher un nom d'utilisateur, vous souhaitez spécifier un LDPA, un serveur de catalogue global ou un domaine d'objet Association (applicable uniquement pour le schéma étendu) au lieu d'utiliser les serveurs retournés par le serveur DNS, tapez la commande suivante pour activer l'option **Spécifier un serveur** :

```
racadm config -g cfgActive Directory -o cfgADSpecifyServer Enable 1
```

REMARQUE : Si vous utilisez cette option, le nom de l'hôte dans le certificat CA ne correspond pas au nom du serveur spécifié. Ceci est tout particulièrement utile si vous êtes un administrateur DRAC car cela vous permet de saisir un nom d'hôte ainsi qu'une adresse IP.

Une fois l'option **Spécifier un serveur** activée, vous pouvez spécifier un serveur LDAP ou de catalogue global avec une adresse IP ou un nom de domaine pleinement qualifié du serveur (FQDN). Le FQDN se compose du nom de l'hôte et du nom de domaine du serveur.

REMARQUE : Si vous utilisez une authenification Active Directory basée sur Kerberos, spécifiez uniquement le FQDN du serveur ; en indiquant que l'adresse IP n'est pas supportée. Pour plus d'informations, voir « Activation de l'authentification Kerberos ».

Pour spécifier un serveur LDAP à l'aide de l'interface de ligne de commande (CLI), tapez :

```
racadm config -g cfgActive Directory -o cfgADDomainController <nom de domaine pleinement qualifié ou adresse IP>
```

Pour spécifier un serveur de catalogue global à l'aide de l'interface de ligne de commande (CLI), tapez :

```
racadm config -g cfgActive Directory -o cfgGlobalCatalog <nom de domaine pleinement qualifié ou adresse IP>
```

Pour spécifier un domaine d'objet Association (applicable uniquement pour le schéma étendu) à l'aide de la CLI, tapez :

```
racadm config -g cfgActive Directory -o cfgGlobalCatalog <nom de domaine pleinement qualifié ou adresse IP>
```

où <domaine> est le domaine où l'objet Association réside et IP/FQDN est l'adresse IP ou le FQDN de l'hôte spécifié (Contrôleur de domaine) auquel le DRAC 5 se connecte.

Pour spécifier l'objet Association, assurez-vous de fournir également l'IP ou le FQDN du catalogue global.

REMARQUE : Si vous spécifiez l'adresse IP 0.0.0.0, le DRAC 5 ne recherche pas de serveur.

Vous pouvez spécifier une liste de serveurs LDAP, de catalogue global ou d'objets d'association séparés par des virgules. Le DRAC 5 vous permet de spécifier jusqu'à trois adresses IP ou noms d'hôte.

Si LDAPS n'est pas correctement configuré pour tous les domaines et applications, son activation peut entraîner des résultats inattendus pendant le fonctionnement des applications/domaines existants.

Pour le schéma étendu, vous pouvez spécifier soit un contrôleur de domaine, soit un catalogue global avec l'objet Association. Le fait de spécifier uniquement le catalogue global ou uniquement l'objet Association ne s'applique pas au schéma étendu. Si vous spécifiez uniquement le contrôleur de domaine, tous les objets, y compris Utilisateur, Groupe, RAC, Privilège et Association doivent se trouver dans le même domaine. Si l'un de ces objets figure dans des domaines différents, utilisez l'option Catalogue global avec objet Association. Vous pouvez spécifier jusqu'à quatre contrôleurs de domaine et toutes ces entrées doivent désigner le même domaine. Vous pouvez spécifier jusqu'à quatre serveurs de catalogue global. Vous pouvez spécifier jusqu'à quatre serveurs d'objet Association. Toutes ces entrées doivent indiquer le même domaine. Si vous utilisez l'option Objet Association, vous devez également configurer l'option Catalogue global pour pouvoir ouvrir une session. Spécifiez le nom du contrôleur de domaine sur lequel vous avez créé l'utilisateur. Vous pouvez spécifier l'IP ou le FQDN ici.

Pour le schéma standard, spécifiez uniquement le contrôleur de domaine et le catalogue global. Spécifier un objet Association ne s'applique pas au schéma standard. Vous pouvez spécifier le contrôleur de domaine sur lequel les groupes de rôles d'utilisateur sont créés. Spécifiez soit l'IP, soit le FQDN. Vous pouvez spécifier jusqu'à quatre contrôleurs de domaine. Toutes les entrées doivent indiquer le même domaine. Si vous spécifiez uniquement le contrôleur de domaine, l'utilisateur et le groupe doivent figurer dans le même domaine. Si les groupes de rôles se trouvent dans des domaines différents, vous devez également spécifier le serveur de catalogue global. Vous pouvez spécifier jusqu'à quatre serveurs de catalogue global. Vous pouvez spécifier l'IP ou le FQDN ici. Vous pouvez également spécifier uniquement les serveurs de catalogue global.

Configuration et gestion des certificats Active Directory

Pour accéder au menu principal d'Active Directory :

1. Développez l'arborescence du **système** et cliquez sur **Accès distant**.
2. Cliquez sur l'onglet **Configuration**, puis sur **Active Directory**.

Tableau 6-9 répertorie les options de la page **Menu principal d'Active Directory**.

Tableau 6-9. Options de la page Menu principal d'Active Directory

Champ	Description
Configurer Active Directory	Configure les paramètres Nom du DRAC d'Active Directory, Nom du domaine ROOT, Nom du domaine du DRAC, Délai d'attente de l'authentification Active Directory, Sélection du schéma Active Directory et Groupe de rôles.
Télécharger le certificat CA d'Active Directory	Télécharge un certificat Active Directory sur le DRAC.
Télécharger un certificat de serveur DRAC	Windows Download Manager vous permet de télécharger un certificat de serveur DRAC sur votre système.

Afficher le certificat CA d'Active Directory	Affiche le certificat Active Directory qui a été téléchargé sur le DRAC.

Configuration d'Active Directory (schéma standard et schéma étendu)

1. Sur la page **Menu principal d'Active Directory**, sélectionnez **Configurer Active Directory** et cliquez sur **Suivant**.
2. Sur la page **Configuration et gestion d'Active Directory**, saisissez les paramètres d'Active Directory.

   Tableau 6-10 décrit les paramètres de la page **Configuration et gestion d'Active Directory**.
3. Cliquez sur **Appliquer** pour enregistrer les paramètres.
4. Cliquez sur le bouton approprié de la page **Configuration d'Active Directory** pour continuer. Reportez-vous à la section Tableau 6-11.
5. Pour configurer les groupes de rôles pour le schéma standard d'Active Directory, cliquez sur le groupe de rôles individuel (1-5). Reportez-vous aux sections Tableau 6-12 et Tableau 6-13.

REMARQUE : Pour enregistrer les paramètres sur la page **Configuration et gestion d'Active Directory**, vous devez cliquer sur **Appliquer** avant de passer à la page **Groupe de rôles personnalisé**.

Tableau 6-10. Paramètres de la page Configuration et gestion d'Active Directory

Paramètre	Description
Activer Active Directory	Active Active Directory. Coché = Activé ; Décoché = Désactivé.
Nom de domaine ROOT	Nom de domaine ROOT d'Active Directory. Cette valeur est **NULL** par défaut. Le nom doit être un nom de domaine valide composé de *x.y*, où *x* est une chaîne de 1 à 254 caractères ASCII sans espace entre les caractères et *y* est un type de domaine valide comme com, edu, gov, int, mil, net, org.
Délai d'attente	Durée, en secondes, accordée aux requêtes Active Directory pour qu'elles se terminent. La valeur minimale est supérieure ou égale à 15 secondes. La valeur par défaut est 120 secondes.
Utiliser le schéma standard	Utilise le schéma standard avec Active Directory
Utiliser le schéma étendu	Utilise le schéma étendu avec Active Directory
Nom du DRAC	Nom qui identifie de façon unique la carte DRAC 5 dans Active Directory. Cette valeur est **NULL** par défaut. Le nom doit être une chaîne de 1 à 254 caractères ASCII sans espace entre les caractères.
Nom de domaine du DRAC	Nom DNS (chaîn) du domaine où l'objet DRAC 5 d'Active Directory réside. Cette valeur est **NULL** par défaut. Le nom doit être un nom de domaine valide composé de *x.y*, où *x* est une chaîne de 1 à 254 caractères ASCII sans espace entre les caractères et *y* est un type de domaine valide comme com, edu, gov, int, mil, net, org.
Groupes de rôles	Liste des groupes de rôles associés à la carte DRAC 5. Pour modifier les paramètres d'un groupe de rôles, cliquez sur le numéro du groupe de rôles dans la liste des groupes de rôles. La fenêtre **Configurer le groupe de rôles** s'affiche. **REMARQUE :** Si vous cliquez sur le lien du groupe de rôles avant d'appliquer les paramètres pour la page **Configuration et gestion d'Active Directory**, vous perdrez ces paramètres.
Nom du groupe	Nom qui identifie le groupe de rôles dans Active Directory associé à la carte DRAC 5.
Domaine du groupe	Domaine dans lequel figure le groupe.
Privilège du groupe	Niveau de privilège du groupe.

Tableau 6-11. Boutons de la page Configuration et gestion d'Active Directory

Bouton	Description
Imprimer	Imprime la page **Configuration et gestion d'Active Directory**.
Appliquer	Enregistre les modifications apportées à la page **Configuration et gestion d'Active Directory**.
Retourner à la page Menu principal d'Active Directory	Retourne à la page **Menu principal d'Active Directory**.

Tableau 6-12. Privilèges du groupe de rôles

Paramètre	Description

Niveau de privilège du groupe de rôles	Spécifie le privilège maximum de l'utilisateur du DRAC sur un des privilèges suivants : Administrateur, Utilisateur privilégié, Invité, Aucun ou Personnalisé. Voir Tableau 6-13 pour connaître les droits **Groupe de rôles**.
Ouvrir une session sur le DRAC	Permet à l'utilisateur d'ouvrir une session sur le DRAC.
Configurer le DRAC	Permet à l'utilisateur de configurer le DRAC.
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 du DRAC.
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.

Tableau 6-13. Droits du groupe de rôles

Propriété	**Description**
Administrateur	**Ouvrir une session sur le DRAC**, **Configurer le DRAC**, **Configurer les utilisateurs**, **Effacer les journaux**, **Exécuter les commandes de contrôle du serveur**, **Accéder à la redirection de console**, **Accéder au média virtuel**, **Tester les alertes**, **Exécuter des commandes de diagnostic**
Utilisateur privilégié	**Ouvrir une session sur le DRAC**, **Effacer les journaux**, **Exécuter les commandes de contrôle du serveur**, **Accéder à la redirection de console**, **Accéder au média virtuel**, **Tester les alertes**
Invité	**Ouvrir une session sur le DRAC**
Personnalisé	Sélectionne n'importe quelle combinaison parmi les droits suivants : **Ouvrir une session sur le DRAC**, **Configurer le DRAC**, **Configurer les utilisateurs**, **Effacer les journaux**, **Exécuter des commandes d'action du serveur**, **Accéder à la redirection de console**, **Accéder au média virtuel**, **Tester les alertes**, **Exécuter des commandes de diagnostic**
Aucun.	Aucun droit attribué

Téléchargement d'un certificat CA d'Active Directory

1. Sur la page **Menu principal d'Active Directory**, sélectionnez **Télécharger le certificat CA d'Active Directory** et cliquez sur **Suivant**.
2. Sur la page **Téléchargement d'un certificat**, dans le champ **Chemin d'accès au fichier**, tapez le chemin d'accès au fichier du certificat ou cliquez sur **Parcourir** pour accéder au fichier de certificat.

   REMARQUE : La valeur **Chemin d'accès au fichier** affiche le chemin de fichier relatif du certificat que vous téléchargez. Vous devez entrer 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 **Téléchargement d'un certificat** pour continuer. Reportez-vous à la section Tableau 6-11.

Téléchargement d'un certificat du serveur DRAC

1. Sur la page **Menu principal d'Active Directory**, sélectionnez **Télécharger un certificat de serveur DRAC** et cliquez sur **Suivant**.
2. Dans la fenêtre **Téléchargement de fichier**, cliquez sur **Enregistrer** et enregistrez le fichier dans un répertoire de votre système.
3. Dans la fenêtre **Téléchargement terminé**, cliquez sur **Fermer**.

Affichage d'un certificat CA d'Active Directory

Utilisez la page **Menu principal d'Active Directory** pour afficher un certificat de serveur CA pour votre DRAC 5.

1. Sur la page **Menu principal d'Active Directory**, sélectionnez **Afficher le certificat CA d'Active Directory** et cliquez sur **Suivant**.

   Tableau 6-14 décrit les champs et les descriptions associées énumérés dans la fenêtre **Certificat**.

2. Cliquez sur le bouton approprié de la page **Afficher le certificat CA d'Active Directory** pour continuer. Reportez-vous à la section Tableau 6-11.

Tableau 6-14. Informations relatives au certificat CA d'Active Directory

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

Activation de SSL sur un contrôleur de domaine

Lorsque le DRAC 5 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 téléchargé sur le DRAC 5. En d'autres termes, pour que le DRAC 5 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**, cliquez-droite 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 CA racine du contrôleur de domaine sur le DRAC 5

REMARQUE : Si votre système exécute Windows 2000, 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 sur **Console** pour les machines Windows 2000**)** et sélectionnez **Ajouter/Supprimer un snap-in**.
5. Dans la fenêtre **Ajouter/Supprimer un snap-in**, cliquez sur **Ajouter**.
6. Dans la fenêtre **Snap-in autonome**, sélectionnez **Certificats** et cliquez sur **Ajouter**.
7. Sélectionnez le compte **Ordinateur** et cliquez sur **Suivant**.
8. Sélectionnez **Ordinateur local** et cliquez sur **Terminer**.
9. Cliquez sur **OK**.
10. Dans la fenêtre **Console 1**, développez le dossier **Certificats**, puis le dossier **Personnel** et cliquez sur le dossier **Certificats**.
11. Repérez et cliquez-droite sur le certificat 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. Téléchargez le certificat que vous avez enregistré à l'étape 14 sur le DRAC 5.

    Pour télécharger le certificat à l'aide de la RACADM, voir « Configuration du DRAC 5 avec Active Directory avec le schéma étendu et l'interface Web ».

Pour télécharger le certificat à l'aide de l'interface Web, effectuez la procédure suivante :

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

b. Ouvrez une session sur l'interface Web du DRAC 5.

c. Développez l'arborescence du **système** et cliquez sur **Accès distant**.

d. Cliquez sur l'onglet **Configuration**, puis sur **Sécurité**.

e. Sur la page **Menu principal du certificat de sécurité**, sélectionnez **Télécharger le certificat du serveur** et cliquez sur **Appliquer**.

f. Sur l'écran **Téléchargement d'un certificat**, effectuez l'une des procédures suivantes :

- Cliquez sur **Parcourir** et sélectionnez le certificat
- Dans le champ **Valeur**, tapez le chemin d'accès au certificat.

g. Cliquez sur **Appliquer**.

Importation du certificat SSL du micrologiciel du DRAC 5

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 télécharger le certificat du serveur DRAC 5 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 du DRAC 5 dans toutes les listes de certificats de confiance de contrôleur de domaine.

REMARQUE : Si votre système exécute Windows 2000, les étapes suivantes peuvent varier.

REMARQUE : Si le certificat SSL du micrologiciel du DRAC 5 est signé par une CA bien connue, vous n'avez pas besoin d'effectuer les étapes décrites dans cette section.

Le certificat SSL du DRAC 5 est le même que celui utilisé pour le serveur Web du DRAC 5. Tous les contrôleurs du DRAC 5 sont expédiés avec un certificat auto-signé par défaut.

Pour accéder au certificat en utilisant l'interface Web du DRAC 5, sélectionnez **Configuration**→ **Active Directory**→ **Télécharger le certificat de serveur du DRAC 5**.

1. Sur le contrôleur de domaine, ouvrez une fenêtre **Console MMC** et sélectionnez **Certificats**→ **Autorités de certification racines de confiance**.

2. Cliquez-droite 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 du RAC 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**.

Définition de l'heure SSL sur le DRAC 5

Lorsque le DRAC 5 authentifie un utilisateur Active Directory, le DRAC 5 vérifie également le certificat publié par le serveur Active Directory pour s'assurer que le DRAC communique avec un serveur Active Directory autorisé.

Cette vérification garantit également que la validité du certificat respecte la période de temps spécifiée par le DRAC 5. Il est toutefois possible qu'une discordance existe entre les fuseaux horaires spécifiés sur le certificat et le DRAC 5. Ceci peut se produire lorsque l'heure du DRAC 5 reflète l'heure locale du système et que le certificat reflète l'heure GMT.

Pour vous assurer que le DRAC 5 utilise l'heure GMT pour la comparer avec les heures du certificat, vous devez définir l'objet de décalage du fuseau horaire.

```
racadm config -g cfgRacTuning -o cfgRacTuneTimeZoneOffset <valeur de décalage>
```

Pour plus d'informations, voir « cfgRacTuneTimezoneOffset (lecture/écriture) ».

Configuration Active Directory prise en charge

L'algorithme de requête d'Active Directory du DRAC 5 prend en charge plusieurs arborescences dans une seule forêt.

L'authentification Active Directory du DRAC 5 prend en charge le mode mixte (c'est-à-dire lorsque les contrôleurs de domaine de la forêt exécutent différents systèmes d'exploitation, comme Microsoft Windows NT® 4.0, Windows 2000 ou Windows Server 2003). Tous les objets utilisés par la procédure de requête du DRAC 5 (parmi l'utilisateur, l'objet Périphérique RAC et l'objet Association) doivent toutefois être dans le même domaine. Le snap-in Utilisateurs et ordinateurs Active Directory étendu par Dell vérifie le mode et limite les utilisateurs pour créer des objets à travers les domaines en mode mixte.

Active Directory du DRAC 5 prend en charge plusieurs environnements du domaine, sous réserve que le niveau de fonction de la forêt du domaine est le mode natif ou le mode Windows 2003. En outre, les groupes parmi lesquels l'objet Association, les objets Utilisateur RAC et les objets Périphérique RAC (y compris l'objet Association) doivent être des groupes universels.

REMARQUE : L'objet Association et l'objet Privilège doivent appartenir au même domaine. Le snap-in Utilisateurs et ordinateurs Active Directory étendu par Dell vous oblige à créer ces deux objets dans le même domaine. D'autres objets peuvent appartenir à différents domaines.

Utilisation d'Active Directory pour ouvrir une session sur le DRAC 5

Vous pouvez utiliser Active Directory pour ouvrir une session DRAC 5 à l'aide de l'un des éléments suivants :

- 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.

Vous pouvez également ouvrir une session du DRAC 5 à l'aide de la carte à puce. Pour plus d'informations, voir « Ouvrir une session du DRAC 5 avec l'autenfication par carte à puce Active Directory ».

Utilisation d'une connexion directe Active Directory

Vous pouvez activer le DRAC 5 pour utiliser le protocole d'autentification de réseau pour activer une ouverture de session individuelle et vous connecter au DRAC 5. Pour plus d'informations sur la configuration du DRAC 5 pour utiliser la fonction d'ouverture de session individuelle d'Active Directory, voir « Activation de l'authentification Kerberos ».

Configuration du DRAC 5 pour utilser une ouverture de session individuelle

1. Accédez à **Accès distant**→ onglet **Configuration**→ sous-onglet **Active Directory**→ sélectionnez **Configurer Active Directory**.
2. A la page Gestion et configuration **Active Directory**, sélectionnez **Ouverture de session individuelle.**

   Cette option vous permet de vous connecter directement à DRAC 5 après avoir ouvert la session de votre poste de travail.

Ouverture d'une session du DRAC 5 à l'aide d'Ouverture de session individuelle

1. Connectez-vous à votre poste de travail à l'aide de votre compte réseau.
2. Accédez à la page Web de DRAC à l'aide de 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 du DRAC 5 et *numéro de port* le numéro de port HTTPS.

   La page Ouverture de session individuelle DRAC 5 apparaît.
3. Cliquez sur **Login (Connexion)**.

Le DRAC 5 se connecte à l'aide de vos références mis en cache de votre système d'exploitation lorsque vous vous connectez à l'aide de votre compte valide Active Directory.

Questions les plus fréquentes

Y a-t-il des restrictions concernant la configuration SSL du contrôleur de domaine ?

Oui. Tous les certificats SSL des serveurs Active Directory de la forêt doivent être signés par la même CA racine puisque le DRAC 5 ne permet de télécharger qu'un seul certificat SSL CA de confiance.

J'ai créé un nouveau certificat du RAC et je l'ai téléchargé ; depuis, l'interface Web ne se lance pas.

Si vous utilisez les services de certificats Microsoft pour générer le certificat du RAC, une cause possible est que vous avez involontairement choisi **Certificat d'utilisateur** au lieu de **Certificat Web** en créant le certificat.

Pour récupérer, générez une CSR, puis créez un nouveau certificat Web à partir des services de certificats Microsoft et chargez-le à l'aide de la CLI RACADM depuis le système géré en utilisant les commandes racadm suivantes : by using the following racadm commands:

```
racadm sslcsrgen [-g] [-u] [-f {nom de fichier}]
```

```
racadm sslcertupload -t 1 -f {web_sslcert}
```

Comment faire si je n'arrive pas à ouvrir une session sur le DRAC 5 avec l'authentification Active Directory ? Comment puis-je résoudre ce problème ?

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 DRAC local, ouvrez une session sur le DRAC 5 à l'aide de vos références d'ouverture locales.

   Lorsque vous avez ouvert une session :

   a. Vérifiez que vous avez coché la case **Activer Active Directory** sur la page Configuration d'Active Directory du DRAC 5.

   b. Vérifiez que le paramètre DNS est correct sur la page Configuration de la mise en réseau du DRAC 5.

   c. Vérifiez que vous avez téléchargé le certificat Active Directory sur le DRAC 5 à partir de la CA racine d'Active Directory.

   d. Vérifiez les certificats SSL des contrôleurs de domaine pour vous assurer qu'ils n'ont pas expiré.

   e. Assurez-vous que le **Nom du DRAC**, le **Nom du domaine racine** et le **Nom du domaine du DRAC** correspondent à la configuration de votre environnement Active Directory.

   f. Assurez-vous que le mot de passe du DRAC 5 contient 127 caractères au maximum. Tandis que le DRAC 5 peut prendre en charge des mots de passe allant jusqu'à 256 caractères, Active Directory prend seulement en charge les mots de passe d'un maximum de 127 caractères.

Retour à la page su sommaire

Retour à la page su sommaire

Configuration de l'authentification par carte à puce

Dell™ Remote Access Controller 5 Guide d'utilisation de la version 1.45 du micrologiciel

La version 1.30 et ultérieure de Dell™ Remote Access Controller 5 (DRAC 5) prend en charge l'*authentification bifactorielle* pour l'ouverture de session sur l'interface Web du DRAC 5. Cette prise en charge est assurée par la fonctionnalité **Ouverture de session par carte à puce** du DRAC 5.

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 de sécurité supérieur en demandant aux utilisateurs d'avoir un mot de passe ou un code PIN et une clé privée pour un certificat numérique.

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 le DRAC 5

Activez la fonctionnalité Ouverture de session par carte à puce du DRAC 5 depuis **Accès distant**→ **Configuration**→ **Carte à puce**.

Si vous sélectionnez :

- **Désactiver** la configuration de la carte à puce, vous êtes invité à saisir un nom d'utilisateur et un mot de passe Microsoft® Active Directory® ou local.
- **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 avec la GUI.

  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 uniquement en charge 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 du DRAC 5 d'utiliser le paramètre **Activer avec la racadm distante** uniquement pour accéder à l'interface utilisateur du DRAC 5 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 du DRAC 5 et/ou la configuration Active Directory a été achevée avant d'activer la fonctionnalité **Ouverture de session par carte à puce**.

- **Activer le contrôle CRL pour l'ouverture de session par carte à puce**, le certificat DRAC 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 du DRAC 5 local pour ouvrir une session avec une carte à puce

Vous pouvez configurer les utilisateurs du DRAC 5 local pour qu'ils ouvrent une session sur le DRAC 5 au moyen de la carte à puce. Accédez à **Accès distant**→ **Configuration**→ **Utilisateurs**.

Toutefois, avant que l'utilisateur puisse ouvrir une session sur le DRAC 5 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 le DRAC 5.

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 téléchargé en tant que certificat de l'utilisateur sur le DRAC 5. 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 télécharger 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 un session du DRAC 5, le nom d'utilisateur que vous configurez dans le DRAC 5 doit avoir la même casse que le User Principle Name (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 d'Active Directory pour ouvrir une session avec une carte à puce

Pour configurer les utilisateurs Active Directory pour qu'ils ouvrent une session sur le DRAC 5 au moyen de la carte à puce, l'administrateur du DRAC 5 doit configurer le serveur DNS, télécharger le certificat CA Active Directory sur le DRAC 5 et activer l'ouverture de session Active Directory. Voir « Utilisation du DRAC 5 avec Microsoft Active Directory » pour plus d'informations sur la configuration des utilisateurs Active Directory.

Vous devez configurer Active Directory et Kerberos pour ouvrir une session Active Directory avec une carte à puce. Voir « Utilisation du DRAC 5 avec Microsoft Active Directory » et « Activation de l'authentification Kerberos » pour des informations sur la manière de les configurer.

Vous avez ouvert une session sur le DRAC avec les privilèges appropriés si vous êtes un utilisateur du DRAC local.

Vous avez ouvert une session sur le DRAC avec les privilèges Microsoft Active Directory appropriés si :

- vous êtes un utilisateur Microsoft Active Directory
- vous êtes configuré dans le DRAC comme pouvant ouvrir une session Active Directory
- le DRAC est activé pour l'authentification Kerberos Active Directory

Configuration de la carte à puce

REMARQUE : Pour modifier ces paramètres, vous devez avoir le droit **Configurer le DRAC 5**.

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.

   Tableau 7-1 fournit des informations sur les paramètres de la page **Carte à puce**.
4. Cliquez sur **Appliquer les modifications**.

Tableau 7-1. 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, saisissez le code PIN de votre carte à puce, puis cliquez sur **Ouvrir une session** pour ouvrir une session sur le DRAC. 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 du DRAC 5 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 le DRAC 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 fonction CRL puisse être utilisée, une adresse IP DNS valide doit être configurée sur le DRAC dans sa configuration réseau. Vous pouvez configurer l'adresse IP DNS dans le DRAC sous **Accès à distance→ Configuration→ Réseau**. L'utilisateur ne sera pas en mesure d'ouvrir une session si : • Le certificat utilisateur est répertorié comme révoqué dans le fichier CRL. • Le DRAC n'est pas en mesure de communiquer avec le serveur de distribution CRL. • Le DRAC 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 le DRAC 5 avec la carte à puce

L'interface Web du DRAC 5 affiche la page Ouverture de session par carte à puce si vous avez activé la fonction Ouverture de session par carte à puce.

REMARQUE : Assurez-vous que la configuration des utilisateurs locaux du DRAC 5 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 du DRAC 5 Web 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 du DRAC 5 et *numéro de port* le numéro de port HTTPS.

   La page **Ouverture de session** du DRAC 5 apparaît et vous invite à insérer la carte à puce.

2. Insérez la carte à puce dans le lecteur et saisissez le code PIN de votre carte à puce.

3. Cliquez sur **Login (Connexion)**.

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, le DRAC 5 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. L'ouverture de session par carte à puce est prise en charge par Microsoft Internet Explorer® uniquement.

Ouvrir une session du DRAC 5 avec l'autenfication par carte à puce Active Directory

1. Ouvrez une session DRAC 5 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 du DRAC 5 et *numéro de port* le numéro de port HTTPS.

   La page Ouverture de session du DRAC 5 apparaît et vous invite à insérer la carte à puce.

2. Insérez la carte à puce dans le lecteur et saisissez le code PIN de votre carte à puce.

3. Cliquez sur **Login (Connexion)**.

   Vous avez ouvert une session du DRAC 5 avec vos références telles qu'elles sont configurées dans Active Directory. Pour plus d'informations, voir « Activation de l'authentification Kerberos ».

Dépannage de l'ouverture de session par carte à puce sur le DRAC 5

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-là, l'émetteur de la carte à puce dans l'entreprise pourra vous aider à obtenir une nouvelle carte à puce.

Impossible d'ouvrir une session sur le DRAC 5 local

Si un utilisateur du DRAC 5 local ne parvient pas à ouvrir une session, vérifiez si le nom d'utilisateur et les certificats utilisateur téléchargés sur le DRAC 5 ont expiré. Les journaux trace du DRAC 5 peuvent fournir des messages importants sur les erreurs, bien que les messages d'erreur soient parfois intentionnellement ambigus à des fins de sécurité.

Impossible d'ouvrir une session sur le DRAC 5 en tant qu'utilisateur Active Directory

Si vous ne parvenez pas à ouvrir une session sur le DRAC 5 en tant qu'utilisateur Active Directory, essayez d'ouvrir une session sur le DRAC 5 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 trace du DRAC 5 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 à la page su sommaire

Retour à la page su sommaire

Activation de l'authentification Kerberos

Dell™ Remote Access Controller 5 Guide d'utilisation de la version 1.45 du micrologiciel

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.

Microsoft® Windows® 2000, Windows XP, Windows Server® 2003, Windows Vista® et Windows Server 2008 utilisent à Kerberos comme méthode d'authentification par défaut.

Au démarrage du DRAC 5 version 1.40, celui-ci utilise Kerberos pour prendre en charge deux types de mécanisme d'authentification : la connexion directe et l'ouverture de session par carte à puce Active Directory®. Pour la connexion directe, le DRAC 5 utilise les références d'utilisateur mises en cache dans le système d'exploitation après que l'utilisateur a ouvert une session avec un compte Active Directory valide.

Au démarrage du DRAC 5 version 1.40, Active Directory utilisera l'authentification à deux facteurs avec carte à puce (TFA) en plus de l'association nom d'utilisateur-mot de passe, comme références valides.

L'authentification Kerberos sur le DRAC 5 échoue si l'heure du DRAC 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** le DRAC.

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 le DRAC 5 pour une ouverture de session Active Directory. Pour plus d'informations, voir « Utilisation d'Active Directory pour ouvrir une session sur le DRAC 5 ».
- Enregistrez le DRAC 5 comme un ordinateur dans le domaine racine Active Directory.
  a. Accédez à **Accès distant**→ onglet **Configuration**→ sous-onglet **Réseau**→ **Paramètres de réseau**.
  b. Fournissez une adresse IP valide pour le **serveur DNS statique/préféré**. Cette valeur est l'adresse IP du DNS faisant partie du domaine racine et qui authentifie les comptes Active Directory des utilisateurs.
  c. Sélectionnez **Enregistrer le DRAC auprès du DNS**
  d. Fournissez un **Nom de domaine DNS** valide.

  Consultez l'*aide en ligne de DRAC 5* pour des informations supplémentaires.

  Étant donné que le DRAC 5 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 server) où vous désirez établir une correspondance entre le DRAC 5 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.domain- name.com@domain-name.COM -mapuser dracname -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -pass * -
  out c:\krbkeytab
  ```

  Le type de cryptage que le DRAC 5 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 produira un fichier keytab que vous devrez télécharger dans le DRAC 5.

REMARQUE : Le fichier keytab contient une clé de cryptage et que vous devrez conserver à un endroit 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 du DRAC doit être synchronisée avec celle du contrôleur de domaine Active Directory.

Configuration du DRAC 5 pour les authentification des ouvertures de session individuelle et Active Directory avec carte à puce

Téléchargez le fichier keytab obtenu à partir du domaine racine Active Directory dans le DRAC 5 :

1. Accédez à **Accès distant**→ onglet **Configuration**→ sous-onglet **Active Directory**.
2. Sélectionnez **Télécharger 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**.

Ouverture d'une session du DRAC 5 à l'aide d'Ouverture de session individuelle

REMARQUE : Pour ouvrir une session du DRAC 5, vérifiez que vous disposez des derniers composants au moment de l'exécution components 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 du DRAC 5 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 fonction pour la première fois.

   Vous venez d'ouvrir une session sur le DRAC 5.

Retour à la page su sommaire

Retour à la page su sommaire

Utilisation de la redirection de console de la GUI

Dell™ Remote Access Controller 5 Guide d'utilisation de la version 1.45 du micrologiciel

Cette section fournit des informations sur l'utilisation de la fonctionnalité de redirection de console du DRAC 5.

Présentation

La fonctionnalité de redirection de console du DRAC 5 vous permet d'accéder à la console locale à distance en mode graphique ou texte. À l'aide de la redirection de console, vous pouvez contrôler un ou plusieurs systèmes compatibles DRAC 5 à partir d'un seul endroit.

Aujourd'hui, avec les possibilités de mise en réseau et Internet, vous n'avez pas à vous trouver devant chaque serveur pour effectuer des tâches de maintenance standard. Vous pouvez gérer les serveurs d'une autre ville ou même à l'autre bout du monde à partir de votre ordinateur de bureau ou 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 redirection de console, le système géré n'indique pas que la console a été redirigée.

La page **Redirection de console** vous permet de gérer le système distant en utilisant le clavier, la vidéo et la souris sur votre station de gestion locale pour contrôler les périphériques correspondants sur un système 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 :

- Seulement deux sessions de redirection de console simultanées sont prises en charge.
- Les sessions de redirection de console peuvent seulement être connectées à un système cible distant.
- Vous ne pouvez pas configurer une session de redirection de console sur le système local.
- Une bande passante réseau disponible minimale de 1 Mo/s est exigée.

Taux de rafraîchissement des résolutions d'écran prises en charge sur le système géré

Tableau 9-1 énumère les résolutions d'écran prises en charge et les taux de rafraîchissement correspondants pour une session de redirection de console qui est exécutée sur le système géré.

Tableau 9-1. Résolutions d'écran prises en charge et taux de rafraîchissement

Résolution d'écran	Taux de rafraîchissement (Hz)
720x400	70
640x480	60, 72, 75, 85
800x600	60, 70, 72, 75, 85
1024x768	60, 70, 72, 75, 85
1280x1024	60

Configuration de votre station de gestion

Pour utiliser la redirection de console sur votre station de gestion, effectuez les procédures suivantes :

1. Installez et configurez un navigateur Web pris en charge. Pour obtenir une liste des navigateurs Web pris en charge, consultez la *Matrice de prise en charge des logiciels des systèmes Dell* sur le site Web Dell Support à l'adresse **support.dell.com**.

PRÉCAUTION : La redirection de console et le média virtuel prennent uniquement en charge les navigateurs Web 32 bits. L'utilisation de navigateurs Web 64 bits peut générer des résultats inattendus ou des défaillances.

   - « Configuration d'un navigateur Web pris en charge »

- Configurez la résolution d'affichage de votre moniteur sur au moins 1280 x 1024 pixels à 60 Hz avec 128 couleurs. Sinon, vous ne pouvez pas voir la console en **Mode plein écran**.
- Si vous utilisez le plug-in Java pour vous connecter, assurez-vous que la version 1.6 ou ultérieure de Java Virtual Machine (JVM) est installée sur votre système.

Configuration de la redirection de console

1. Sur votre station de gestion, ouvrez un navigateur Web pris en charge et ouvrez une session sur le DRAC 5. Pour plus d'informations, voir « Accès à l'interface Web ».
2. Dans l'arborescence **Système**, cliquez sur **Système**.
3. Cliquez sur l'onglet **Console**, puis sur **Configuration**.
4. Dans la page **Configuration de la redirection de console**, utilisez les informations dans le tableau 9-2 pour configurer votre session de redirection de console.
5. Dans la version 1.40 ou versions ultérieures du DRAC 5, vous pouvez sélectionner le type de plug-in **Natif** ou **Java** que vous désirez installer.

   Cliquez sur **Appliquer les modifications**.

Tableau 9-2. Informations de la page Configuration de la redirection de console

Information	Description
Activé	Coché = Activé ; Décoché = Désactivé
Nombre maximal de sessions	Indique le nombre de sessions de redirection de console disponibles.
Sessions actives	Indique le nombre de sessions de redirection de console actives.
Numéro de port de clavier et de souris	Valeur par défaut = 5900
Numéro du port vidéo	Valeur par défaut = 5901
Cryptage vidéo activé	Coché = Activé ; Décoché = Désactivé
Vidéo locale du serveur activée	Coché = Activé ; Décoché = Désactivé
Type de Plug-in	Vous permet de sélectionner le plug-in **Native** (ActiveX pour Windows et XPI plug-in pour Linux) ou **Java**. **REMARQUE :** Si vous sélectionnez le plug-in Java, assurez-vous d'avoir déjà installé la version 1.6 ou ultérieure de Java Virtual Machine (JVM) sur votre système.

Les boutons répertoriés dans le tableau 9-3 sont disponibles sur la page **Configuration de la redirection** de console.

Tableau 9-3. Boutons de la page Configuration de la redirection de console

Propriété	Description
Imprimer	Imprime la page **Configuration de la redirection** de console.
Actualiser	Imprime la page **Configuration de la redirection** de console.
Appliquer les modifications	Enregistre vos paramètres de configuration.

REMARQUE : La version 1.30 et ultérieure du DRAC 5 vous permet de désactiver la redirection de console pour un utilisateur distant. Pour plus d'informations, voir « Désactivation du KVM virtuel distant du DRAC 5 ».

Ouverture d'une session de redirection de console

Quand 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 du visualiseur KVM virtuel, vous pouvez contrôler les fonctions de souris et de clavier du système à partir d'une station de gestion locale ou distante.

Pour ouvrir une session de redirection de console :

1. Sur votre station de gestion, ouvrez un navigateur Web pris en charge et ouvrez une session sur le DRAC 5. Pour plus d'informations, voir « Accès à l'interface Web ».
2. Dans l'arborescence **Système**, cliquez sur **Système** puis, dans l'onglet **Console**, cliquez sur **Redirection de console**.

REMARQUE : Si vous recevez un avertissement de sécurité vous demandant d'installer et d'exécuter le plug-in de redirection de console, vérifiez l'authenticité du plug-in et cliquez ensuite sur **Oui** pour installer et exécuter le plug-in. Si vous exécutez Firefox, redémarrez le navigateur et allez à étape 1.

3. Dans la page **Redirection de console**, utilisez les informations dans le tableau 9-4 pour garantir qu'une session de redirection de console est disponible.

Tableau 9-4. Informations de la page Redirection de console

Propriété	Description
Redirection de console activée	Oui/Non
Cryptage vidéo activé	Oui/Non
Vidéo locale du serveur activée	Oui/Non
État	Connecté ou Déconnecté
Nombre maximal de sessions	Nombre maximal de sessions de redirection de console prises en charge
Sessions actives	Nombre actuel de sessions de redirection de console actives.
Type de Plug-in	Le type de plug-in que vous sélectionnez sur la page **Configuration de la redirection de console**.

Les boutons répertoriés dans le tableau 9-5 sont disponibles sur la page **Redirection de console**.

Tableau 9-5. Boutons de la page Redirection de console

Bouton	Définition
Actualiser	Recharge la page **Configuration de la redirection de console**
Connecter	Ouvre une session de redirection de console sur le système distant ciblé.
Imprimer	Imprime la page **Configuration de la redirection de console**.

4. Pour ouvrir une nouvelle console, cliquez sur **Connecter**.

   Si une session de redirection de console est disponible, cliquez sur **Connecter**. Si vous utilisez un navigateur Firefox, il vous invitera à ouvrir ou à enregistrer un fichier JNLP. Vous pouvez l'ouvrir avec *Java™ Web Start Launcher*. Si vous choisissez d'enregistrer le fichier JNLP, ouvrez-le manuellement avant de déconnecter la session. Lorsque vous avez déconnecté la session, il sera impossible de valider le fichier JNLP enregistré. Si vous utilisez Internet Explorer®, celui-ci met en cache le fichier JNLP dans le dossier *Fichiers Internet temporaires* et s'exécute automatiquement au moyen de *Java Web Start Launcher*.

   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.

   Lorsque vous avez fini d'utiliser la console et que vous avez fermé la session (en suivant la procédure de fermeture de session du système distant), cliquez sur **Déconnecter** dans la page Redirection de console ou fermez le visualiseur.

   La station de gestion se connecte au DRAC 5 et le bureau du système distant apparaît dans l'application du visualiseur KVM numérique de Dell.

5. Si deux pointeurs de souris apparaissent sur le bureau du système distant, synchronisez les curseurs de la souris sur la station de gestion et le système distant. Voir « Synchronisation des curseurs de souris ».

Désactivation ou activation de la vidéo locale

Pour désactiver ou activer la vidéo locale, procédez comme suit :

1. Sur votre station de gestion, ouvrez un navigateur Web pris en charge et ouvrez une session sur le DRAC 5. Pour plus d'informations, voir « Accès à l'interface Web ».

2. Dans l'arborescence **Système**, cliquez sur **Système**.

3. Cliquez sur l'onglet **Console**, puis sur **Configuration**.

4. Si vous souhaitez activer (mettre sur MARCHE) la vidéo locale sur le serveur, dans la page **Configuration de la redirection de console**, cochez la case **Vidéo locale du serveur activée** puis cliquez sur **Appliquer les modifications**. La valeur par défaut est MARCHE.

5. Si vous souhaitez désactiver (mettre sur ARRÊT) la vidéo locale sur le serveur, dans la page **Configuration de la redirection de console**, décochez la case **Vidéo locale du serveur activée** puis cliquez sur **Appliquer les modifications**.

La page **Redirection de console** affiche l'état de la vidéo locale du serveur.

REMARQUE : La fonction Vidéo locale du serveur activée est prise en charge sur tous les systèmes *x9xx* PowerEdge™, à l'exception des systèmes PowerEdge SC1435 et 6950.

REMARQUE : En désactivant (mettant sur ARRÊT) la vidéo locale sur le serveur, seul le moniteur connecté au serveur local sera désactivé.

REMARQUE : La version 1.30 et ultérieure du DRAC 5 vous permet de désactiver la redirection de console pour un utilisateur distant. Pour plus d'informations, voir « Désactivation du KVM virtuel distant du DRAC 5 ».

Utilisation du visualiseur vidéo

Le visualiseur vidéo fournit une interface utilisateur entre la station de gestion et le système distant, vous permettant de visualiser le bureau du système distant et de contrôler ses fonctions de clavier et de souris à partir de votre station de gestion. Lorsque vous vous connectez au système distant, le visualiseur de vidéo démarre dans une fenêtre séparée.

Le visualiseur de vidéo propose différents réglages de commande comme le calibrage vidéo, l'accélération de la souris et la création d'instantanés. Cliquez sur **Aide** pour plus d'informations sur ces fonctions.

Lorsque vous démarrez une session de redirection de console et que le visualiseur vidéo apparaît, vous pouvez être amené à régler les commandes suivantes pour visualiser et contrôler correctement le système distant. Ces réglages incluent :

- Accès à la barre de menus du visualiseur
- Réglage de la qualité vidéo
- Synchronisation des curseurs de souris

Accès à la barre de menus du visualiseur

La barre de menus du visualiseur est une barre de menus masquée. Pour accéder à la barre de menus, déplacez votre curseur en haut et au centre de la fenêtre du bureau du visualiseur.

La barre de menus peut également être activée en appuyant sur la touche de fonction par défaut <F9>. Pour réattribuer cette touche de fonction à une nouvelle fonction :

1. Appuyez sur <F9> ou déplacez votre curseur de souris en haut du visualiseur vidéo.
2. Appuyez sur la « punaise » pour fermer la barre de menus du visualiseur.
3. Dans la barre de menus du visualiseur, cliquez sur **Outils** et sélectionnez **Options de session**.
4. Dans la fenêtre **Options de session**, cliquez sur l'onglet **Généralités**.
5. Dans la fenêtre de l'onglet **Généralités**, dans la case **Séquence de touches d'activation de menu**, cliquez sur le menu déroulant et sélectionnez une autre touche de fonction.
6. Cliquez sur **Appliquer**, puis sur **OK**.

Tableau 9-6 illustre les principales fonctionnalités qui sont disponibles dans la barre de menus du visualiseur.

Tableau 9-6. Sélections sur la barre de menus du visualiseur

Élément de menu	Élément	Description
Fichier	Capturer vers un fichier	Capture l'écran du système distant actuel dans un fichier **.bmp** (Windows) ou **.png** (Linux) sur le système local. Une boîte de dialogue s'affiche pour que vous puissiez enregistrer le fichier dans un emplacement précisé.
	Quitter	Quitte la page **Redirection de console**.
Afficher	Actualiser	Met à jour toute la fenêtre d'affichage du système distant.
	Plein écran	Développe l'écran de session d'une fenêtre vers le plein écran.
Macros	Divers raccourcis clavier	Exécute une séquence de touches sur le système distant Pour connecter le clavier de votre station de gestion au système distant et exécuter une macro : 1. Cliquez sur **Outils**. 2. Dans la fenêtre **Options de session**, cliquez sur l'onglet **Généralités**. 3. Sélectionnez **Transmettre toutes les séquences de touches à la cible**. 4. Cliquez sur **OK**. 5. Cliquez sur **Macros**. 6. Dans le menu **Macros**, cliquez sur une séquence de touches à exécuter sur le système cible.
Outils	Réglage vidéo automatique	Recalibre la sortie vidéo du visualiseur de session.
	Réglage vidéo manuel	Fournit des commandes individuelles pour régler manuellement la sortie vidéo du visualiseur de session. **REMARQUE :** Le réglage excentré de la position horizontale désynchronise les curseurs de la souris.
	Options de	Fournit des réglages de commandes du visualiseur de session supplémentaires.

	session	L'onglet **Souris** vous permet d'optimiser les performances de la souris en fonction de votre système d'exploitation. Sélectionnez une frappe de terminaison dans le menu déroulant pour quitter le mode curseur unique. L'option **Frappe de terminaison** est disponible si le type de plug-in est **Java**. L'onglet **Généralités** fournit les options suivantes : • **Mode de transmission au clavier :** sélectionnez **Transmettre toutes les séquences de touches à la cible** pour transmettre les séquences de touches de votre station de gestion au système distant. • **Séquence de touches d'activation de menus** : sélectionne la touche de fonction qui active la barre de menus du visualiseur. La zone de liste **Délai de masquage de la barre d'outils** vous permet de régler l'intervalle entre le retrait du curseur de la souris et la disparition de la barre de menus lorsque vous ne cliquez pas sur le bouton en forme de punaise sur la barre de menus. Cette option est disponible si le type de plug-in est **Natif**.
Aide	N/A	Active le menu **Aide**.

Réglage de la qualité vidéo

Le visualiseur vidéo propose des réglages vidéo qui vous permettent d'optimiser la vidéo pour obtenir le meilleur affichage possible. Cliquez sur **Aide** pour plus d'informations.

Pour régler automatiquement la qualité vidéo :

1. Accédez à la barre de menus du visualiseur. Voir « Accès à la barre de menus du visualiseur ».
2. Cliquez sur **Outils** et sélectionnez **Réglage vidéo automatique** (pour le plug-in **Natif**) ou **Réglages vidéo** (pour le plug-in **Java**) afin de régler automatiquement la qualité vidéo de la fenêtre Visualiseur.

Pour régler manuellement la qualité vidéo :

1. Accédez à la barre de menus du visualiseur. Voir « Accès à la barre de menus du visualiseur ».
2. Cliquez sur **Outils** et sélectionnez **Réglage vidéo manuel** (pour le plug-in **Natif**) ou **Réglages vidéo** (pour le plug-in **Java**).
3. Dans la fenêtre **Réglage vidéo manuel**, cliquez sur chaque bouton de réglage vidéo et réglez les commandes, si nécessaire.
4. Lorsque vous avez terminé, cliquez sur **Fermer** pour quitter la boîte de dialogue **Réglage vidéo manuel**.

Lorsque vous réglez manuellement la qualité vidéo, suivez les instructions suivantes :

- Pour empêcher toute désynchronisation des pointeurs de souris, réglez le paramètre horizontal de sorte que le bureau du système distant soit centré dans la fenêtre de session.
- La réduction du paramètre Rapport pixel/parasite sur zéro déclenche plusieurs commandes d'actualisation vidéo, ce qui génère un trafic réseau excessif et une vidéo tremblotante dans la fenêtre du visualiseur vidéo. Dell vous recommande de régler le paramètre Rapport pixel/parasite sur un niveau qui offre une performance optimale du système et une optimisation des pixels tout en minimisant le trafic réseau.

Synchronisation des curseurs de souris

Lorsque vous vous connectez à un système Dell distant en utilisant la redirection de console, la vitesse d'accélération de la souris sur le système distant peut ne pas être synchronisée avec le curseur de souris de votre station de gestion, provoquant l'apparition de deux curseurs de souris dans la fenêtre du visualiseur vidéo.

Pour synchroniser les curseurs de souris :

1. Accédez à la barre de menus du visualiseur. Voir « Accès à la barre de menus du visualiseur ».
2. Cliquez sur **Outils** et sélectionnez **Options de session**.
3. Cliquez sur l'onglet **Souris**, sélectionnez le système d'exploitation de votre station de gestion et cliquez sur **OK**.
4. Cliquez sur **Outils** et sélectionnez **Réglage vidéo manuel**.
5. Réglez les commandes horizontales de sorte que le bureau du système distant apparaisse au centre de la fenêtre de session.
6. Cliquez sur **OK**.

Lorsque vous utilisez Linux (Red Hat® ou Novell®), les paramètres de souris par défaut du système d'exploitation sont utilisés pour diriger la flèche de la souris sur l'écran de redirection de console du DRAC 5.

REMARQUE : Les systèmes Linux (Red Hat ou Novell) présentent des problèmes connus de synchronisation des curseurs de souris. Pour éviter des problèmes de synchronisation de souris, assurez-vous que tous les utilisateurs utilisent les paramètres de souris par défaut.

Pour des informations sur la désactivation de la redirection de console, voir « Désactivation du KVM virtuel distant du DRAC 5 ».

Questions les plus fréquentes

Peut-on démarrer une nouvelle session vidéo de console distante lorsque la vidéo locale sur le serveur est désactivée ?

Oui.

Pourquoi la désactivation de la vidéo locale sur le serveur prend-elle 15 secondes après avoir demandé à désactiver la vidéo locale ?

Cela permet à un utilisateur local de prendre des mesures avant que la vidéo ne soit désactivée.

Un délai s'applique-t-il à l'activation de la vidéo locale ?

Non, dès qu'une demande d'activation de la vidéo locale est reçue par le DRAC 5, la vidéo est activée instantanément.

L'utilisateur local peut-il également désactiver la vidéo ?

Oui, un utilisateur local peut utiliser la CLI racadm (locale) pour désactiver la vidéo.

L'utilisateur local peut-il également activer la vidéo ?

Oui, l'utilisateur doit avoir installé la CLI racadm sur le serveur et il doit être capable d'accéder au serveur sur une connexion RDP, comme les services de terminal, une connexion telnet ou SSH. L'utilisateur peut alors ouvrir une session sur le serveur et exécuter la racadm (locale) pour activer la vidéo.

Ma vidéo locale est désactivée et, pour une raison quelconque, mon DRAC 5 n'est pas accessible à distance et le serveur n'est pas accessible avec une connexion RDP, telnet ou SSH. Comment puis-je récupérer la vidéo locale ?

La seule manière de récupérer la vidéo locale dans ce cas consiste à débrancher le cordon d'alimentation en CA du serveur, en évacuant l'alimentation libre du serveur et en rebranchant le cordon d'alimentation en CA afin de ramener la vidéo locale sur le moniteur du serveur . En outre, la configuration du DRAC 5 est modifiée, la vidéo locale étant activée (par défaut). Le DRAC 5 doit être reconfiguré si la vidéo locale doit à nouveau être désactivée.

La coupure de la vidéo locale coupe-t-elle également le clavier et la souris locaux ?

Non, la coupure de la vidéo locale coupe uniquement la vidéo provenant du connecteur de sortie du moniteur du serveur, elle ne coupe *pas* le clavier et la souris connectés localement au serveur.

La désactivation de la vidéo locale du serveur désactive-t-elle la vidéo lors de la session à distance du vKVM ?

Non, l'activation ou la désactivation de la vidéo locale est indépendante de la session à distance de la console.

Quels sont les privilèges que doit posséder un utilisateur du DRAC 5 pour activer ou désactiver la vidéo locale du serveur ?

Tout utilisateur possédant des privilèges de configuration du DRAC 5 peut activer ou désactiver la vidéo locale du serveur.

Comment connaître l'état actuel de la vidéo locale du serveur ?

L'état est affiché dans la page **Configuration de la redirection de console** de l'interface Web du DRAC 5. La commande CLI racadm (`racadm getconfig -g cfgRacTuning`) affiche l'état dans l'objet cfgRacTuneLocalServerVideo. L'utilisateur local peut également consulter l'état sur l'écran LCD du serveur sous la forme « Vidéo désactivée » ou « Vidéo désactivée dans 15 ».

Pour quelle raison l'état « Vidéo désactivée » ou « Vidéo désactivée dans 15 » n'apparaît-il pas parfois sur l'écran LCD du serveur ?

L'état de la vidéo locale est un message de faible priorité qui sera masqué si un événement de haute priorité s'est produit sur le serveur. Les messages de l'écran LCD sont affichés par ordre de priorité ; vous devez résoudre les messages de haute priorité de l'écran LCD et une fois cet événement effacé ou résolu, le message de faible priorité suivant est affiché. Le message relatif à la vidéo du serveur sur l'écran LCD est purement informationnel.

Où puis-je obtenir des informations supplémentaires sur la fonctionnalité Vidéo locale du serveur ?

Consultez le site Web de support de Dell à l'adresse **support.dell.com** pour un livre blanc traitant de cette fonctionnalité.

Je vois une corruption vidéo sur mon écran. Comment résoudre ce problème ?

Dans la fenêtre **Redirection de console**, cliquez sur **Actualiser** pour actualiser l'écran.

REMARQUE : Vous devrez peut-être cliquer plusieurs fois sur **Actualiser** pour corriger la corruption vidéo.

Pendant la redirection de console, le clavier et la souris se sont verrouillés quand mon système Windows 2000 est sorti d'une veille prolongée. Pourquoi ?

Pour résoudre ce problème, réinitialisez le DRAC 5 en exécutant la commande **racadm racreset**.

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.

Pendant la redirection de console, la souris s'est verrouillée quand mon système Windows Server 2003 est sorti d'une veille prolongée. Pourquoi ?

Pour résoudre ce problème, sélectionnez un système d'exploitation autre que Windows pour l'accélération de la souris à partir du menu déroulant de la fenêtre KVM virtuel (vKVM), patientez 5 à 10 secondes, puis sélectionnez Windows de nouveau. Si le problème n'est pas résolu, vous devez réinitialiser le DRAC 5 en exécutant la commande **racadm racreset**.

Si le problème n'est toujours pas résolu, vous devez réinitialiser le DRAC 5 en exécutant la commande **racadm racreset hard**.

Le clavier et la souris vKVM ne fonctionnent pas. Pourquoi ?

Vous devez définir le contrôleur USB sur **Activé avec prise en charge du BIOS** dans les paramètres du BIOS du système géré. Redémarrez le système géré et appuyez sur <F2> pour accéder au programme de configuration. Sélectionnez **Périphériques intégrés**, puis **Contrôleur USB**. Enregistrez vos modifications et redémarrez le système.

L'écran de la console du système géré est vide quand celui de Windows est bleu. Pourquoi ?

Le système géré n'a pas le pilote vidéo ATI qui convient. Vous devez mettre le pilote vidéo à jour avec le DVD *Dell Systems Management Tools and Documentation*.

L'écran est blanc sur la console distante quand l'installation de Windows 2000 est terminée. Pourquoi ?

Le système géré n'a pas le pilote vidéo ATI qui convient. La redirection de console du DRAC 5 ne fonctionne pas correctement avec le pilote vidéo SGVA du CD de distribution de Windows 2000. Vous devez installer Windows 2000 à l'aide du DVD *Dell Systems Management Tools and Documentation* pour obtenir les tous derniers pilotes pris en charge pour le système géré.

L'écran du système géré est vide lorsque je charge le système d'exploitation Windows 2000. Pourquoi ?

Le système géré n'a pas le pilote vidéo ATI qui convient. Vous devez mettre le pilote vidéo à jour avec le DVD *Dell Systems Management Tools and Documentation*.

L'écran du système géré est vide dans la fenêtre DOS plein écran de Windows. Pourquoi ?

Le système géré n'a pas le pilote vidéo ATI qui convient. Vous devez mettre le pilote vidéo à jour avec le DVD *Dell Systems Management Tools and Documentation*.

Je n'arrive pas à accéder au programme de configuration du BIOS en appuyant sur la touche <F2>. Pourquoi ?

Ce comportement est typique des environnements Windows. Utilisez votre souris pour cliquer sur une zone de la fenêtre Redirection de console pour ajuster le point de référence. Pour déplacer le point de référence sur la barre de menus du bas de la fenêtre Redirection de console, utilisez la souris et cliquez sur l'un des objets de cette barre.

La souris vKVM ne se synchronise pas lorsque j'utilise le DVD *Dell Systems Management Tools and Documentation* pour installer le système d'exploitation à distance. Pourquoi ?

Configurez la redirection de console pour le système d'exploitation qui est exécuté sur le système cible.

1. Dans le menu de barre d'outils vKVM, cliquez sur **Outils** et sélectionnez **Options de session**.
2. Dans la fenêtre **Options de session**, cliquez sur l'onglet **Souris**.
3. Dans la case **Accélération de la souris**, sélectionnez le système d'exploitation qui est exécuté sur le système cible et cliquez sur **OK**.

La souris vKVM ne se synchronise pas lorsque mon système Windows sort d'un état de veille prolongée. Pourquoi ?

Sélectionnez un autre système d'exploitation pour l'accélération de la souris dans le menu déroulant de la fenêtre vKVM. Ensuite, retournez au système d'exploitation d'origine pour initialiser le périphérique de souris USB.

1. Dans la barre d'outils vKVM, cliquez sur **Outils** et sélectionnez **Options de session**.
2. Dans la fenêtre **Options de session**, cliquez sur l'onglet **Souris**.
3. Dans la boîte **Accélération de la souris**, sélectionnez un autre système d'exploitation et cliquez sur **OK**.
4. Initialisez le périphérique de souris USB.

La souris ne se synchronise pas sous DOS pendant la redirection de console. Pourquoi ?

Le BIOS de Dell émule le pilote de souris comme s'il s'agissait d'une souris PS/2. La souris PS/2 est conçue pour utiliser la position relative de son pointeur, ce qui produit un délai de synchronisation. Le DRAC 5 a un pilote de souris USB, ce qui permet un positionnement absolu et un suivi plus proche du pointeur de la souris. Même si le DRAC 5 passait la position absolue de la souris USB au BIOS de Dell, l'émulation du BIOS la reconvertirait en position relative et le comportement ne changerait pas.

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 le bureau du système cible est centré dans la fenêtre de redirection de console.

1. Dans la barre d'outils vKVM, cliquez sur **Outils** et sélectionnez **Réglage vidéo manuel**.
2. Réglez les commandes horizontales et verticales, si nécessaire, pour aligner le bureau dans la fenêtre de redirection de console.
3. Cliquez sur **Close (Fermer)**.
4. Déplacez le curseur de souris du système cible en haut à gauche de la fenêtre de redirection de console et remettez-le au centre de la fenêtre.

5. Répétez les étapes 2 à 4 jusqu'à ce que les deux curseurs soient synchronisés.

La souris et le clavier vKVM ne fonctionnent pas si l'on change l'accélération de la souris pour différents systèmes d'exploitation. Pourquoi ?

Le clavier et la souris vKVM USB sont inactifs pendant les 5 à 10 secondes qui suivent le changement de l'accélération de la souris. Si le réseau est chargé, il arrive que cette opération prenne plus de temps (plus de 10 secondes).

Je ne vois pas le bas de l'écran du serveur sur la fenêtre vKVM. Pourquoi ?

Assurez-vous que la résolution d'écran du serveur est de 1280 x 1024 pixels à 60 Hz avec 128 couleurs.

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 du DRAC 5. Pourquoi ?

Lorsque vous installez à distance un système d'exploitation Microsoft pris en charge sur un système dont la fonctionnalité 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 système 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.

La redirection de console ne montre pas le menu de démarrage du système d'exploitation dans les versions chinoises, japonaises et coréennes de Microsoft Windows 2000. Pourquoi ?

Sur les systèmes fonctionnant sous Windows 2000 qui peuvent démarrer sur plusieurs systèmes d'exploitation, changez le système d'exploitation de démarrage par défaut en effectuant les étapes suivantes :

1. Cliquez-droite sur l'icône **Poste de travail** et sélectionnez **Propriétés**.
2. Cliquez sur l'onglet **Avancé**.
3. Cliquez sur **Démarrage et récupération**.
4. Sélectionnez le nouveau système d'exploitation par défaut dans la liste **Démarrage**.
5. Dans la case **Afficher** la liste pendant, tapez la durée, en secondes, pendant laquelle la liste de choix doit s'afficher avant que le système d'exploitation par défaut ne démarre automatiquement.

Pourquoi l'indicateur Verr Num sur ma station de gestion ne reflète-t-il pas l'état Verr Num sur le serveur distant ?

Quand on y accède via le DRAC 5, l'indicateur Verr Num sur la station de gestion ne correspond pas nécessairement à l'état Verr Num sur le serveur distant. L'état Verr Num dépend du paramètre sur le serveur distant 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 du visualiseur de session apparaissent-elles lorsque j'établis une session de redirection de console ?

Vous configurez une session de redirection de console sur le système local. Reconfigurez la session sur un système distant.

Si j'exécute une session de redirection de console et qu'un utilisateur local accède au système distant, est-ce que je reçois un message d'avertissement ?

Non Si un utilisateur local accède au système, il peut passer outre vos actions sans qu'un avertissement n'apparaisse.

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.

Quel est le nombre maximum de sessions de redirection de console que je peux exécuter sur un système distant ?

Le DRAC 5 prend en charge jusqu'à deux sessions de redirection de console simultanées.

Je rencontre des problèmes pour synchroniser la souris. Pourquoi ?

Les systèmes Linux (Red Hat ou Novell) présentent des problèmes connus de synchronisation des curseurs de souris. Pour éviter des problèmes de synchronisation de souris, assurez-vous que tous les utilisateurs utilisent les paramètres de souris par défaut.

Comment faire pour installer un navigateur Web sur ma station de gestion qui dispose d'un système de fichiers en lecture seule ?

Si vous exécutez Linux et que votre station de gestion a un système de fichiers en lecture seule, un navigateur peut être installé sur un système client sans nécessiter de connexion à un DRAC 5. En utilisant le progiciel d'installation de plug-in natif, le navigateur peut être installé manuellement pendant la phase de configuration du client.

△ **PRÉCAUTION : Dans un environnement client en lecture seule, si le micrologiciel du DRAC 5 est mis à jour avec une version plus récente du plug-in, le plug-in du média virtuel installé devient alors inopérationnel. C'est parce que les fonctionnalités de plug-in plus anciennes ne peuvent pas fonctionner lorsque le micrologiciel contient une version de plug-in plus récente. Dans ce cas, vous êtes invité à installer le plug-in. Comme le système de fichiers est en lecture seule, l'installation échouera et les fonctionnalités de plug-in ne seront pas disponibles.**

Pour vous procurer le progiciel d'installation du plug-in :

1. Ouvrez une session sur un DRAC 5 existant.
2. Dans la barre d'adresses du navigateur, remplacez l'URL :

   ```
   https://<IP_RAC>/cgi-bin/webcgi/main
   ```

   par :

   ```
   https://<IP_RAC>/plugins/ # N'oubliez pas d'inclure la barre oblique.
   ```

3. Identifiez les deux sous-répertoires vm et vkvm. Accédez au sous- répertoire approprié, cliquez-droite sur le fichier rac5XXX.xpi, puis sélectionnez **Enregistrer la cible du lien sous....**
4. Sélectionnez un emplacement pour enregistrer le fichier du progiciel d'installation du plug-in.

Pour installer le progiciel d'installation du plug-in :

1. Copiez le progiciel d'installation sur le partage de système de fichiers natif du client qui est accessible par le client.
2. Ouvrez une instance du navigateur sur le système client.
3. Saisissez le chemin d'accès du fichier vers le progiciel d'installation du plug-in dans la barre d'adresses du navigateur. Par exemple :

   ```
   file:///tmp/rac5vm.xpi
   ```

4. Le navigateur guide l'utilisateur à travers les différentes étapes d'installation du plug-in.

Une fois installé, le navigateur ne demandera plus l'installation de ce plug-in, tant que le micrologiciel du DRAC 5 cible ne contient pas une version plus récente du plug-in.

Pourquoi la session de redirection de console s'arrête et redémarre mon terminal ?

Lorsque les paramètres NIC du DRAC 5 sont en mode « partagé » ou « partagé avec basculement », une réinitialisation système provoque également celle du LAN sur carte mère (LOM). Sur les réseaux avec des commutateurs où le Spanning Tree Protocol (STP) est activé, la connexion entre la station de gestion et le client doit être rétablie après environ de dix à quinze secondes. Par conséquent, la connectivité ave le système distant est perdue et un message d'erreur de connexion perdue est affiché sur la redirection de console et les clients médias virtuels. Si vous accédez à l'interface GUI du DRAC à ce moment, vous recevrez un message d'erreur « Page introuvable ».

Pour contourner ce problème :

- Utilisez le NIC dédié du DRAC 5 pour la connexion sur réseau.
- Désactivez les STP sur les commutateurs réseau.

Retour à la page su sommaire

Retour à la page su sommaire

Glossaire

Dell™ Remote Access Controller 5 Guide d'utilisation de la version 1.45 du micrologiciel

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.

AGP

Abréviation d'Accelerated Graphics Port (port graphique accéléré), une spécification du bus qui permet aux cartes graphiques d'accéder plus rapidement à la mémoire du système principal

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.

BMC

Abréviation de Baseboard Management Controller (contrôleur de gestion de la carte de base), l'interface de contrôleur entre le DRAC 5 et le contrôleur BMC du système géré.

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 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 sur un 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. Le DRAC 5 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).

DRAC 5

Sigle de Dell Remote Access Controller 5.

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.

ICMB

Abréviation d'Intelligent Chassis Management Bus (bus de gestion intelligente du châssis).

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) créée par le DRAC 5 ou le contrôleur BMC qui contient des informations sur les changements d'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 le DRAC 5 et le contrôleur BMC.

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).

LED

Abréviation de Light-Emitting Diode (diode électroluminescente).

LOM

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

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.

PKI

Abréviation de Public Key Infrastructure (infrastructure à clé publique). Une PKI permet aux utilisateurs d'un réseau public non sécurisé comme Internet d'échanger en toute sécurité et en privé des données via une paire de clés cryptographiques publique et privée obtenue et partagée via une autorité de confiance.

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 le DRAC 5.

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 système 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 système géré.

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 déterminer l'accès de l'utilisateur au DRAC 5 ; utilise les objets Active Directory définis par Dell.

schéma standard

Solution utilisée avec Active Directory pour déterminer l'accès de l'utilisateur au DRAC 5 ; utilise les objets du groupe Active Directory uniquement.

SEL

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

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).

SNMP

Abréviation de Simple Network Management Protocol (protocole simplifié de gestion de réseau), protocole conçu pour gérer des nuds sur un réseau IP. Les DRAC 5 sont des périphériques gérés par SNMP (nuds).

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 qui accède au DRAC 5 à distance.

système géré

Le système géré est le système dans lequel le DRAC 5 est installé ou intégré.

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 progiciels Red Hat), un système de gestion de progiciels pour le système d'exploitation Red Hat Enterprise Linux qui facilite l'installation de progiciels. Il ressemble à un programme d'installation.

USB

Abréviation de Universal Serial Bus (bus série universel).

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).

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).

Retour à la page su sommaire